

# 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 URL<sup>4</sup>. Using the My Domain URL allows Salesforce to identify the identity provider and initiate the SSO process<sup>5</sup>. 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 setups<sup>4,6</sup>. 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 (UC) is planning to deploy a custom mobile app that will allow users to get e-signatures from its customers on their mobile devices. The mobile app connects to Salesforce to upload the e-signature as a file attachment and uses OAuth protocol for both authentication and authorization. What is the most recommended and secure OAuth scope setting that an Architect should recommend?

- A. Id
- B. Web
- C. Api
- D. Custom\_permissions

**Answer:** D

**Explanation:**

The most recommended and secure OAuth scope setting for UC's custom mobile app is custom\_permissions. Custom\_permissions are settings that can be used in Apex code or validation rules to check whether a user has access to a custom feature or functionality. Custom\_permissions can also be used as OAuth scopes to limit the access of an external application, such as UC's mobile app, to certain custom features or functionalities in Salesforce. By configuring custom\_permissions as OAuth scopes in the connected app settings, UC can restrict the mobile app access to only the e-signature feature and protect against unauthorized or excessive access.

The other options are not recommended or secure OAuth scope settings for UC's custom mobile app. Id is an OAuth scope that allows the mobile app to access basic information about the user and their org, such as name, email, profile picture, and instance URL. This scope does not provide any access to Salesforce data or features, such as uploading e-signatures. Web is an OAuth scope that allows the mobile app to access Salesforce data and features through a browser or web-view. This scope provides full access to Salesforce data and features, which could expose sensitive information or allow unwanted actions. Api is an OAuth scope that allows the mobile app to make REST or SOAP API calls to Salesforce using the access token. This scope also provides full access to Salesforce data and features, which could compromise security and compliance. References: [OAuth Scopes], [Connected Apps], [Custom Permissions]

**NEW QUESTION 4**

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 risk 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 services and salesforce?

- A. Include client ID and client secret in the login header callout.
- B. Set up a proxy server for the login service in the DMZ.
- C. Require the use of Salesforce security Tokens on password.
- D. Enforce mutual Authentication between systems using SSL.

**Answer:** D

**Explanation:**

To enable a trusted connection between the login services and Salesforce, UC should enforce mutual authentication between systems using SSL. Mutual authentication is a process in which both parties in a communication verify each other's identity using certificates<sup>7</sup>. SSL (Secure Sockets Layer) is a protocol that provides secure communication over the Internet using encryption and certificates<sup>8</sup>. By using mutual authentication with SSL, UC can ensure that only authorized login services can access Salesforce and vice versa. This can prevent unauthorized access, impersonation, or phishing attacks.

References: Mutual Authentication, SSL (Secure Sockets Layer)

**NEW QUESTION 5**

A large consumer company is planning to create a community and will require login through the customers social identity. The following requirements must be met:

- \* 1. The customer should be able to login with any of their social identities, however salesforce should only have one user per customer.
- \* 2. Once the customer has been identified with a social identity, they should not be required to authorize Salesforce.
- \* 3. The customers personal details from the social sign on need to be captured when the customer logs into Salesforce using their social Identity.
- \* 3. If the customer modifies their personal details in the social site, the changes should be updated in Salesforce.

Which two options allow the Identity Architect to fulfill the requirements? Choose 2 answers

- A. Use Login Flows to call an authentication registration handler to provision the user before logging the user into the community.
- B. Use authentication providers for social sign-on and use the custom registration handler to insert or update personal details.
- C. Redirect the user to a custom page that allows the user to select an existing social identity for login.
- D. Use the custom registration handler to link social identities to Salesforce identities.

**Answer:** BD

**Explanation:**

To allow customers to log in to the community with any of their social identities, such as Facebook, Google, or Twitter, the identity architect needs to use authentication providers for social sign-on. Authentication providers are configurations that enable users to authenticate with an external identity provider and access Salesforce resources. To ensure that Salesforce has only one user per customer, regardless of how many social identities they have, the identity architect needs to use the custom registration handler to link social identities to Salesforce identities. The custom 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 custom registration handler can also be used to insert or update personal details of the customers when they log in to Salesforce using their social identity.

References: Authentication Providers, Social Sign-On with Authentication Providers, Create a Custom Registration Handler

**NEW QUESTION 6**

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 7**

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 8**

Universal Containers (UC) has implemented SAML SSO to enable seamless access across multiple applications. UC has regional Salesforce orgs and wants its users to be able to access them from their main Salesforce org seamlessly. 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 9**

Universal Containers (UC) wants to provide single sign-on (SSO) for a business-to-consumer (B2C) application using Salesforce Identity. Which Salesforce license should UC utilize to implement this use case?

- A. Identity Only
- B. Salesforce Platform
- C. External Identity
- D. Partner Community

**Answer:** C

**Explanation:**

External Identity is the license that enables SSO for B2C applications using Salesforce Identity. It also provides self-registration, social sign-on, and user profile management features. References: Certification - Identity and Access Management Architect - Trailhead

**NEW QUESTION 10**

Universal Containers is creating a web application that will be secured by Salesforce Identity using the OAuth 2.1 Web Server Flow (uses the OAuth 2.0 authorization code grant type).

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

- A. Verification URL
- B. Client Secret
- C. Access Token
- D. Scopes

**Answer:** BCD

**Explanation:**

The OAuth 2.0 Web Server Flow requires the client secret to authenticate the web application to Salesforce. The access token is used to access the Salesforce resources on behalf of the user. The scopes define the permissions and access levels for the web application. References: OAuth 2.0 Web Server Authentication Flow, Digging Deeper into OAuth 2.0 on Force.com

**NEW QUESTION 10**

Northern Trail Outfitters (NTO) has an off-boarding process where a terminated employee is first disabled in the Lightweight Directory Act Protocol (LDAP) directory, then requests are sent to the various application support teams to finish user deactivations. A terminated employee recently was able to login to NTO's Salesforce instance 24 hours after termination, even though the user was disabled in the corporate LDAP directory.

What should an identity architect recommend to prevent this from happening in the future?

- A. Create a Just-in-Time provisioning registration handler to ensure users are deactivated in Salesforce as they are disabled in LDAP.
- B. Configure an authentication provider to delegate authentication to the LDAP directory.
- C. use a login flow to make a callout to the LDAP directory before authenticating the user to Salesforce.
- D. Setup an identity provider (IdP) to authenticate users using LDAP, set up single sign-on to Salesforce and disable Login Form authentication.

**Answer:** B

**Explanation:**

Login History allows administrators to view the login attempts of all users in the org, including the status, source IP, login type, and application. This can help identify and troubleshoot any login errors or issues. References: Login History

**NEW QUESTION 15**

Universal Containers wants Salesforce inbound OAuth-enabled integration clients to use SAML-BASED single Sign-on for authentication. What OAuth flow would be recommended in this scenario?

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

**Answer:** B

**Explanation:**

The SAML assertion OAuth flow allows a connected app to use a SAML assertion to request an OAuth access token to call Salesforce APIs. This flow provides an alternative for orgs that are currently using SAML to access Salesforce and want to access the web services API in the same way. This flow can be used for inbound OAuth-enabled integration clients that want to use SAML-based single sign-on for authentication.

References: OAuth 2.0 SAML Bearer Assertion Flow for Previously Authorized Apps, Access Data with AP Integration, Error 'Invalid assertion' in OAuth 2.0 SAML Bearer Flow



**NEW QUESTION 16**

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 18**

Universal Containers (UC) uses a home-grown Employee portal for their employees to collaborate. UC decides to use Salesforce Ideas to allow employees to post Ideas from the Employee portal. When users click on some of the links in the Employee portal, the users should be redirected to Salesforce, authenticated, and presented with the relevant pages. What OAuth flow is best suited for this scenario?

- A. Web Application flow
- B. SAML Bearer Assertion flow
- C. User-Agent flow
- D. Web Server flow

**Answer: D**

**Explanation:**

The best OAuth flow for this scenario is the web server flow. The web server flow is an OAuth authorization flow that allows a web application, such as UC's employee portal, to obtain an access token and a refresh token from Salesforce after the user grants permission. The web application can then use the access token to access Salesforce data and features, such as posting ideas, and use the refresh token to obtain a new access token when the previous one expires or becomes invalid. This flow is suitable for UC's scenario because it allows users to be redirected to Salesforce, authenticated, and presented with the relevant pages when they click on some of the links in the employee portal. This flow also provides a secure and seamless user experience by using a confidential client secret that is stored on the web server and not exposed to the browser.

The other options are not valid OAuth flows for this scenario. The web application flow is not a standard term for OAuth, but it could refer to the user-agent flow, which is an OAuth authorization flow that allows a browser or web-view, such as a mobile app or a desktop app, to obtain an access token from Salesforce by using a script or a pop-up window. This flow is not suitable for UC's scenario, as it does not use a web server or a client secret, and it does not provide a refresh token. The SAML bearer assertion flow is an OAuth authorization flow that allows an external application to obtain an access token from Salesforce by using a SAML assertion from an identity provider (IdP) that verifies the user's identity. This flow is not suitable for UC's scenario, as it does not involve user interaction or redirection to Salesforce. The user-agent flow is an OAuth authorization flow that allows a browser or web-view, such as a mobile app or a desktop app, to obtain an access token from Salesforce by using a script or a pop-up window. This flow is not suitable for UC's scenario, as it does not use a web server or a client secret, and it does not provide a refresh token. References: [OAuth Authorization Flows], [OAuth 2.0 Web Server Flow for Web App Integration], [OAuth 2.0 User-Agent Flow for Desktop Apps], [OAuth 2.0 SAML Bearer Assertion Flow for Server-to-Server Integration]

**NEW QUESTION 23**

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. Configure Registration for Communities to use a custom Visualforce Page.
- B. Modify the SelfRegistration trigger to assign Profile and Account.
- C. Modify the CommunitiesSelfRegController to assign the Profile and Account.
- D. Configure Registration for Communities to use a custom Apex Controller.

**Answer: CD**

**Explanation:**

To enable self-registration for partner community users, UC should modify the CommunitiesSelfRegController class to assign the Profile and Account values based on the custom data elements captured from the partner user. UC should also configure Registration for Communities to use a custom Apex controller that extends the CommunitiesSelfRegController class and overrides the default registration logic.

References:

➤ [Customize Self-Registration](#)

**NEW QUESTION 24**

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 27**

Which two capabilities does My Domain enable in the context of a SAML SSO configuration? Choose 2 answers

- A. App Launcher
- B. Resource deep linking
- C. SSO from Salesforce Mobile App
- D. Login Forensics

**Answer:** BC

**Explanation:**

These are two capabilities that My Domain enables in the context of a SAML SSO configuration. My Domain is a feature that lets you customize your Salesforce domain name and login page<sup>1</sup>. Resource deep linking is the ability to access a specific page or resource within Salesforce directly from a link, without having to navigate through the app<sup>2</sup>. SSO from Salesforce Mobile App is the ability to log in to the Salesforce Mobile App using your SSO credentials, without having to enter your username and password<sup>3</sup>. My Domain enables these capabilities by allowing you to specify your identity provider (IdP) and SSO settings for your unique domain name, and by providing a custom login URL that can be used for deep linking and mobile app login<sup>1</sup>. The other options are not correct for this question because:

➤ App Launcher is a feature that lets you access all your connected apps from one place in Salesforce. It does not require My Domain or SAML SSO to work, although it can be enhanced by using them.

➤ Login Forensics is a feature that analyzes login behavior and identifies anomalous or suspicious logins.

It does not require My Domain or SAML SSO to work, although it can be used with them.

References: My Domain, Deep Linking into Salesforce, Salesforce Mobile App Basics, [App Launc [Login Forensics]

**NEW QUESTION 31**

Which two are valid choices for digital certificates when setting up two-way SSL between Salesforce and an external system. Choose 2 answers

- A. Use a trusted CA-signed certificate for salesforce and a trusted CA-signed cert for the external system
- B. Use a trusted CA-signed certificate for salesforce and a self-signed cert for the external system
- C. Use a self-signed certificate for salesforce and a self-signed cert for the external system
- D. Use a self-signed certificate for salesforce and a trusted CA-signed cert for the external system

**Answer:** CD

**Explanation:**

Two-way SSL is a method of mutual authentication between two parties using digital certificates. A digital certificate is an electronic document that contains information about the identity of the certificate owner and a public key that can be used to verify their signature. A digital certificate can be either self-signed or CA-signed. A self-signed certificate is created and signed by its owner, while a CA-signed certificate is created by its owner but signed by a trusted Certificate Authority (CA). For setting up two-way SSL between Salesforce and an external system, two valid choices for digital certificates are:

➤ Use a self-signed certificate for Salesforce and a self-signed certificate for the external system. This option is simple and cost-effective, but requires both parties to trust each other's self-signed certificates explicitly.

➤ Use a self-signed certificate for Salesforce and a trusted CA-signed certificate for the external system.

This option is more secure and reliable, but requires Salesforce to trust the CA that signed the external system's certificate implicitly.

References: Know more about all the SSL certificates that are supported by Salesforce, two way ssl. How to

**NEW QUESTION 36**

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 37**

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

- A. Entity id
- B. Issuer
- C. Identity provider login URL
- D. SAML identity location

**Answer:** A

**Explanation:**

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

**NEW QUESTION 38**

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 43**

Northern Trail Outfitters (NTO) wants to improve its engagement with existing customers to boost customer loyalty. To get a better understanding of its customers, NTO establishes a single customer view including their buying behaviors, channel preferences and purchasing history. All of this information exists but is spread across different systems and formats.

NTO has decided to use Salesforce as the platform to build a 360 degree view. The company already uses Microsoft Active Directory (AD) to manage its users and company assets.

What should an Identity Architect do to provision, deprovision and authenticate users?

- A. Salesforce Identity is not needed since NTO uses Microsoft AD.
- B. Salesforce Identity can be included but NTO will be required to build a custom integration with Microsoft AD.
- C. Salesforce Identity is included in the Salesforce licenses so it does not need to be considered separately.
- D. A Salesforce Identity can be included but NTO will require Identity Connect.

**Answer:** D

**Explanation:**

Identity Connect is a Salesforce product that integrates Microsoft Active Directory with Salesforce user records. It allows provisioning, deprovisioning, and authentication of users based on AD data. The other options are either incorrect or irrelevant for this use case. References: Get to Know Identity Connect, Identit Connect

**NEW QUESTION 44**

Universal containers (UC) wants users to authenticate into their salesforce org using credentials stored in a custom identity store. UC does not want to purchase or use a third-party Identity provider. Additionally, UC is extremely wary of social media and does not consider it to be trust worthy. Which two options should an architect recommend to UC? Choose 2 answers

- A. Use a professional social media such as LinkedIn as an Authentication provider
- B. Build a custom web page that uses the identity store and calls frontdoor.jsp
- C. Build a custom Web service that is supported by Delegated Authentication.
- D. Implement the Openid protocol and configure an authentication provider

**Answer:** CD

**Explanation:**

The two options that an architect should recommend to UC are to build a custom web service that is supported by delegated authentication and to implement the OpenID protocol and configure an authentication provider. Delegated authentication is a feature that allows Salesforce to delegate user authentication to an external service instead of using Salesforce credentials<sup>3</sup>. A custom web service can be built to use the credentials stored in the custom identity store and validate them against Salesforce using SOAP or REST API<sup>3</sup>. OpenID is an open standard protocol that allows users to authenticate with various web services using an existing account<sup>4</sup>. An authentication provider can be configured in Salesforce to use OpenID and connect with the custom identity store<sup>5</sup>.

References: Delegated Authentication, OpenID, Authentication Providers



**NEW QUESTION 48**

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

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

**Answer:** D

**Explanation:**

Using custom login flows to connect to the existing custom 2fa system for use in salesforce is the recommended solution because it allows you to leverage your existing 2fa infrastructure and provide a consistent user experience across your applications. Custom login flows let you customize the authentication process by adding extra screens or logic before or after the standard 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 Authentic

**NEW QUESTION 53**

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 58**

What are three capabilities of Delegated Authentication? Choose 3 answers

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

**Answer:** BCE

**Explanation:**

The three capabilities of delegated authentication are:

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

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

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

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

**NEW QUESTION 63**

Universal Containers has multiple Salesforce instances where users receive emails from different instances. Users should be logged into the correct Salesforce instance authenticated by their IdP when clicking on an email link to a Salesforce record.

What should be enabled in Salesforce as a prerequisite?

- A. My Domain
- B. External Identity
- C. Identity Provider
- D. Multi-Factor Authentication

**Answer:** A

**Explanation:**

My Domain is a feature that allows you to personalize your Salesforce org with a subdomain within the Salesforce domain. For example, instead of using a generic URL like <https://na30.salesforce.com>, you can use a custom URL like <https://somethingReallycool.my.salesforce.com><sup>10</sup>. My Domain should be enabled in



Salesforce as a prerequisite for the following reasons:

- My Domain lets you work in multiple Salesforce orgs in the same browser. Without My Domain, you can only log in to one org at a time in the same browser.
- My Domain lets you set up single sign-on (SSO) with third-party identity providers (IdPs). SSO is an authentication method that allows users to access multiple applications with one login and one set of credentials. With My Domain and SSO, users can log in to Salesforce using their corporate credentials or social accounts.
- My Domain lets you customize your login page with your brand. You can add your logo, background image, right-frame content, and authentication service buttons to your login page.

References:

- My Domain
- [Customize Your Login Process with My Domain]

#### NEW QUESTION 64

Universal Container's (UC) is using Salesforce Experience Cloud site for its container wholesale business. The identity architect wants to an authentication provider for the new site.

Which two options should be utilized in creating an authentication provider? Choose 2 answers

- A. A custom registration handler can be set.
- B. A custom error URL can be set.
- C. The default login user can be set.
- D. The default authentication provider certificate can be set.

**Answer:** AB

#### Explanation:

An authentication provider is a configuration that allows users to log in to Salesforce using an external identity provider, such as Facebook, Google, or a custom one. When creating an authentication provider, two options that can be utilized are:

- A custom registration handler, which 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.
- A custom error URL, which is a URL that users are redirected to when an error occurs during the authentication process. References: Authentication Providers, Create an Authentication Provider

#### NEW QUESTION 69

Which two security risks can be mitigated by enabling Two-Factor Authentication (2FA) in Salesforce? Choose 2 answers

- A. Users leaving laptops unattended and not logging out of Salesforce.
- B. Users accessing Salesforce from a public Wi-Fi access point.
- C. Users choosing passwords that are the same as their Facebook password.
- D. Users creating simple-to-guess password reset questions.

**Answer:** BC

#### Explanation:

Enabling Two-Factor Authentication (2FA) in Salesforce can mitigate the security risks of users accessing Salesforce from a public Wi-Fi access point or choosing passwords that are the same as their Facebook password. 2FA is an additional layer of protection beyond your password that requires users to verify their identity with another factor, such as a mobile app, a security key, or a verification code. This can prevent unauthorized access even if the user's password is compromised or guessed by a malicious actor. The other options are not directly related to 2FA, but rather to user behavior or password policies.

#### NEW QUESTION 72

A company with 15,000 employees is using Salesforce and would like to take the necessary steps to highlight or curb fraudulent activity.

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 Forensics
- B. Login Report
- C. Login Inspector
- D. Login History

**Answer:** A

#### Explanation:

To track login data and highlight or curb fraudulent activity, the identity architect should use Login Forensics. Login Forensics is a tool that analyzes login history data and provides insights into user login patterns, such as average number of logins, login outliers, login anomalies, and login risk scores. Login Forensics can help identify suspicious or malicious login attempts and take preventive actions. References: Login Forensics, Login Forensics Implementation Guide

#### NEW QUESTION 73

Northern Trail Outfitters (NTO) is setting up Salesforce to authenticate users with an external identity provider. The NTO Salesforce Administrator is having trouble getting things setup.

What should an identity architect use to show which part of the login assertion is fading?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 78**

Universal Containers wants to allow its customers to log in to its Experience Cloud via a third-party authentication provider that supports only the OAuth protocol. What should an identity architect do to fulfill this requirement?

- A. Contact Salesforce Support and enable delegate single sign-on.
- B. Create a custom external authentication provider.
- C. Use certificate-based authentication.
- D. Configure OpenID Connect authentication provider.

**Answer: B**

**Explanation:**

If the third-party authentication provider supports only the OAuth protocol and not OpenID Connect, then an identity architect needs to create a custom external authentication provider for it. A custom external authentication provider is a configuration that allows users to log in to Salesforce using an external identity provider that is not predefined by Salesforce. It requires implementing the Auth.AuthProviderPlugin interface and defining the OAuth endpoints and parameters.

References: Custom External Authentication Providers, Create a Custom Authentication Provider

**NEW QUESTION 83**

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

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

**Answer: C**

**Explanation:**

The default client certificate or the certificate from the Certificate and Key Management menu is sent along with the outbound message. When sending outbound messages, Salesforce will present the CA-signed or self-signed certificate configured under Setup | Security Controls | Certificate and Key Management | API Client Certificate1. The default client certificate is a self-signed certificate that Salesforce generates for you when you enable outbound messages2. You can also create your own self-signed or CA-signed certificates and upload them to the Certificate and Key Management menu3. The certificate from the Develop | API menu is not used for outbound messages, but for SOAP API clients that need to authenticate with Salesforce4. References: 1: Know more about all the SSL certificates that are supported by Salesforce 2: Setting Up Outbound Messaging 3: Create a Self-Signed Certificate 4: [Generate or Regenerate a Client Certificate]

**NEW QUESTION 86**

The executive sponsor for an organization has asked if Salesforce supports the ability to embed a login widget into its service providers in order to create a more seamless user experience.

What should be used and considered before recommending it as a solution on the Salesforce Platform?

- A. OpenID Connect Web Server Flo
- B. Determine if the service provider is secure enough to store the client secret on.
- C. Embedded Logi
- D. Identify what level of UI customization will be required to make it match the service providers look and feel.
- E. Salesforce REST api
- F. Ensure that Secure Sockets Layer (SSL) connection for the integration is used.
- G. Embedded Logi
- H. Consider whether or not it relies on third party cookies which can cause browser compatibility issues.

**Answer: D**

**Explanation:**

Embedded Login is a feature that allows Salesforce to embed a login widget into any web page, such as a service provider's site, to enable users to log in with their Salesforce credentials. However, Embedded Login relies on third-party cookies, which can cause browser compatibility issues and require users to adjust their browser settings. Therefore, this should be considered before recommending it as a solution on the Salesforce Platform. References: Embedded Login, Embedded Login Implementation Guide

**NEW QUESTION 88**

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

- A. As part of the body of a Salesforce Knowledge article.
- B. In the mobile navigation menu on Salesforce for Android.
- C. The sidebar of a Salesforce Console as a console component.
- D. Included in the Call Control Tool that's part of Open CTI.

**Answer: CD**

**Explanation:**

The sidebar of a Salesforce Console as a console component and included in the Call Control Tool that's part of Open CTI are two options that are correct in

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

**NEW QUESTION 92**

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 95**

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 100**

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:**

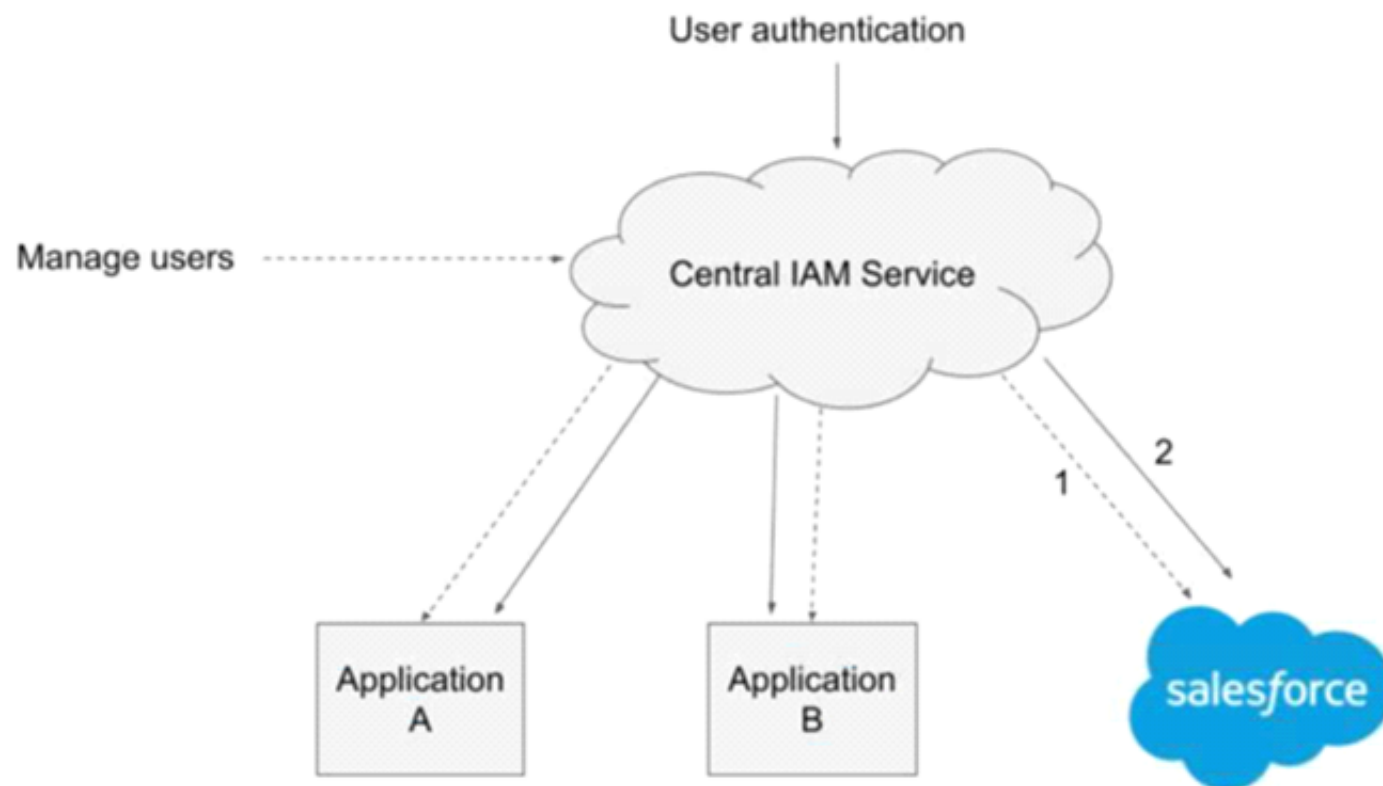
The Entity Id is the SAML SSO setting in Salesforce that provides the capability to differentiate Salesforce from other service providers. The Entity Id is a unique identifier for the service provider that is sent to the identity provider as part of the SSO request<sup>4</sup>. The identity provider 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 101**



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 105**

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 106**

A security architect is rolling out a new multi-factor authentication (MFA) mandate, where all employees must go through a secure authentication process before accessing Salesforce. There are multiple Identity Providers (IdP) in place and the architect is considering how the "Authentication Method Reference" field (AMR) in the Login History can help.

Which two considerations should the architect keep in mind? Choose 2 answers

- A. AMR field shows the authentication methods used at IdP.
- B. Both OIDC and Security Assertion Markup Language (SAML) are supported but AMR must be implemented at IdP.
- C. High-assurance sessions must be configured under Session Security Level Policies.



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

**Answer:** AB

**Explanation:**

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

**NEW QUESTION 110**

Universal containers (UC) built a customer Community for customers to buy products, review orders, and manage their accounts. UC has provided three different options for customers to log in to the customer Community: salesforce, Google, and Facebook. Which two role combinations are represented by the systems in the scenario? Choose 2 answers

- A. Google is the service provider and Facebook is the identity provider
- B. Salesforce is the service provider and Google is the identity provider
- C. Facebook is the service provider and salesforce is the identity provider
- D. Salesforce is the service provider and Facebook is the identity provider

**Answer:** BD

**Explanation:**

The two role combinations that are represented by the systems in the scenario are Salesforce as the service provider and Google as the identity provider, and Salesforce as the service provider and Facebook as the identity provider. This means that Salesforce hosts the customer community app and relies on Google or Facebook to authenticate the users who log in with those options<sup>4</sup>. Therefore, option B and D are the correct answers.  
References: Salesforce as Service Provider and Identity Provider for SSO

**NEW QUESTION 113**

After a recent audit, universal containers was advised to implement Two-factor Authentication for all of their critical systems, including salesforce. Which two actions should UC consider to meet this requirement? Choose 2 answers

- A. Require users to provide their RSA token along with their credentials.
- B. Require users to supply their email and phone number, which gets validated.
- C. Require users to enter a second password after the first Authentication
- D. Require users to use a biometric reader as well as their password

**Answer:** AD

**Explanation:**

A is correct because requiring users to provide their RSA token along with their credentials is a form of two-factor authentication. An RSA token is a hardware device that generates a one-time password (OTP) that changes every few seconds. The user needs to enter both their password and the OTP to log in to Salesforce.  
D is correct because requiring users to use a biometric reader as well as their password is another form of two-factor authentication. A biometric reader is a device that scans a user's fingerprint, face, iris, or other physical characteristics to verify their identity. The user needs to provide both their password and their biometric data to log in to Salesforce.  
B is incorrect because requiring users to supply their email and phone number, which gets validated, is not a form of two-factor authentication. This is a form of identity verification, which is used to confirm that the user owns the email and phone number they provided. However, this does not add an extra layer of protection beyond their password when they log in to Salesforce.  
C is incorrect because requiring users to enter a second password after the first authentication is not a form of two-factor authentication. This is a form of single-factor authentication, which only relies on something the user knows (their passwords). This does not increase security against unauthorized account access.  
References: 4: Multi-Factor Authentication - Salesforce 5: Salesforce Multi-Factor Authentication 6: Factor Authentication - Salesforce India 7: Customer 360 | Increase Productivity - Salesforce UK 8: Secu Salesforce Login Using Two-Factor Authentication and Salesforce ...

**NEW QUESTION 114**

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 119**

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 124**

Universal Containers is implementing Salesforce Identity to broker authentication from its enterprise single sign-on (SSO) solution through Salesforce to third party applications using SAML.

What role does Salesforce Identity play in its relationship with the enterprise SSO system?

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 125**

Universal Containers (UC) is using Active Directory as its corporate identity provider and Salesforce as its CRM for customer care agents, who use SAML based sign sign-on to login to Salesforce. The default agent profile does not include the Manage User permission. UC wants to dynamically update the agent role and permission sets.

Which two mechanisms are used to provision agents with the appropriate permissions? Choose 2 answers

- A. Use Login Flow in User Context to update role and permission sets.
- B. Use Login Flow in System Context to update role and permission sets.
- C. Use SAML Just-in-Time (JIT) Handler class run as current user to update role and permission sets.
- D. Use SAML Just-in-Time (JIT) handler class run as an admin user to update role and permission sets.

**Answer: BD**

**Explanation:**

To dynamically update the agent role and permission sets using Active Directory as the corporate identity provider and Salesforce as the CRM for customer care agents, who use SAML based sign-on to login to Salesforce, the identity architect should use two mechanisms:

- Use Login Flow in System Context to update role and permission sets. 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 System Context is a mode that allows a Login Flow to run as an administrator user with full access to Salesforce data and metadata. By using a Login Flow in System Context, the identity architect can update the agent role and permission sets based on the information from Active Directory or other criteria.
- Use SAML Just-in-Time (JIT) handler class run as an admin user to update role and permission sets. A SAML JIT handler class is a class that implements the Auth.SamlJitHandler interface and 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. By using a SAML JIT handler class run as an admin user, the identity architect can update the agent role and permission sets based on the information from the SAML assertion. References: Login Flows, SAML Just-in-Time Provisioning, Auth.SamlJitHandler Interface

**NEW QUESTION 129**

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

- A. Sp-Initiated
- B. IDP-initiated with deep linking
- C. IDP-initiated
- D. Web server flow.

**Answer: A**

**Explanation:**

The type of single sign-on that UC is using is SP-initiated, which means that the service provider (Salesforce) initiates the SSO process by sending a SAML request to the identity provider (PingFederate) when the user navigates to the My Domain URL. Therefore, option A is the correct answer. References: SAML SSO with Salesforce as the Service Provider

**NEW QUESTION 134**

Universal Containers would like its customers to register and log in to a portal built on Salesforce Experience Cloud. Customers should be able to use their Facebook or LinkedIn credentials for ease of use.

Which three steps should an identity architect take to implement social sign-on? Choose 3 answers

- A. Register both Facebook and LinkedIn as connected apps.
- B. Create authentication providers for both Facebook and LinkedIn.

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

**Answer:** BCE

**Explanation:**

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

- Create authentication providers for both Facebook and LinkedIn. Authentication providers are configurations that enable users to authenticate with an external identity provider and access Salesforce resources. Salesforce provides predefined authentication providers for some common identity providers, such as Facebook and LinkedIn, which can be easily configured with minimal customization.
- Check "Facebook" and "LinkedIn" under Login Page Setup. Login Page Setup is a setting that allows administrators to customize the login page for Experience Cloud sites. By checking "Facebook" and "LinkedIn", the identity architect can enable social sign-on buttons for these identity providers on the login page.
- Update the default registration handlers to create and update users. Registration handlers are classes that implement the Auth.RegistrationHandler interface and define how to create or update users in Salesforce based on the information from the external identity provider. The identity architect can update the default registration handlers to link the user's social identity with their Salesforce identity and prevent duplicate accounts. References: Authentication Providers, Social Sign-On with Authentication Providers, Login Page Setup, Create a Custom Registration Handler

**NEW QUESTION 136**

Universal Containers (UC) has an existing Salesforce org configured for SP-Initiated SAML SSO with their Idp. A second Salesforce org is being introduced into the environment and the IT team would like to ensure they can use the same Idp for new org. What action should the IT team take while implementing the second org?

- A. Use the same SAML Identity location as the first org.
- B. Use a different Entity ID than the first org.
- C. Use the same request bindings as the first org.
- D. Use the Salesforce Username as the SAML Identity Type.

**Answer:** B

**Explanation:**

The Entity ID is a unique identifier for a service provider or an identity provider in SAML SSO. It is used to differentiate between different service providers or identity providers that may share the same issuer or login URL. In Salesforce, the Entity ID is automatically generated based on the organization ID and can be viewed in the Single Sign-On Settings page<sup>1</sup>. If you have a custom domain set up, you can use [https:// \[customDomain\].my.salesforce.com](https://[customDomain].my.salesforce.com) as the Entity ID<sup>2</sup>. If you want to use the same IdP for two Salesforce orgs, you need to use different Entity IDs for each org, otherwise the IdP will not be able to distinguish them and may send incorrect assertions. You can also use different certificates, issuers, or login URLs for each org, but using different Entity IDs is the simplest and recommended way<sup>3</sup>.

**NEW QUESTION 139**

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 Connect<sup>1</sup>. The Employee portal does not use any of these protocols to integrate with Salesforce, but only uses its API.

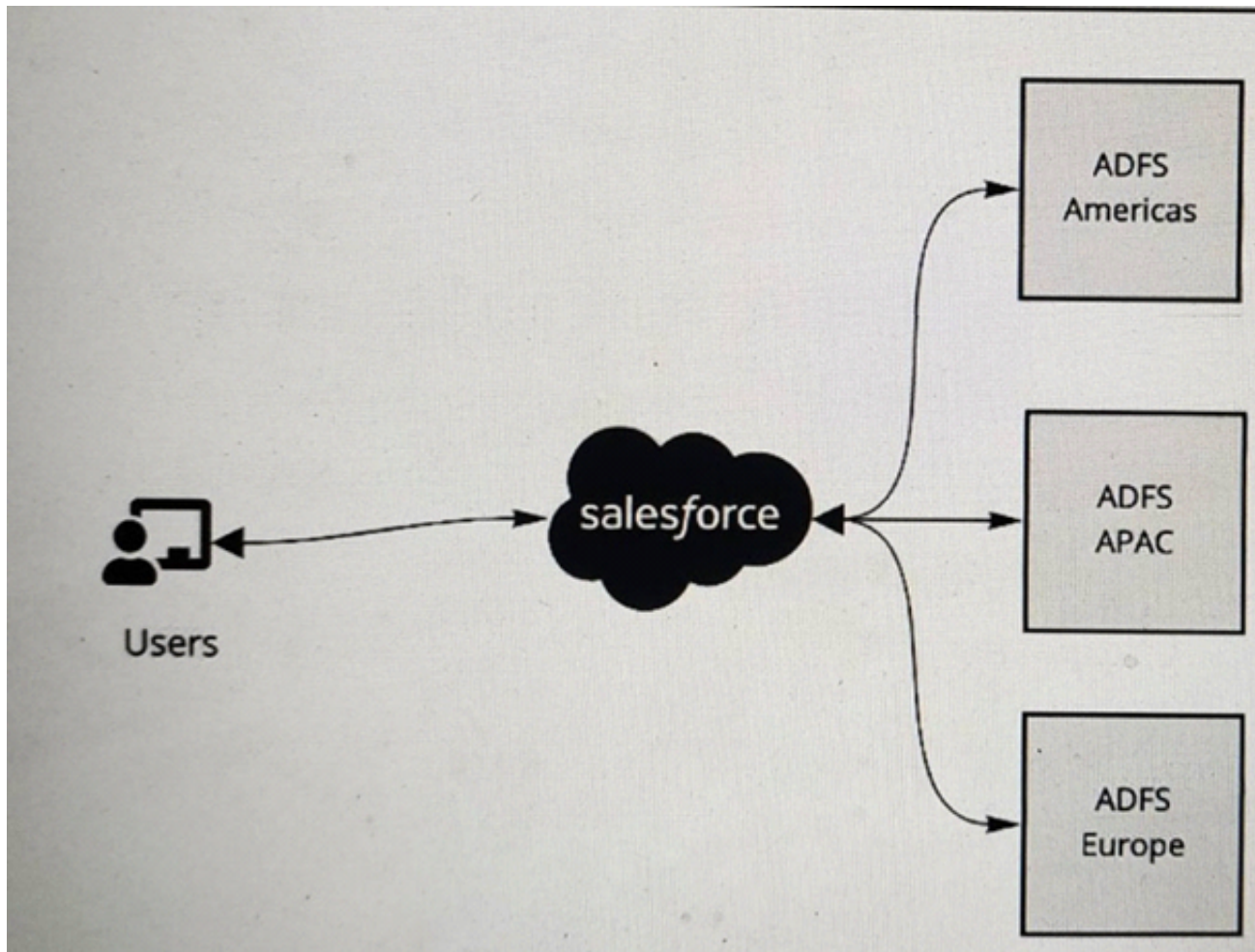
C is incorrect because Salesforce is not an identity provider for the SSO. The IdP is the system that authenticates users and issues tokens or assertions to allow access to other systems. In this scenario, the IdP is Active Directory, not Salesforce.

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

**NEW QUESTION 140**

Refer to the exhibit.





A multinational company is looking to rollout Salesforce globally. The company has a Microsoft Active Directory Federation Services (ADFS) implementation for the Americas, Europe and APAC. The company plans to have a single org and they would like to have all of its users access Salesforce using the ADFS. The company would like to limit its investments and prefer not to procure additional applications to satisfy the requirements. What is recommended to ensure these requirements are met ?

- A. Use connected apps for each ADFS implementation and implement Salesforce site to authenticate users across the ADFS system applicable to their geo.
- B. Implement Identity Connect to provide single sign-on to Salesforce and federate across multiple ADFS systems.
- C. Add a central identity system that federates between the ADFS systems and integrate with Salesforce for single sign-on.
- D. Configure Each ADFS system under single sign-on settings and allow users to choose the system to authenticate during sign on to Salesforce

**Answer: B**

**Explanation:**

To have all of its user's access Salesforce using the ADFS, the multinational company should implement Identity Connect to provide single sign-on to Salesforce and federate across multiple ADFS systems. Identity Connect is a tool that synchronizes user data between Microsoft Active Directory and Salesforce. It allows single sign-on and federation between multiple Active Directory domains and a single Salesforce org. Identity Connect can also handle user provisioning and deprovisioning based on the changes made in Active Directory. The other options are not recommended for this scenario, as they either require additional applications, do not support federation, or do not provide a seamless user experience. References: Identity Connect Implementation Guide, Identity Connect Overview

**NEW QUESTION 145**

Northern Trail Outfitters (NTO) has a requirement to ensure all user logins include a single multi-factor authentication (MFA) prompt. Currently, users are allowed the choice to login with a username and password or via single sign-on against NTO's corporate Identity Provider, which includes built-in MFA. Which configuration will meet this requirement?

- A. Create and assign a permission set to all employees that includes "MFA for User Interface Logins."
- B. Create a custom login flow that enforces MFA and assign it to a permission set
- C. Then assign the permission set to all employees.
- D. Enable "MFA for User Interface Logins" for your organization from Setup -> Identity Verification.
- E. For all employee profiles, set the Session Level Required at Login to High Assurance and add the corporate identity provider to the High Assurance list for the org's Session Security Levels.

**Answer: C**

**Explanation:**

Enabling "MFA for User Interface Logins" for the organization is the simplest way to ensure that all user logins include a single MFA prompt. This setting applies to both direct logins and SSO logins, and overrides any other MFA settings at the profile or permission set level. References: Enable MFA for Direct User Logins, Everything You Need to Know About MFA Auto-Enablement and Enforcement

**NEW QUESTION 150**

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 151**

Northern Trail Outfitters manages application functional permissions centrally as Active Directory groups. The CRM\_SuperUser and CRM\_Reportmg\_SuperUser groups should respectively give the user the SuperUser and Reportmg\_SuperUser permission set in Salesforce. Salesforce is the service provider to a Security Assertion Markup Language (SAML) identity provider.

Now should an identity architect ensure the Active Directory groups are reflected correctly when a user accesses Salesforce?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 155**

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

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

**Answer:** B

**Explanation:**

IDP-initiated SSO flow is when the user starts at the identity provider (IDP) site and then is redirected to the service provider (SP) site with a SAML assertion. This flow is suitable for UC's scenario because they want to use their existing portal as the primary site and also enable seamless access to the partner community. The IDP-initiated flow does not require the user to log in again at the SP site, which is Salesforce in this case.

References: SAML SSO Flows, Single Sign-On, Salesforce Community Single Sign-on (SSO)

**NEW QUESTION 157**

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 159**

Universal Containers (UC) has decided to use Salesforce as an Identity Provider for multiple external applications. UC wants to use the Salesforce App Launcher to control the Apps that are available to individual users. Which three steps are required to make this happen?

- A. Add each connected App to the App Launcher with a Start URL.
- B. Set up an Auth Provider for each External Application.
- C. Set up Salesforce as a SAML IdP with My Domain.
- D. Set up Identity Connect to Synchronize user data.
- E. Create a Connected App for each external application.

**Answer:** ACE

**Explanation:**

These are the steps required to enable Salesforce as a SAML Identity Provider and use the App Launcher to access external applications. According to the Salesforce documentation<sup>1</sup>, you need to:

- Enable Salesforce as a SAML Identity Provider with My Domain<sup>2</sup>.
- Create a Connected App for each external application that you want to integrate with Salesforce<sup>3</sup>.
- Add each Connected App to the App Launcher with a Start URL that points to the external application<sup>1</sup>.

Option B is incorrect because setting up an Auth Provider is not necessary for SAML SSO. Auth Providers are used for OAuth SSO, which is a different protocol<sup>4</sup>.

Option D is incorrect because Identity Connect is a tool for synchronizing user data between Active Directory and Salesforce, which is not related to SSO or App Launcher<sup>5</sup>.

References: 1: App Launcher - Salesforce 2: Enable Salesforce as a SAML Identity Provider 3: Connec Apps Overview 4: Identity Providers and Service Providers - Salesforce 5: Identity Connect Overview

**NEW QUESTION 164**

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 166**

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 170**

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

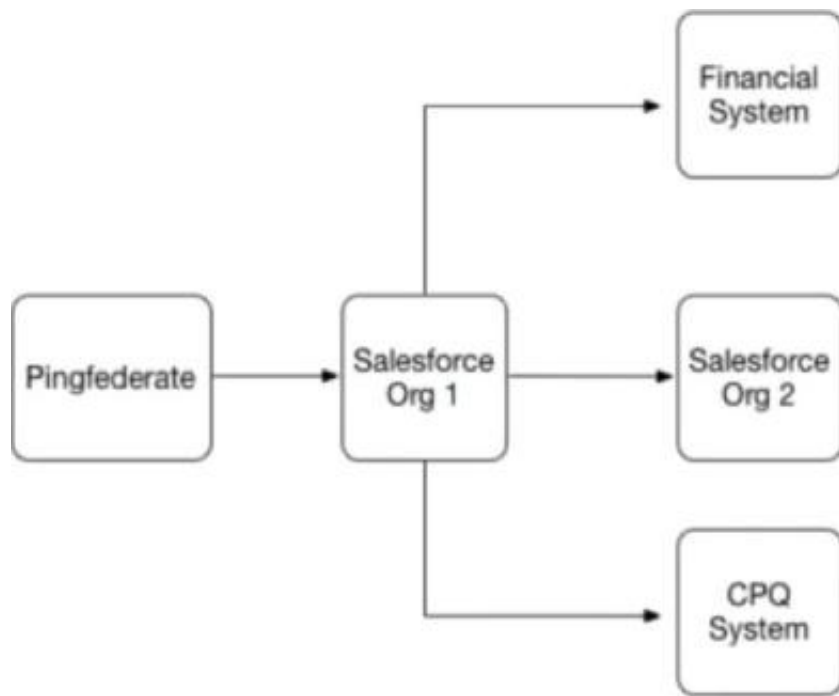
**Explanation:**

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 user<sup>1</sup>. UC should also configure registration for communities to use a custom Visualforce page to capture the custom data elements from the partner user<sup>2</sup>. Therefore, option A and C are the correct answers.

References: Salesforce Partner Community, Partner Community Registration Guide

**NEW QUESTION 173**

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 178**

Universal Containers (UC) is considering a Customer 360 initiative to gain a single source of the truth for its customer data across disparate systems and services. UC wants to understand the primary benefits of Customer 360 Identity and how it contributes to a successful Customer 360 Truth project.

What are two key benefits of Customer 360 Identity as it relates to Customer 360? Choose 2 answers

- A. Customer 360 Identity automatically integrates with Customer 360 Data Manager and Customer 360 Audiences to seamlessly populate all user data.
- B. Customer 360 Identity enables an organization to build a single login for each of its customers, giving the organization an understanding of the user's login activity across all its digital properties and applications.
- C. Customer 360 Identity supports multiple brands so you can deliver centralized identity services and correlation of user activity, even if it spans multiple corporate brands and user experiences.
- D. Customer 360 Identity not only provides a unified sign up and sign in experience, but also tracks anonymous user activity prior to signing up so organizations can understand user activity before and after the users identify themselves.

**Answer: BC**

**Explanation:**

Customer 360 Identity is a cloud-based identity service that provides a single, trusted identity for customers across all your digital properties and applications<sup>2</sup>. Customer 360 Identity has several benefits that relate to Customer 360, such as<sup>3</sup>:

- > Customer 360 Identity enables an organization to build a single login for each of its customers, giving the organization an understanding of the user's login activity across all its digital properties and applications. This helps to create a unified customer profile and deliver personalized experiences based on user preferences and behaviors<sup>3</sup>.
- > Customer 360 Identity supports multiple brands so you can deliver centralized identity services and correlation of user activity, even if it spans multiple corporate brands and user experiences. This helps to maintain brand consistency and loyalty while providing seamless access to your products and services<sup>3</sup>.

References:

- > Customer 360 Identity
- > Customer 360 Identity Benefits

**NEW QUESTION 180**

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

What should an identity architect recommend to meet these requirements?

- A. Configure a predefined authentication provider for Amazon.
- B. Create a custom external authentication provider for Amazon.
- C. Configure an OpenID Connect Authentication Provider for Amazon.
- D. Configure Amazon as a connected app.

**Answer: C**

**Explanation:**



Amazon supports OpenID Connect as an authentication protocol, which allows users to sign in with their Amazon credentials and access Salesforce resources. To enable this, an identity architect needs to configure an OpenID Connect Authentication Provider for Amazon and link it to a connected app. References: OpenID Connect Authentication Providers, Social Sign-On with OpenID Connect

**NEW QUESTION 181**

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

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

Choose 2 answers

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

**Answer:** AC

**Explanation:**

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

**NEW QUESTION 186**

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 188**

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 189**

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



- A. Web Server flow with a Refresh Token.
- B. Mobile Agent flow with a Bearer Token.
- C. User Agent flow with a Refresh Token.
- D. SAML Assertion flow with a Bearer Token.

**Answer:** AC

**Explanation:**

The OAuth 2.0 user-agent flow and the OAuth 2.0 web server flow are both suitable for building a custom mobile app that can access Salesforce data without prompting the user to log in again<sup>1</sup>. Both of these flows use a refresh token that can be used to obtain a new access token when the previous one expires<sup>2</sup>. The user-agent flow uses the Canvas JavaScript SDK to obtain an OAuth token by using the login function in the SDK<sup>2</sup>. The web server flow redirects the user to the Salesforce OAuth authorization endpoint and then obtains an OAuth access token by making a POST request to the Salesforce OAuth token endpoint<sup>2</sup>. The mobile agent flow and the SAML assertion flow are not valid OAuth flows for Salesforce<sup>3</sup>.

References: OAuth Authorization Flows, Mastering Salesforce Canvas Apps, Access Data with API Integration

**NEW QUESTION 192**

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 company's 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 MyDomain 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 196**

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 197**

Universal Containers (UC) would like its community users to be able to register and log in with LinkedIn or Facebook Credentials. UC wants users to clearly see Facebook & LinkedIn Icons when they register and login. What are the two recommended actions UC can take to achieve this Functionality? Choose 2 answers

- A. Enable Facebook and LinkedIn as Login options in the login section of the Community configuration.
- B. Create custom Registration Handlers to link LinkedIn and Facebook accounts to user records.
- C. Store the LinkedIn or Facebook user IDs in the Federation ID field on the Salesforce User record.
- D. Create custom buttons for Facebook and LinkedIn using JavaScript/CSS on a custom Visualforce page.

**Answer:** AB

**Explanation:**

The two recommended actions UC can take to achieve the functionality of allowing community users to register and log in with LinkedIn or Facebook credentials are:

➤ Enable Facebook and LinkedIn as login options in the login section of the community configuration.

This action allows UC to configure Facebook and LinkedIn as authorization providers in Salesforce, which are external services that authenticate users and provide information about their identity and

attributes. By enabling these login options in the community configuration, UC can display Facebook and LinkedIn icons on the community login page and allow users to log in with their existing credentials from these services.

➤ Create custom registration handlers to link LinkedIn and Facebook accounts to user records. This action allows UC to create Apex classes that implement the Auth.RegistrationHandler interface and define the logic for creating or updating user accounts in Salesforce when users log in with LinkedIn or Facebook. By creating custom registration handlers, UC can map the information from the authorization providers to the user fields in Salesforce, such as name, email, profile, or contact.

The other options are not recommended actions for this scenario. Storing the LinkedIn or Facebook user IDs in the Federation ID field on the Salesforce user record is not necessary or sufficient for enabling SSO with these services, as the Federation ID is used for SAML-based SSO, not OAuth-based SSO. Creating custom buttons for Facebook and LinkedIn using JavaScript/CSS on a custom Visualforce page is not advisable, as it would require custom code and UI development, which could increase complexity and maintenance efforts. Moreover, it would not leverage the built-in functionality of authorization providers and registration handlers that Salesforce provides. References: [Authorization Providers], [Enable Social Sign-On for Your Community], [Create a Registration Handler Class], [Auth.RegistrationHandler Interface], [Federation ID]

**NEW QUESTION 199**

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 200**

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

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

**Answer:** A

**Explanation:**

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

References: [Outbound Messages], [Sign Outbound Messages with a Certificate], [CA-Signed Certificates], [Default Client Certificate], [Self-Signed Certificates]

**NEW QUESTION 201**

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

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

**Answer:** ACE

**Explanation:**

AD groups can control public group assignment, role assignment, and permission set assignment through Identity Connect. Identity Connect is a tool that integrates Microsoft Active Directory (AD) user accounts with Salesforce user 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 205**

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

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

**Answer:** D

**Explanation:**

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

References: Salesforce Identity Connect Implementation Guide, Single Sign-On Implementation Guide

**NEW QUESTION 210**

.....

## 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](#)**