



Salesforce

Exam Questions Identity-and-Access-Management-Architect

Salesforce Certified Identity and Access Management Architect (SU23)

NEW QUESTION 1

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

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

Answer: BD

Explanation:

To use SAML SSO for accessing the Salesforce1 mobile app, the architect should recommend configuring the embedded web browser to use the My Domain URL and configuring the Salesforce1 app to use the My Domain URL⁴. Using the My Domain URL allows Salesforce to identify the identity provider and initiate the SSO process⁵. Using the existing SAML SSO flow along with user agent flow or web server flow is not necessary because Salesforce Mobile Applications only work with service provider initiated setups^{4,6}. 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

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 certificates⁷. SSL (Secure Sockets Layer) is a protocol that provides secure communication over the Internet using encryption and certificates⁸. 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 3

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

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

Answer: CD

Explanation:

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

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

➤ OAuth JWT Bearer Token Flow, which allows the client app to use a JSON Web Token (JWT) signed by a private key to request an access token from Salesforce. This flow does not require any user interaction or consent, and uses a certificate to verify the identity of the client app.

Verified References: [OAuth 2.0 SAML Bearer Assertion Flow for Server-to-Server Integration], [OAuth 2.0 JWT Bearer Token Flow for Server-to-Server Integration]

NEW QUESTION 4

Northern Trail Outfitters (NTO) uses Salesforce for Sales Opportunity Management. Okta was recently brought in to Just-in-Time (JIT) provision and authenticate NTO users to applications. Salesforce users also use Okta to authorize a Forecasting web application to access Salesforce records on their behalf. Which two roles are being performed by Salesforce? Choose 2 answers

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

Answer: BD

Explanation:

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

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

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

NEW QUESTION 5

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

- A. Configure SSO to use the third-party portal as an identity provider.
- B. Create a custom external authentication provider.
- C. Add the third-party portal as a connected app.
- D. Configure Salesforce for Delegated Authentication.

Answer: A

Explanation:

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

NEW QUESTION 6

Which two considerations should be made when implementing Delegated Authentication? Choose 2 answers

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

Answer: BE

Explanation:

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

- The authentication web service can include custom attributes, such as user roles or permissions, in the response to Salesforce. These attributes can be used to update user records or trigger workflows in Salesforce².
- Delegated authentication can be used to authenticate API clients and mobile apps that use the SOAP API or REST API login() methods. However, it does not support OAuth 2.0 flows or other authentication methods².
- Delegated authentication does not require trusted IP ranges at the User Profile level. However, you can use them to restrict access to Salesforce from specific IP addresses or ranges².
- Salesforce servers receive but do not validate a user's credentials. Instead, they pass the credentials to the external authentication service, which validates them and returns a response to Salesforce².
- Just-in-time provisioning can be configured for new users who log in with delegated authentication. This feature allows Salesforce to create or update user accounts based on the information provided by the external authentication service³.

References:

- Delegated Authentication
- Delegated Authentication Single Sign-On
- Just-in-Time Provisioning for Delegated Authentication

NEW QUESTION 7

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 8

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

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

Answer: A

Explanation:

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

NEW QUESTION 9

An identity architect has built a native mobile application and plans to integrate it with a Salesforce Identity solution. The following are the requirements for the solution:

- * 1. Users should not have to login every time they use the app.
- * 2. The app should be able to make calls to the Salesforce REST API.
- * 3. End users should NOT see the OAuth approval page.

How should the identity architect configure the Salesforce connected app to meet the requirements?

- A. Enable the API Scope and Offline Access Scope, upload a certificate so JWT Bearer Flow can be used and then set the connected app access settings to "Admin Pre-Approved".
- B. Enable the API Scope and Offline Access Scope on the connected app, and then set the connected app to access settings to 'Admin Pre-Approved'.
- C. Enable the Full Access Scope and then set the connected app access settings to "Admin Pre-Approved".
- D. Enable the API Scope and Offline Access Scope on the connected app, and then set the Connected App access settings to "User may self authorize".

Answer: A

Explanation:

JWT Bearer Flow is an OAuth 2.0 flow that allows a client app to obtain an access token without user interaction. It requires a certificate to sign the JWT and the API and Offline Access scopes to access the Salesforce REST API and refresh the token. The connected app must also be pre-approved by the admin to avoid the OAuth approval page. References: OAuth 2.0 JWT Bearer Flow for Server-to-Server Integration, Authorize an Org Using the JWT Flow

NEW QUESTION 10

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 page¹. 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 app². 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 password³. 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 login¹. 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 10

Universal Containers (UC) uses Salesforce as a CRM and identity provider (IdP) for their Sales Team to seamlessly login to internaJ portals. The IT team at UC is now evaluating Salesforce to act as an IdP for its remaining employees.

Which Salesforce license is required to fulfill this requirement?

- A. External Identity
- B. Identity Verification
- C. Identity Connect
- D. Identity Only

Answer: D

Explanation:

To use Salesforce as an IdP for its remaining employees, the IT team at UC should use the Identity Only license. The Identity Only license is a license type that enables users to access external applications that are integrated with Salesforce using single sign-on (SSO) or delegated authentication, but not access Salesforce objects or data. The other license types are not relevant for this scenario. References: Identity Only License, User Licenses

NEW QUESTION 13

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

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

Answer: A

Explanation:

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

NEW QUESTION 16

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 credentials³. 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 API³. OpenID is an open standard protocol that allows users to authenticate with various web services using an existing account⁴. An authentication provider can be configured in Salesforce to use OpenID and connect with the custom identity store⁵.

References: Delegated Authentication, OpenID, Authentication Providers

NEW QUESTION 21

Sales users at Universal containers use salesforce for Opportunity management. Marketing uses a third-party application called Nest for Lead nurturing that is accessed using username/password. The VP of sales wants to open up access to nest for all sales users to provide them access to lead history and would like SSO for better adoption. Salesforce is already setup for SSO and uses Delegated Authentication. Nest can accept username/Password or SAML-based Authentication. IT teams have received multiple password-related issues for nest and have decided to set up SSO access for Nest for Marketing users as well. The CIO does not want to invest in a new IDP solution and is considering using Salesforce for this purpose. Which are appropriate license type choices for sales and marketing users, giving salesforce is using Delegated Authentication? Choose 2 answers

- A. Salesforce license for sales users and Identity license for Marketing users
- B. Salesforce license for sales users and External Identity license for Marketing users
- C. Identity license for sales users and Identity connect license for Marketing users
- D. Salesforce license for sales users and platform license for Marketing users.

Answer: AD

Explanation:

The appropriate license type choices for sales and marketing users, given that Salesforce is using delegated authentication, are:

➤ Salesforce license for sales users. This license type allows internal users, such as employees, to access standard and custom Salesforce objects and features, such as opportunities and reports. This license type also supports delegated authentication, which 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 license type is suitable for sales users who use Salesforce for opportunity management and need to log in with delegated authentication.

➤ Platform license for marketing users. This license type allows internal users to access custom Salesforce objects and features, such as custom apps and tabs. This license type also supports delegated authentication and single sign-on (SSO), which are features that allow users to log in with an external identity provider (IdP) or service provider (SP). This license type is suitable for marketing users who use a third-party application called Nest for lead nurturing and need to log in with SSO using Salesforce as the IdP or SP.

The other options are not appropriate license types for this scenario. Identity license for sales or marketing users would not allow them to access standard or custom Salesforce objects and features, as this license type only supports identity features, such as SSO and social sign-on. External Identity license for marketing users would not allow them to access custom Salesforce objects and features, as this license type is designed for external users, such as customers or partners, who access a limited set of standard and custom objects in a community. Identity Connect license for marketing users is not a valid license type, as Identity Connect is a desktop application that integrates Salesforce with Microsoft Active Directory (AD) and enables SSO between the two systems. References: [Salesforce Licenses], [Delegated Authentication], [Platform Licenses], [Single Sign-On], [External Identity Licenses], [Identity Connect]

NEW QUESTION 26

Northern Trail Outfitters would like to use a portal built on Salesforce Experience Cloud for customer self-service. Guests of the portal be able to self-register, but be unable to automatically be assigned to a contact record until verified. External Identity licenses have been purchased for the project. After registered guests complete an onboarding process, a flow will create the appropriate account and contact records for the user. Which three steps should an identity architect follow to implement the outlined requirements? Choose 3 answers

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

Answer: ABE

Explanation:

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

NEW QUESTION 28

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

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

Answer: A

Explanation:

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

NEW QUESTION 30

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 35

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>. 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 37

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

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

Answer: D

NEW QUESTION 39

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

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

Answer: C

Explanation:

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

NEW QUESTION 40

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 45

Universal containers uses an 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 Active Directory. What is the role of Active Directory in this scenario?

- A. Identity store
- B. Authentication store
- C. Identity provider
- D. Service provider

Answer: C

Explanation:

The role of Active Directory in this scenario is an identity provider. An identity provider is an application that authenticates users and provides information about them to service providers⁶. A service provider is an application that provides a service to users and relies on an identity provider for authentication⁶. In this scenario, the employee portal is a service provider that provides collaboration features to employees and relies on Active Directory for authentication. Active Directory is an identity provider that authenticates employees using their corporate credentials and sends information about them to the employee portal⁷. References: Identity Provider Overview, Configure SSO to Salesforce Using Microsoft AD FS as the Identity Provider

NEW QUESTION 48

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 52

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 57

Universal Containers (UC) is rolling out its new Customer Identity and Access Management Solution built on top of its existing Salesforce instance. UC wants to allow customers to login using Facebook, Google, and other social sign-on providers.

How should this functionality be enabled for UC, assuming all social sign-on providers support OpenID Connect?

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

Answer: A

Explanation:

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

NEW QUESTION 61

Northern Trail Outfitters (NTO) is planning to implement a community for its customers using Salesforce Experience Cloud. Customers are not able to self-register. NTO would like to have customers set their own passwords when provided access to the community.

Which two recommendations should an identity architect make to fulfill this requirement? Choose 2 answers

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

Answer: CD

Explanation:

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

NEW QUESTION 62

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

- A. Disallow the use of single Sign-on for any users of the mobile app.
- B. Require high assurance sessions in order to use the connected App
- C. Use Google Authenticator as an additional part of the logical processes.
- D. Set login IP ranges to the internal network for all of the app users profiles.

Answer: BC

Explanation:

High assurance sessions are sessions that require a stronger level of identity verification, such as two-factor authentication or SAML assertions¹. Google Authenticator is an app that generates verification codes on your mobile device that you can use as a second factor of authentication². These measures can help prevent unauthorized access to the connected app by ensuring that the user is who they claim to be and that they have access to their mobile device. Disallowing the use of single sign-on (SSO) for the mobile app is not a recommendation because SSO can provide a seamless and secure user experience across multiple applications³. Setting login IP ranges to the internal network for the app users profiles is not a recommendation because it can limit the mobility and flexibility of the users who are commonly out of the office. References: 1: Session Security Levels 2: Google Authenticator 3: Connected Apps : [Restrict Access by IP Address]

NEW QUESTION 67

An identity architect is setting up an integration between Salesforce and a third-party system. The third-party system needs to authenticate to Salesforce and then make API calls against the REST API.

One of the requirements is that the solution needs to ensure the third party service providers connected app in Salesforce must need for end user interaction and maximizes security.

Which OAuth flow should be used to fulfill the requirement?

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

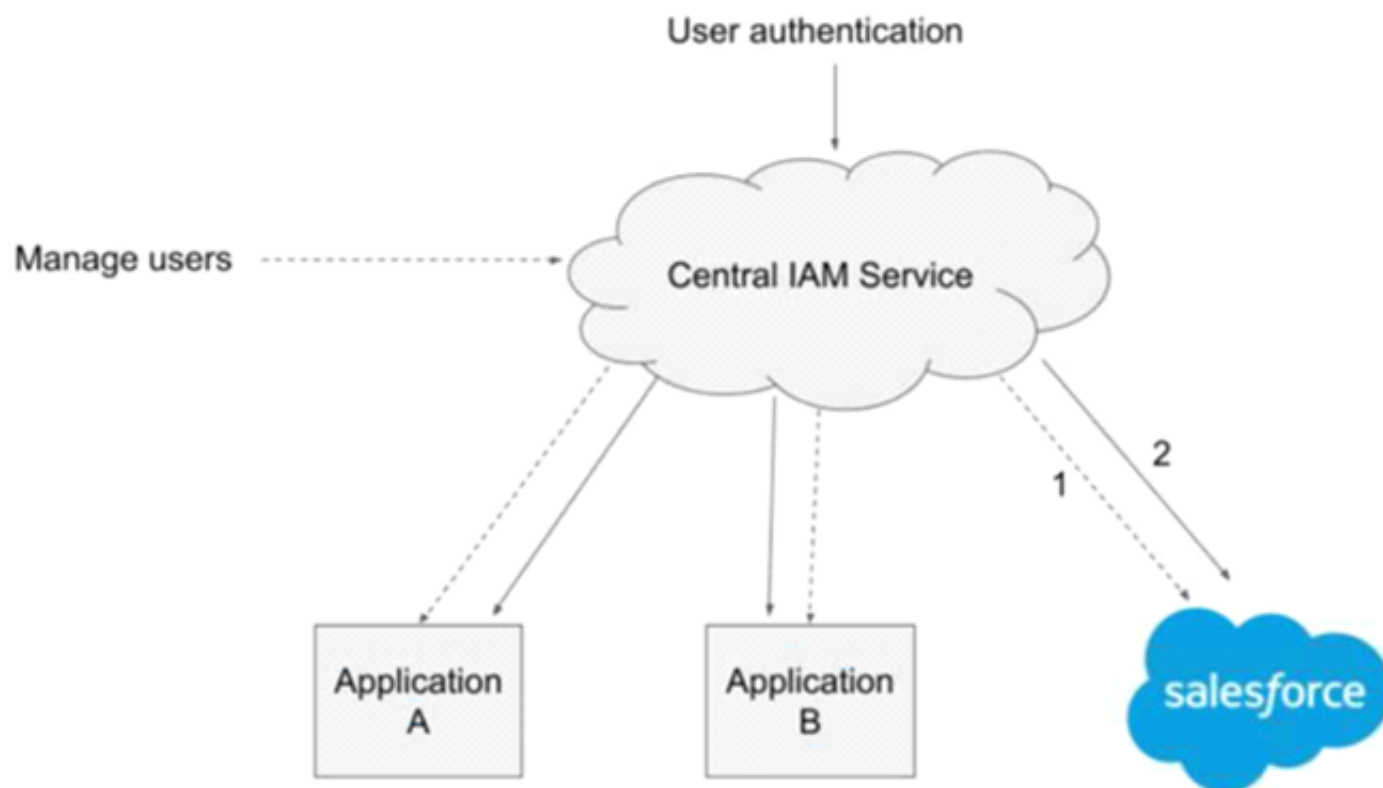
Answer: A

Explanation:

JWT Bearer Flow allows the third-party system to authenticate to Salesforce using a digital certificate and a JSON Web Token (JWT) without any user interaction. It also provides a high level of security as it does not require sharing credentials or storing tokens. References: OAuth 2.0 JWT Bearer Token Flow

NEW QUESTION 71

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 74

Universal Containers (UC) is looking to purchase a third-party application as an Identity Provider. UC is looking to develop a business case for the purchase in general and has enlisted an Architect for advice. Which two capabilities of an Identity Provider should the Architect detail to help strengthen the business case? Choose 2 answers

- A. The Identity Provider can authenticate multiple applications.
- B. The Identity Provider can authenticate multiple social media accounts.
- C. The Identity provider can store credentials for multiple applications.
- D. The Identity Provider can centralize enterprise password policy.

Answer: AD

Explanation:

The two capabilities of an identity provider that the architect should detail to help strengthen the business case are that the identity provider can authenticate multiple applications and that the identity provider can centralize enterprise password policy. These capabilities can provide benefits such as reducing login friction, improving user experience, enhancing security, and simplifying administration. Option B is not a good choice because the identity provider can authenticate multiple social media accounts may not be relevant for UC's business case, as it does not specify how UC will use social media for its identity management. Option C is not a good choice because the identity provider can store credentials for multiple applications may not be desirable or secure for UC's business case, as it may imply that the identity provider is using password vaulting or federation rather than single sign-on (SSO) or identity federation. References: Identity Management Concepts, [Single Sign-On Implementation Guide]

NEW QUESTION 79

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 84

Universal Containers (UC) has an existing web application that it would like to access from Salesforce without requiring users to re-authenticate. The web application is owned UC and the UC team that is responsible for it is willing to add new javascript code and/or libraries to the application. What implementation should an Architect recommend to UC?

- A. Create a Canvas app and use Signed Requests to authenticate the users.
- B. Rewrite the web application as a set of Visualforce pages and Apex code.
- C. Configure the web application as an item in the Salesforce App Launcher.
- D. Add the web application as a ConnectedApp using OAuth User-Agent flow.

Answer: A

Explanation:

A Canvas app is a web application that can be embedded within Salesforce and access Salesforce data using the signed request authentication method. This method allows the Canvas app to receive a signed request that contains the context and OAuth token when it is loaded. The Canvas app can use the SDK to request a new or refreshed signed request on demand². This way, the users do not need to re-authenticate when accessing the web application from Salesforce. References: Requesting a Signed Request, SAML Single Sign-On for Canv Apps, Mastering Salesforce Canvas Apps

NEW QUESTION 85

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 URL³. Therefore, option A is the correct answer. References: SAML SSO with Salesforce as the Service Provider

NEW QUESTION 90

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 94

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 98

Universal Containers (UC) has built a custom time tracking app for its employee. UC wants to leverage Salesforce Identity to control access to the custom app. At a minimum, which Salesforce license is required to support this requirement?

- A. Identity Verification
- B. Identity Connect
- C. Identity Only
- D. External Identity

Answer: C

Explanation:

To use Salesforce Identity to control access to the custom time tracking app, the identity architect should use the Identity Only license. The Identity Only license is a license type that enables users to access external applications that are integrated with Salesforce using single sign-on (SSO) or delegated authentication, but not access Salesforce objects or data. The other license types are not relevant for this scenario. References: Identity Only License, User Licenses

NEW QUESTION 103

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.

How 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 107

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 109

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 112

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

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

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

Answer: BCE

Explanation:

Multi-factor authentication (MFA) is a security feature that requires users to verify their identity with two or more factors when they log in to Salesforce⁴. Salesforce supports several types of authentication and verification methods that meet the criteria for secure MFA, such as⁵:

➤ Username and password + security key: A security key is a physical device that plugs into a USB port or connects wirelessly to your computer or mobile device. It generates a unique code that you use to verify your identity when you log in to Salesforce⁵.

➤ Third-party single sign-on with Mobile Authenticator app: Single sign-on (SSO) is an authentication method that allows users to access multiple applications with one login and one set of credentials. A mobile authenticator app is an app that generates temporary codes or sends push notifications that you use to verify your identity when you log in to Salesforce via SSO⁵.

➤ Lightning Login: Lightning Login is an authentication method that allows users to log in to Salesforce without entering a password. Instead, users scan a QR code with their mobile device or click an email

link that they receive when they try to log in. Then they use their fingerprint, face ID, or PIN to verify their identity on their mobile device⁵.

References:

- Multi-Factor Authentication
- Authentication and Verification Methods

NEW QUESTION 117

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 credentials⁴. There are two types of SSO flows that can be used with Salesforce as the service provider (SP) and an external identity provider (IdP)⁵:

➤ 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 user⁵. This type of SSO flow supports deep linking, which means that the user can access a specific page within Salesforce without logging in again⁶.

➤ 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 user⁵. This type of SSO flow does not support deep linking, which means that the user can only access the default landing page of Salesforce⁶.

References:

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

NEW QUESTION 122

Universal Containers (UC) uses Salesforce for its customer service agents. UC has a proprietary system for order tracking which supports Security Assertion Markup Language (SAML) based single sign-on. The VP of customer service wants to ensure only active Salesforce users should be able to access the order tracking system which is only visible within Salesforce.

What should be done to fulfill the requirement? Choose 2 answers

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

Answer: AD

Explanation:

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

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

➤ Setup order tracking as a Canvas app in Salesforce to POST IdP initiated SAML assertion. A Canvas app is an application that can be embedded within a Salesforce page and interact with Salesforce data and APIs. To set up order tracking as a Canvas app, you need to create a connected app for order tracking in Salesforce, enable SAML and configure the SAML settings, such as the entity ID, ACS URL, and subject type. You also need to enable IdP initiated SAML assertion POST binding for the connected app, which allows Salesforce to initiate the SSO process by sending a SAML assertion to order tracking.

References:

- [SAML Single Sign-On]
- [Set Up Your Domain as an Identity Provider]
- [Canvas Apps]
- [Create a Connected App for Your Canvas App]
- [IdP Initiated SAML Assertion POST Binding]

NEW QUESTION 127

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 130

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 131

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

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

Answer: B

Explanation:

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

NEW QUESTION 135

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

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

Answer: BD

Explanation:

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

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

NEW QUESTION 137

An Identity architect works for a multinational, multi-brand organization. As they work with the organization to understand their Customer Identity and Access Management requirements, the identity architect learns that the brand experience is different for each of the customer's sub-brands and each of these branded experiences must be carried through the login experience depending on which sub-brand the user is logging into.
Which solution should the architect recommend to support scalability and reduce maintenance costs, if the organization has more than 150 sub-brands?

- A. Assign each sub-brand a unique Experience ID and use the Experience ID to dynamically brand the login experience.
- B. Use Audiences to customize the login experience for each sub-brand and pass an audience ID to the community during the OAuth and Security Assertion Markup Language (SAML) flows.
- C. Create a community subdomain for each sub-brand and customize the look and feel of the Login page for each community subdomain to match the brand.
- D. Create a separate Salesforce org for each sub-brand so that each sub-brand has complete control over the user experience.

Answer: A

Explanation:

To support scalability and reduce maintenance costs for a multinational, multi-brand organization, the architect should recommend assigning each sub-brand a unique Experience ID and using the Experience ID to dynamically brand the login experience. Experience ID is a parameter that can be used to identify different brands or experiences within a single Experience Cloud site (formerly known as Community). Dynamic branding is a feature that allows Experience Cloud sites to display different branding elements, such as logos, colors, or images, based on the Experience ID or other criteria. This solution can provide a consistent and personalized brand experience for each sub-brand without creating multiple subdomains or orgs. References: Experience ID, Dynamic Branding for Experience Cloud Sites

NEW QUESTION 139

Containers (UC) has an existing Customer Community. UC wants to expand the self-registration capabilities such that customers receive a different community experience based on the data they provide during the registration process. What is the recommended approach an Architect Should recommend to UC?

- A. Create an After Insert Apex trigger on the user object to assign specific custom permissions.
- B. Create separate login flows corresponding to the different community user personas.
- C. Modify the Community pages to utilize specific fields on the User and Contact records.
- D. Modify the existing Communities registration controller to assign different profiles.

Answer: C

Explanation:

The recommended approach for UC to expand the self-registration capabilities such that customers receive a different community experience based on the data

they provide during the registration process is to modify the community pages to utilize specific fields on the user and contact records. This approach allows UC to customize the community pages based on the user's profile, preferences, interests, or other attributes that are stored in the user or contact fields. For example, UC can use conditional visibility rules or audience criteria to display different components or content based on the user's field values. This approach does not require any code or complex configuration, and it provides a flexible and personalized community experience for different customer segments. The other options are not recommended for this scenario. Creating an after-insert Apex trigger on the user object to assign specific custom permissions would require UC to write code and manage custom permissions, which could increase maintenance and testing efforts. Creating separate login flows corresponding to the different community user personas would require UC to create multiple login pages and logic, which could increase complexity and confusion. Modifying the existing communities' registration controller to assign different profiles would require UC to write code and manage multiple profiles, which could increase security and governance risks. References: [Customize Your Community Pages], [Set Component Visibility], [Create Custom Login Flows], [Customize Self-Registration]

NEW QUESTION 141

An identity architect has been asked to recommend a solution that allows administrators to configure personalized alert messages to users before they land on the Experience Cloud site (formerly known as Community) homepage.

What is recommended to fulfill this requirement with the least amount of customization?

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

Answer: B

Explanation:

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

NEW QUESTION 144

Northern Trail Outfitters want to allow its consumer to self-register on its business-to-consumer (B2C) portal that is built on Experience Cloud. The identity architect has recommended to use Person Accounts.

Which three steps need to be configured to enable self-registration using person accounts? Choose 3 answers

- A. Enable access to person and business account record types under Public Access Settings.
- B. Contact Salesforce Support to enable business accounts.
- C. Under Login and Registration settings, ensure that the default account field is empty.
- D. Contact Salesforce Support to enable person accounts.
- E. Set organization-wide default sharing for Contact to Public Read Only.

Answer: ACD

Explanation:

To enable self-registration using person accounts for consumers on a B2C portal built on Experience Cloud, the identity architect should configure three steps:

- Enable access to person and business account record types under Public Access Settings. Public Access Settings are settings that control the access level and permissions for guest users on Experience Cloud sites. By enabling access to person and business account record types, the identity architect can allow guest users to create person accounts or business accounts when they self-register on the portal.
- Under Login and Registration settings, ensure that the default account field is empty. Login and Registration settings are settings that control the login and registration options for Experience Cloud sites. By ensuring that the default account field is empty, the identity architect can prevent guest users from being associated with a default account when they self-register on the portal.
- Contact Salesforce Support to enable person accounts. Person accounts are a type of account that combines an individual consumer with an account record. Person accounts are not enabled by default in Salesforce orgs and require contacting Salesforce Support to enable them. References: Public Access Settings, Login and Registration Settings, Person Accounts

NEW QUESTION 147

Universal Containers is implementing a new Experience Cloud site and the identity architect wants to use dynamic branding features as of the login process.

Which two options should the identity architect recommend to support dynamic branding for the site? Choose 2 answers

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

Answer: BC

Explanation:

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

References: Dynamic Branding for Experience Cloud Sites, Create a Customer Account Portal

NEW QUESTION 152

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

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

Answer: A

Explanation:

A is correct because creating a connected app that supports the JWT Bearer Token OAuth Flow allows the middleware to authenticate to Salesforce without storing usernames and passwords. The JWT Bearer Token OAuth Flow uses a certificate and a private key to sign a JSON Web Token (JWT) that contains information about the user identity and requested access. The middleware sends the JWT to Salesforce, which verifies it using the certificate and grants an access token².

B is incorrect because creating a connected app that supports the Refresh Token OAuth Flow requires storing usernames and passwords in the middleware. The Refresh Token OAuth Flow uses a username-password authentication flow to obtain an access token and a refresh token. The middleware can use the refresh token to obtain new access tokens without user interaction, but it still needs to store the username and password for the initial authentication³.

C is incorrect because creating a connected app that supports the Web Server OAuth Flow requires user interaction to authenticate to Salesforce. The Web Server OAuth Flow redirects the user to a Salesforce login page, where they enter their credentials and grant access to the middleware. The middleware then receives an authorization code that it can exchange for an access token and a refresh token⁴.

D is incorrect because creating a connected app that supports the User-Agent OAuth Flow also requires user interaction to authenticate to Salesforce. The User-Agent OAuth Flow is similar to the Web Server OAuth Flow, except that it does not return a refresh token. The middleware can only use the access token until it expires⁵.

References: 2: Accessing Salesforce with JWT OAuth Flow 3: OAuth Authorization Flows - Salesforce 4: OAuth Authorization Flows - Salesforce 5: OAuth Authorization Flows - Salesforce

NEW QUESTION 155

What is one of the roles of an Identity Provider in a Single Sign-on setup using SAML?

- A. Validate token
- B. Create token
- C. Consume token
- D. Revoke token

Answer: B

Explanation:

Creating a token is one of the roles of an Identity Provider in a Single Sign-on setup using SAML. SAML is a standard protocol that allows users to access multiple applications with a single login. In SAML, an Identity Provider (IdP) is a system that authenticates users and issues a security token that contains information about the user's identity and permissions. A Service Provider (SP) is a system that consumes the token and grants access to the user based on the token's attributes. The other options are not roles of an IdP, but rather functions of the SAML protocol or the SP.

NEW QUESTION 158

universal container plans to develop a custom mobile app for the sales team that will use salesforce for authentication and access management. The mobile app access needs to be restricted to only the sales team. What would be the recommended solution to grant mobile app access to sales users?

- A. Use a custom attribute on the user object to control access to the mobile app
- B. Use connected apps OAuth policies to restrict mobile app access to authorized users.
- C. Use the permission set license to assign the mobile app permission to sales users
- D. Add a new identity provider to authenticate and authorize mobile users.

Answer: B

Explanation:

The recommended solution to grant mobile app access to sales users is to use connected apps OAuth policies to restrict mobile app access to authorized users. A connected app is a configuration in Salesforce that allows an external application, such as a mobile app, to connect to Salesforce using OAuth. OAuth is a protocol that allows the mobile app to obtain an access token from Salesforce after the user grants permission. The access token can then be used by the mobile app to access Salesforce data and features. OAuth policies are settings that control how users can access a connected app, such as who can use the app, how long the access token is valid, and what level of access the app requests. By configuring OAuth policies in the connected app settings, Universal Containers can restrict the mobile app access to only the sales team and protect against unauthorized or excessive access.

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

NEW QUESTION 162

Users logging into Salesforce are frequently prompted to verify their identity.

The identity architect is required to provide recommendations so that frequency of prompt verification can be reduced.

What should the identity architect recommend to meet the requirement?

- A. Implement 2FA authentication for the Salesforce org.
- B. Set trusted IP ranges for the organization.
- C. Implement a single sign-on for Salesforce using an external identity provider.
- D. Implement multi-factor authentication for the Salesforce org.

Answer: B

Explanation:

To reduce the frequency of prompt verification for users logging into Salesforce, the identity architect should recommend setting trusted IP ranges for the organization. Trusted IP ranges are IP addresses that are considered safe for logging in without any additional verification. Users who log in from trusted IP ranges do not need to activate their computer or use a verification code. Trusted IP ranges can improve user convenience and security. References: Trusted IP Ranges, Set Trusted IP Ranges for Your Organization

NEW QUESTION 165

Northern Trail Outfitters (NTO) has an existing custom business-to-consumer (B2C) website that does NOT support single sign-on standards, such as Security Assertion Markup Language (SAML) or OAuth. NTO wants to use Salesforce Identity to register and authenticate new customers on the website.

Which two Salesforce features should an identity architect use in order to provide username/password authentication for the website? Choose 2 answers

- A. Identity Connect
- B. Delegated Authentication
- C. Connected Apps
- D. Embedded Login

Answer: BD

Explanation:

To register and authenticate new customers on the website using Salesforce Identity, the identity architect should use Delegated Authentication and Embedded Login. Delegated Authentication is a feature that allows Salesforce to delegate the authentication process to an external service, such as a custom website, instead of validating the username and password internally. Embedded Login is a feature that allows Salesforce to embed a login widget into any web page, such as a custom website, to enable users to log in with their Salesforce credentials. The other options are not relevant for this scenario. References: Delegated Authentication, Embedded Login

NEW QUESTION 168

Northern Trail Outfitters (NTO) leverages Microsoft Active Directory (AD) for management of employee usernames, passwords, permissions, and asset access. NTO also owns a third-party single sign-on (SSO) solution. The third-party party SSO solution is used for all corporate applications, including Salesforce. NTO has asked an architect to explore Salesforce Identity Connect for automatic provisioning and deprovisioning of users in Salesforce. What role does identity Connect play in the outlined requirements?

- A. Service Provider
- B. Single Sign-On
- C. Identity Provider
- D. User Management

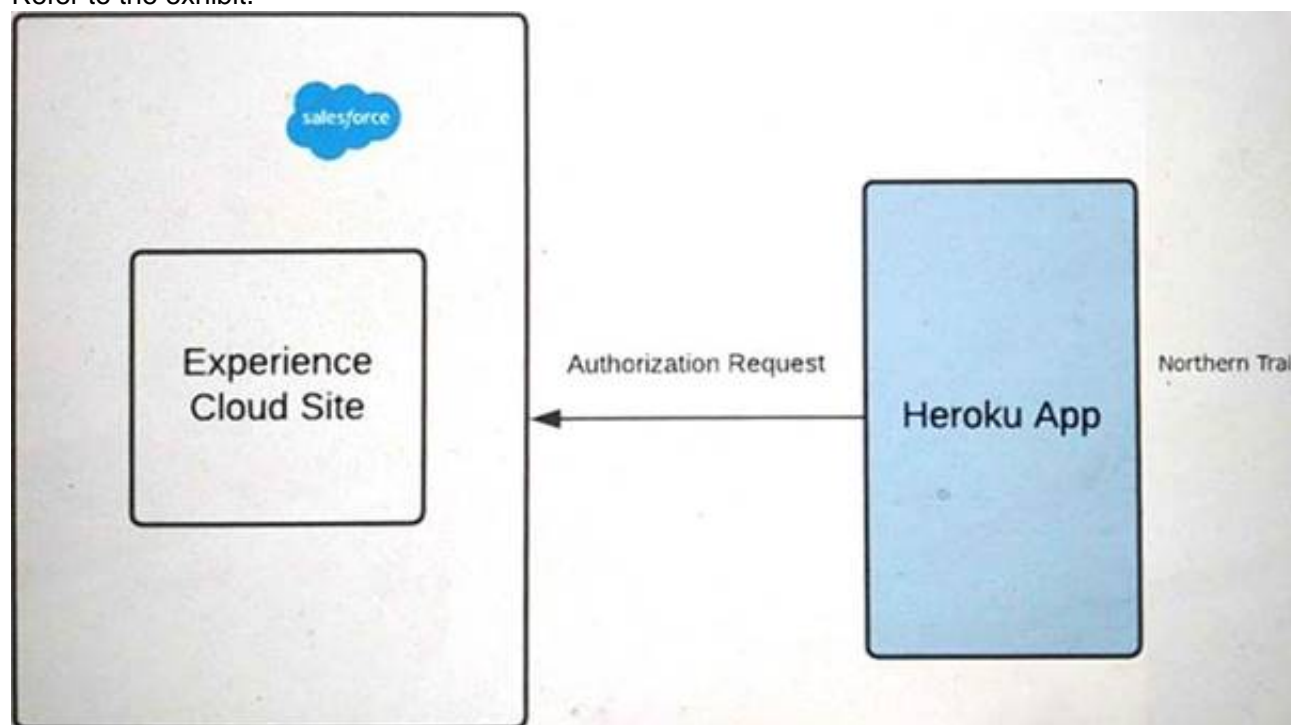
Answer: D

Explanation:

Salesforce Identity Connect is a tool that synchronizes user data between Microsoft Active Directory and Salesforce. It allows automatic provisioning and deprovisioning of users in Salesforce based on the changes made in Active Directory. Therefore, Identity Connect plays the role of user management in the outlined requirements. References: Identity Connect Implementation Guide, Identity Connect Overview

NEW QUESTION 173

Refer to the exhibit.



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

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

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

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

Answer: D

Explanation:

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

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

References:

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

NEW QUESTION 174

Which three are capabilities of SAML-based Federated authentication? Choose 3 answers

- A. Trust relationships between Identity Provider and Service Provider are required.
- B. SAML tokens can be in XML or JSON format and can be used interchangeably.
- C. Web applications with no passwords are more secure and stronger against attacks.
- D. Access tokens are used to access resources on the server once the user is authenticated.
- E. Centralized federation provides single point of access, control and auditing.

Answer: ACE

Explanation:

A is correct because SAML-based Federated authentication requires trust relationships between the IdP and the SP. The IdP issues a SAML assertion that contains information about the user's identity and attributes. The SP validates the assertion and grants access to the user.

C is correct because web applications that use SAML-based Federated authentication do not require passwords for users to log in. Instead, they rely on the IdP to authenticate the users and provide a secure token. This eliminates the risk of password breaches and phishing attacks.

E is correct because centralized federation provides a single point of access, control, and auditing for web applications that use SAML-based Federated authentication. Users can access multiple applications with one login, administrators can manage user access from one place, and auditors can monitor user activity across applications.

B is incorrect because SAML tokens are always in XML format. They cannot be used interchangeably with JSON tokens, which are used by OAuth or OpenID Connect protocols.

D is incorrect because access tokens are not used by SAML-based Federated authentication. Access tokens are used by OAuth or OpenID Connect protocols to access resources on the server once the user is authenticated.

References: : [Single Sign-On Implementation Guide Developer Documentation] : [Identity 101: Design Patterns for Access Management Salesforce Developers YouTube] : Certification - Identity and Access Management Architect - Trailhead : OAuth Authorization Flows Trailblazer Community Documentation : User Authentication Module - Trailhead

NEW QUESTION 179

Northern Trail Outfitters (NTO) uses a Security Assertion Markup Language (SAML)-based Identity Provider (IdP) to authenticate employees to all systems. The IdP authenticates users against a Lightweight Directory Access Protocol (LDAP) directory and has access to user information. NTO wants to minimize Salesforce license usage since only a small percentage of users need Salesforce.

What is recommended to ensure new employees have immediate access to Salesforce using their current IdP?

- A. Install Salesforce Identity Connect to automatically provision new users in Salesforce the first time they attempt to login.
- B. Build an integration that queries LDAP periodically and creates new active users in Salesforce.
- C. Configure Just-in-Time provisioning using SAML attributes to create new Salesforce users as necessary when a new user attempts to login to Salesforce.
- D. Build an integration that queries LDAP and creates new inactive users in Salesforce and use a login flow to activate the user at first login.

Answer: C

Explanation:

Just-in-Time (JIT) provisioning is a feature that allows Salesforce to create or update user records on the fly when users log in through an external identity provider, such as a SAML-based IdP. This eliminates the need for manual or batch user provisioning in Salesforce and minimizes license usage. To use JIT provisioning, the identity architect needs to configure the SAML settings in Salesforce and include the user attributes in the SAML assertion sent by the IdP.

References: Just-in-Time Provisioning for SAML and OpenID Connect, Identity 101: Design Patterns for Access Management

NEW QUESTION 183

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

- A. Use a custom connected App handler using Apex to dynamically allow access to the system based on whether the staff owns any open "classified" cases.
- B. Use Apex trigger on case to dynamically assign permission sets that grant access when a user is assigned with an open "classified" case, and remove it when the case is closed.
- C. Use custom SAML JIT provisioning to dynamically query the user's open "classified" cases when attempting to access the classified information system.
- D. Use Salesforce reports to identify users that currently own open "classified" cases and should be granted access to the classified information system.

Answer: A

Explanation:

Use a custom connected app handler using Apex to dynamically allow access to the system based on whether the staff owns any open "classified" cases is the recommended solution for this scenario. A custom connected app handler is an Apex class that implements the ConnectedAppPlugin interface and can customize the behavior of a connected app. The custom handler can support new protocols or respond to user attributes in a way that benefits a business process. In this case, the custom handler can query the user's open "classified" cases and grant or deny access to the classified information system accordingly. Use Apex trigger on case to dynamically assign permission sets that grant access when a user is assigned with an open "classified" case, and remove it when the case is closed is not a good solution, as permission sets are not related to SSO and cannot control access to external systems. Use custom SAML JIT provisioning to dynamically query the user's open "classified" cases when attempting to access the classified information system is not feasible, as JIT provisioning is used to create or update user records in Salesforce, not in external systems. Use Salesforce reports to identify users that currently own open "classified" cases and

should be granted access to the classified information system is not an automated solution, as it requires manual intervention and does not leverage SSO.
References: Certification - Identity and Access Management Architect - Trailhead, Create a Custom Connected App Handler, Manage Access Through a Custom Connected App Handler

NEW QUESTION 187

Northern Trail Outfitters (NTO) recently purchased Salesforce Identity Connect to streamline user provisioning across Microsoft Active Directory (AD) and Salesforce Sales Cloud.

NTO has asked an identity architect to identify which salesforce security configurations can map to AD permissions.
Which three Salesforce permissions are available to map to AD permissions? Choose 3 answers

- A. Public Groups
- B. Field-Level Security
- C. Roles
- D. Sharing Rules
- E. Profiles and Permission Sets

Answer: ACE

Explanation:

Salesforce Identity Connect can map AD groups to Salesforce public groups, roles, profiles, and permission sets. These permissions control the access and visibility of data and features in Salesforce. References:
Salesforce Identity Connect Implementation Guide

NEW QUESTION 191

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 the updateUser() method on the registration handler class.
- B. Use SAML just-in-time provisioning between Facebook and Salesforce
- C. Use information in the signed request that is received from Facebook.
- D. Develop a schedule job that calls out to Facebook on a nightly basis.

Answer: C

Explanation:

Using information in the signed request that is received from Facebook is how this requirement can be met. A signed request is a parameter that contains information about the user who is logging in with Facebook credentials. The signed request can include information such as the user ID, name, email, and profile picture. You can use this information to update the corresponding customer community user in Salesforce by implementing a registration handler class. The registration handler class is an Apex class that defines how Salesforce handles user registration and authentication when using an auth provider. You can use the updateUser() method in the registration handler class to update the user record with the information from the signed request. Using the updateUser() method on the registration handler class is not how this requirement can be met because it is only part of the solution. You also need to use information from the signed request as the source of the updates. Using SAML just-in-time provisioning between Facebook and Salesforce is not how this requirement can be met because Facebook does not support SAML as an identity provider protocol. Developing a scheduled job that calls out to Facebook on a nightly basis is not how this requirement can be met because it is inefficient and unnecessary. You can update the user record in real time using the signed request instead of waiting for a nightly batch process.

NEW QUESTION 196

which three are features of federated Single Sign-on solutions? Choose 3 answers

- A. It federates credentials control to authorized applications.
- B. It establishes trust between Identity store and service provider.
- C. It solves all identity and access management problems.
- D. It improves affiliated applications adoption rates.
- E. It enables quick and easy provisioning and deactivating of users.

Answer: ABD

Explanation:

- It federates credentials control to authorized applications. This means that users can access multiple applications across different domains or organizations using one set of credentials, without having to share their passwords with each application¹. The applications rely on a trusted identity provider (IdP) to authenticate the users and grant them access.
- It establishes trust between Identity store and service provider. This means that the IdP and the service provider (SP) have a mutual agreement to exchange identity information using standard protocols, such as SAML, OpenID Connect, or OAuth2. The IdP and the SP also share metadata and certificates to ensure secure communication and verification.
- It improves affiliated applications adoption rates. This means that users are more likely to use applications that are connected to their existing identity provider, as they do not have to create or remember multiple passwords³. This also reduces the friction and frustration of logging in to different applications, and enhances the user experience.

The other options are not features of federated single sign-on solutions because:

- It solves all identity and access management problems. This is false, as federated single sign-on solutions only address the authentication aspect of identity and access management, not the authorization, provisioning, governance, or auditing aspects. Federated single sign-on solutions also have some challenges, such as complexity, interoperability, and security risks.
- It enables quick and easy provisioning and deactivating of users. This is not necessarily true, as federated single sign-on solutions do not automatically create or delete user accounts in the service provider applications. Users still need to be provisioned and deprovisioned manually or through other mechanisms, such as just-in-time provisioning or SCIM.

References: Federated Identity Management vs. Single Sign-On: What's the Difference?, What is single sign-on?, Single Sign-On (SSO) Solution, [Identity Management vs. Access Management: What's the Difference?], [Federated Identity Management Challenges], [Just-in-Time Provisioning for SAML], [SCIM User Provisioning]

NEW QUESTION 199

An identity architect's client has a homegrown identity provider (IdP). Salesforce is used as the service provider (SP). The head of IT is worried that during a SP initiated single sign-on (SSO), the Security Assertion Markup Language (SAML) request content will be altered. What should the identity architect recommend to make sure that there is additional trust between the SP and the IdP?

- A. Ensure that there is an HTTPS connection between IDP and SP.
- B. Ensure that on the SSO settings page, the "Request Signing Certificate" field has a self-signed certificate.
- C. Ensure that the Issuer and Assertion Consumer service (ACS) URL is properly configured between SP and IDP.
- D. Encrypt the SAML Request using certification authority (CA) signed certificate and decrypt on IdP.

Answer: D

Explanation:

Encrypting the SAML Request using a CA signed certificate and decrypting it on the IdP ensures that the request content is not altered or tampered with during transit. This also adds an extra layer of security and trust between the SP and the IdP. References: SAML Single Sign-On Overview, SAML Assertion Encryption

NEW QUESTION 200

Universal Containers (UC) is both a Salesforce and Google Apps customer. The UC IT team would like to manage the users for both systems in a single place to reduce administrative burden. Which two optimal ways can the IT team provision users and allow Single Sign-on between Salesforce and Google Apps ? Choose 2 answers

- A. Build a custom app running on Heroku as the Identity Provider that can sync user information between Salesforce and Google Apps.
- B. Use a third-party product as the Identity Provider for both Salesforce and Google Apps and manage the provisioning from there.
- C. Use Identity Connect as the Identity Provider for both Salesforce and Google Apps and manage the provisioning from there.
- D. Use Salesforce as the Identity Provider and Google Apps as a Service Provider and configure UserProvisioning for Connected Apps.

Answer: BD

Explanation:

B is correct because a third-party product can act as an Identity Provider (IdP) for both Salesforce and Google Apps and manage the user provisioning from a single place¹². This reduces the administrative burden and provides a consistent user experience.

D is correct because Salesforce can act as an IdP and Google Apps can act as a Service Provider (SP) and they can use SAML or OpenID Connect for Single Sign-on (SSO)³⁴. Salesforce also supports User Provisioning for Connected Apps, which allows the creation, update, and deactivation of users in Google Apps based on changes in Salesforce.

A is incorrect because building a custom app on Heroku as an IdP is not an optimal way to provision users and allow SSO. It would require more development and maintenance effort than using a third-party product or Salesforce as an IdP.

C is incorrect because Identity Connect is a tool that synchronizes users between Active Directory and Salesforce. It does not support Google Apps as a target system for user provisioning or SSO.

References: 1: Architect Journey: Identity and Access Management Trailmix - Trailhead 2: Free Salesfo Identity-and-Access-Management-Architect Questions ... 3: [Single Sign-On Implementation Guide Developer Documentation] 4: [Social Single Sign-On with OpenID Connect Salesforce Developer YouTube] : [Authorize Apps with OAuth Trailblazer Community Documentation] : Identity Connect Implementation Guide Developer Documentation

NEW QUESTION 202

Which three different attributes can be used to identify the user in a SAML 65> assertion when Salesforce is acting as a Service Provider? Choose 3 answers

- A. Federation ID
- B. Salesforce User ID
- C. User Full Name
- D. User Email Address
- E. Salesforce Username

Answer: ADE

Explanation:

The three different attributes that can be used to identify the user in a SAML assertion when Salesforce is acting as a Service Provider are Federation ID, User Email Address, and Salesforce Username. According to the Salesforce documentation, "Salesforce supports three attributes for identifying users in a SAML assertion: Federation ID, User Email Address, and Salesforce Username." Therefore, option A, D, and E are the correct answers.

References: [SAML Assertion Attributes]

NEW QUESTION 207

Containers (UC) has decided to implement a federated single Sign-on solution using a third-party Idp. In reviewing the third-party products, they would like to ensure the product supports the automated provisioning and deprovisioning of users. What are the underlining mechanisms that the UC Architect must ensure are part of the product?

- A. SOAP API for provisioning; Just-in-Time (JIT) for Deprovisioning.
- B. Just-In-time (JIT) for Provisioning; SOAP API for Deprovisioning.
- C. Provisioning API for both Provisioning and Deprovisioning.
- D. Just-in-Time (JIT) for both Provisioning and Deprovisionin

Answer: D

Explanation:

Just-in-Time (JIT) provisioning and deprovisioning can be used to create, update, or deactivate users in Salesforce based on the information in the SAML assertion sent by the IdP. This way, the user lifecycle can be managed automatically without the need for a separate provisioning API. Reference: [Salesforce Help: Just-in-Time Provisioning for SAML]

NEW QUESTION 208

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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](#)