

Salesforce

Exam Questions Identity-and-Access-Management-Architect

Salesforce Certified Identity and Access Management Architect (SU23)



NEW QUESTION 1

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

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

Answer: D

Explanation:

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

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

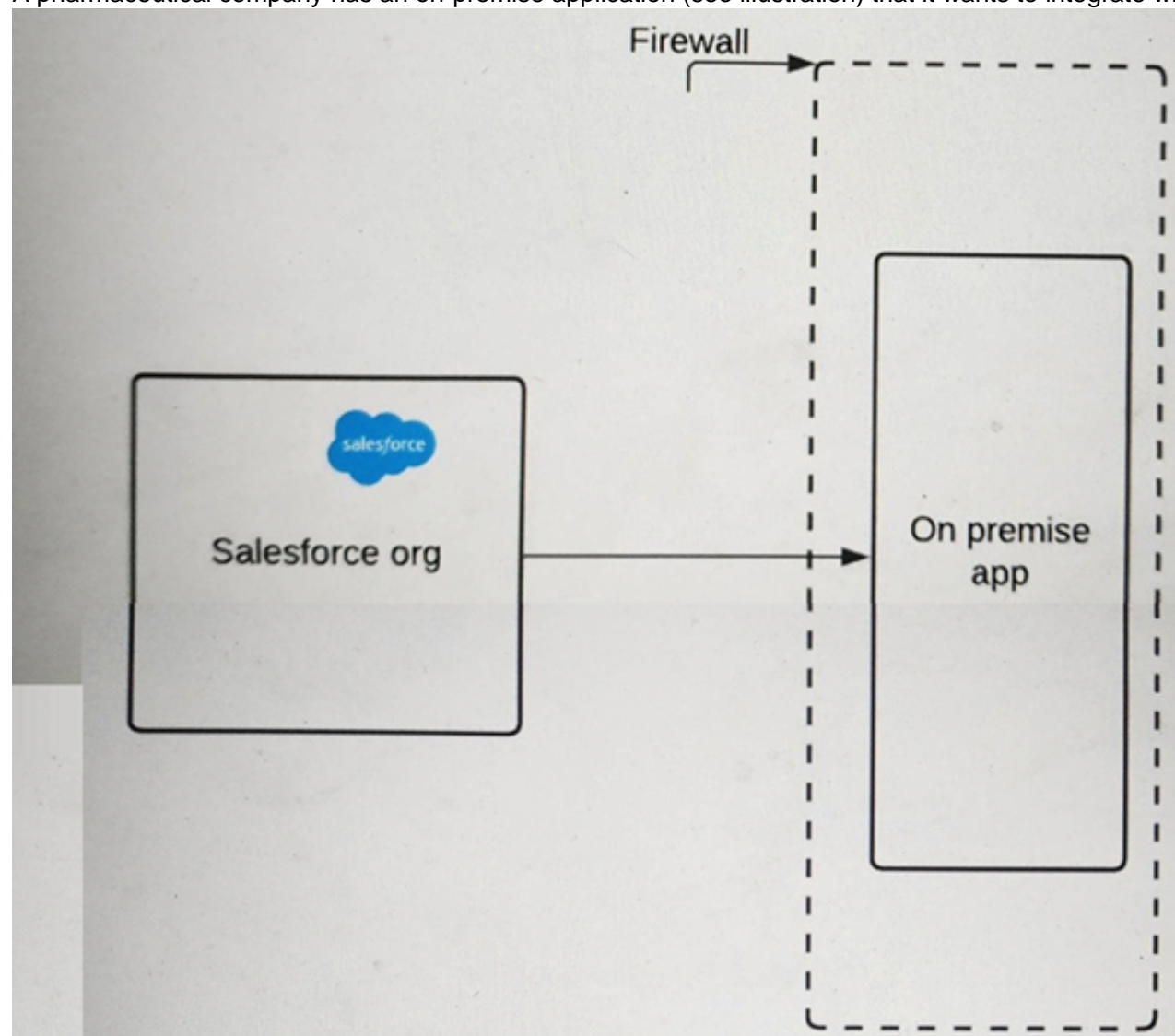
B is incorrect because using a self-signed certificate does not make the trusted party act as the trusted CA (Certificate Authority). The trusted CA is the entity that issues and validates certificates for servers. The trusted party only needs to trust the CA's root certificate, which is usually pre-installed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

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

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

NEW QUESTION 2

A pharmaceutical company has an on-premise application (see illustration) that it wants to integrate with Salesforce.



The IT director wants to ensure that requests must include a certificate with a trusted certificate chain to access the company's on-premise application endpoint. What should an Identity architect do to meet this requirement?

- A. Use open SSL to generate a Self-signed Certificate and upload it to the on-premise app.
- B. Configure the company firewall to allow traffic from Salesforce IP ranges.
- C. Generate a certificate authority-signed certificate in Salesforce and uploading it to the on-premise application Truststore.
- D. Upload a third-party certificate from Salesforce into the on-premise server.

Answer: C

Explanation:

To ensure that requests must include a certificate with a trusted certificate chain to access the company's on-premise application endpoint, the identity architect should generate a certificate authority-signed certificate in Salesforce and upload it to the on-premise application Truststore. A certificate authority-signed certificate is a certificate that is issued by a trusted third-party entity, such as VeriSign or Thawte, that verifies the identity and authenticity of the certificate holder. A Truststore is a repository that stores trusted certificates and public keys. By generating a certificate authority-signed certificate in Salesforce and uploading it to the on-premise application Truststore, the identity architect can enable mutual authentication and secure communication between Salesforce and the on-premise application. The other options are not recommended for this scenario, as they either do not provide a trusted certificate chain, do not enable mutual authentication, or do not secure the communication. References: Create Certificate Authority-Signed Certificates, Mutual Authentication

NEW QUESTION 3

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 4

Universal Containers (UC) is building an authenticated Customer Community for its customers. UC does not want customer credentials stored in Salesforce and is confident its customers would be willing to use their social media credentials to authenticate to the community. Which two actions should an Architect recommend UC to take?

- A. Use Delegated Authentication to call the Twitter login API to authenticate users.
- B. Configure an Authentication Provider for LinkedIn Social Media Accounts.
- C. Create a Custom Apex Registration Handler to handle new and existing users.
- D. Configure SSO Settings For Facebook to serve as a SAML Identity Provider.

Answer: BC

Explanation:

Configuring an Authentication Provider for LinkedIn Social Media Accounts allows UC to use LinkedIn as an external identity provider for its customer community. This means that customers can use their LinkedIn credentials to log in to the community without storing their credentials in Salesforce. Creating a Custom Apex Registration Handler allows UC to customize how new and existing users are handled when they log in with an external identity provider. This means that UC can control how user records are created, updated, or matched when customers use their social media credentials to authenticate to the community. These two actions can meet the requirement of UC to use social media credentials for its customer community.

NEW QUESTION 5

Universal Containers is considering using Delegated Authentication as the sole means of Authenticating of Salesforce users. A Salesforce Architect has been brought in to assist with the implementation. What two risks Should the Architect point out? Choose 2 answers

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

Answer: BC

Explanation:

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

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

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

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

NEW QUESTION 6

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 7

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 8

Universal Containers (UC) has a desktop application to collect leads for marketing campaigns. UC wants to extend this application to integrate with Salesforce to create leads. Integration between the desktop application and Salesforce should be seamless. What Authorization flow should the Architect recommend?

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

Answer: B

Explanation:

This is an OAuth authorization flow that allows a web server application to obtain an access token to access Salesforce resources on behalf of the user¹. This flow is suitable for integrating a desktop application with Salesforce, as it does not require the user to enter their credentials in the application, but rather redirects them to the Salesforce login page to authenticate and authorize the application². This way, the integration between the desktop application and Salesforce is seamless and secure. The other options are not optimal for this requirement because:

- JWT Bearer Token Flow is an OAuth authorization flow that allows a client application to obtain an access token by sending a signed JSON Web Token (JWT) to Salesforce³. This flow does not involve user interaction, and requires the client application to have a certificate and a private key to sign the JWT. This flow is more suitable for server-to-server integration, not for desktop application integration.
- User Agent Flow is an OAuth authorization flow that allows a user-agent-based application (such as a browser or a mobile app) to obtain an access token by redirecting the user to Salesforce and receiving the token in the URL fragment⁴. This flow is not suitable for desktop application integration, as it requires the application to parse the URL fragment and store the token securely.
- Username and Password Flow is an OAuth authorization flow that allows a client application to obtain an access token by sending the user's username and password to Salesforce⁵. This flow is not recommended for desktop application integration, as it requires the user to enter their credentials in the application, which is not secure or seamless. References: OAuth Authorization Flows, Implement the OAuth 2.0 Web Server Flow, JWT-Based Access Tokens (Beta), User-Agent Flow, Username-Pass Flow

NEW QUESTION 9

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 service.

References:

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

NEW QUESTION 10

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 10

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

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

Answer: C

Explanation:

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

NEW QUESTION 15

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

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

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

Answer: BCD

Explanation:

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

NEW QUESTION 20

Universal Containers (UC) employees have Salesforce access from restricted IP ranges only, to protect against unauthorized access. UC wants to roll out the Salesforce1 mobile app and make it accessible from any location. Which two options should an Architect recommend? Choose 2 answers

- A. Relax the IP restriction with a second factor in the Connect App settings for Salesforce1 mobile app.
- B. Remove existing restrictions on IP ranges for all types of user access.
- C. Relax the IP restrictions in the Connect App settings for the Salesforce1 mobile app.
- D. Use Login Flow to bypass IP range restriction for the mobile app.

Answer: AC

Explanation:

The two options that an architect should recommend for UC to roll out the Salesforce1 mobile app and make it accessible from any location are:

- Relax the IP restriction with a second factor in the Connected App settings for Salesforce1 mobile app.

This option allows UC to enable two-factor authentication (2FA) for the Salesforce1 mobile app, which requires users to verify their identity with a second factor, such as a verification code or a mobile app, after entering their username and password. By enabling 2FA in the Connected App settings, UC can relax the IP restriction for the Salesforce1 mobile app, as users can access it from any location as long as they provide the second factor.

➤ Relax the IP restrictions in the Connected App settings for the Salesforce1 mobile app. This option allows UC to disable or modify the IP restriction for the Salesforce1 mobile app in the Connected App settings, which control how users can access a connected app, such as Salesforce1. By relaxing the IP restrictions, UC can allow users to access the Salesforce1 mobile app from any location without requiring 2FA. The other options are not recommended for this scenario. Removing existing restrictions on IP ranges for all types of user access would compromise security and compliance, as it would expose Salesforce to unauthorized access from any location. Using Login Flow to bypass IP range restriction for the mobile app would require custom code and logic, which could introduce complexity and errors. References: [Connected Apps], [Two-Factor Authentication], [Require a Second Factor of Authentication for Connected Apps], [IP Restrictions for Connected Apps], [Login Flows]

NEW QUESTION 24

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 29

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

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

Answer: B

Explanation:

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

NEW QUESTION 32

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

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

Answer: BC

Explanation:

these are the optimal actions to troubleshoot a SAML error. According to the Salesforce documentation¹, you can use the following methods to debug a SAML error:

- Use a browser that has an add-on/extension that can inspect SAML. This will allow you to see the SAML request and response messages and identify any issues with the SAML assertion or the SAML response².
- Paste the SAML Assertion Validator in Salesforce. This is a tool that helps you validate the last SAML operation on your organization and shows you any errors or warnings with the SAML assertion or the SAML response¹.

Option A is incorrect because the Callback URL is not related to SAML SSO. The Callback URL is used for OAuth SSO, which is a different protocol³. Option D is incorrect because using the browser's Development tools to view the Salesforce page's markup will not help you debug a SAML error. The page's markup does not contain any information about the SAML request or response⁴.

References: 1: SAML Login Errors - Salesforce 2: How to Troubleshoot a Single Sign-On Error | Salesforce Ben 3: Identity Providers and Service Providers - Salesforce 4: Single Sign-On - Salesforce

NEW QUESTION 36

Universal Containers (UC) would like to enable self-registration for their Salesforce Partner Community Users. UC wants to capture some custom data elements from the partner user, and based on these data elements, wants to assign the appropriate Profile and Account values. Which two actions should the Architect recommend to UC? Choose 2 answers

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

Answer: CD

Explanation:

To enable self-registration for partner community users, UC should modify the CommunitiesSelfRegController class to assign the Profile and Account values based on the custom data elements captured from the partner user. UC should also configure Registration for Communities to use a custom Apex controller that extends the CommunitiesSelfRegController class and overrides the default registration logic3.

References:

➤ [Customize Self-Registration](#)

NEW QUESTION 40

Northern Trail Outfitters (NTO) wants its customers to use phone numbers to log in to their new digital portal, which was designed and built using Salesforce Experience Cloud. In order to access the portal, the user will need to do the following:

- * 1. Enter a phone number and/or email address
- * 2. Enter a verification code that is to be sent via email or text.

What is the recommended approach to fulfill this requirement?

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

Answer: A

Explanation:

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

NEW QUESTION 44

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

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

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

Answer: BD

Explanation:

To give customers the ability to login with their Facebook and Twitter credentials, the identity architect should configure a predefined authentication provider for Facebook and a predefined authentication provider for Twitter. Authentication providers are configurations that enable users to authenticate with an external identity provider and access Salesforce resources. Salesforce provides predefined authentication providers for some common identity providers, such as Facebook and Twitter, which can be easily configured with minimal customization. Creating a custom external authentication provider is not necessary for this scenario. References: [Authentication Providers](#), [Social Sign-On with Authentication Providers](#)

NEW QUESTION 47

An insurance company has a connected app in its Salesforce environment that is used to integrate with a Google Workspace (formerly knot as G Suite).

An identity and access management (IAM) architect has been asked to implement automation to enable users, freeze/suspend users, disable users, and reactivate existing users in Google Workspace upon similar actions in Salesforce.

Which solution is recommended to meet this requirement?

- A. Configure user Provisioning for Connected Apps.
- B. Update the Security Assertion Markup Language Just-in-Time (SAML JIT) handler in Salesforce for user provisioning and de-provisioning.
- C. Build a custom REST endpoint in Salesforce that Google Workspace can poll against.
- D. Build an Apex trigger on the userlogin object to make asynchronous callouts to Google APIs.

Answer: A

Explanation:

User Provisioning for Connected Apps allows Salesforce to create, update, and deactivate users in an external service such as Google Workspace based on user and permission set assignments in Salesforce. References: [User Provisioning for Connected Apps](#)

NEW QUESTION 52

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

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 56

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 59

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 60

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 63

A financial services company uses Salesforce and has a compliance requirement to track information about devices from which users log in. Also, a Salesforce Security Administrator needs to have the ability to revoke the device from which users log in. What should be used to fulfill this requirement?

- A. Use multi-factor authentication (MFA) to meet the compliance requirement to track device information.
- B. Use the Activations feature to meet the compliance requirement to track device information.
- C. Use the Login History object to track information about devices from which users log in.
- D. Use Login Flows to capture device from which users log in and store device and user information in a custom object.

Answer: B

Explanation:

To track information about devices from which users log in and revoke the device access, the identity architect should use the Activations feature. Activations are records that store information about the devices and browsers that users use to access Salesforce. Administrators can view, manage, and revoke activations for users from the Setup menu. Activations can help monitor and control user access from different devices. References: Activations, Manage Activations for Your Users

NEW QUESTION 66

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 70

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

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

Answer: A

Explanation:

According to the Salesforce documentation², OAuth2 RPs (relying parties) are applications that use OAuth 2.0 for authentication and authorization with an external identity provider. This allows users to log in to multiple applications with a single identity provider account. The identity provider issues an access token to the relying party, which can be used to access protected resources on behalf of the user. This solution can support high volumes of logins per minute and unify multiple B2C Commerce sites and an Experience Cloud community with a single identity.

NEW QUESTION 71

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 73

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

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

Answer: B

Explanation:

The OAuth 2.0 Device Flow is a type of authorization flow that allows users to register an IoT device with limited display input or capabilities, such as a smart TV, a printer, or a smart speaker¹. The device flow works as follows¹:

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

References:

➤ OAuth 2.0 Device Flow

NEW QUESTION 78

Containers (UC) has implemented SAML-based single Sign-on for their Salesforce application and is planning to provide access to Salesforce on mobile devices using the Salesforce1 mobile app. UC wants to ensure that Single Sign-on is used for accessing the Salesforce1 mobile App. Which two recommendations should the Architect make? Choose 2 Answers

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

Answer: BC

Explanation:

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

NEW QUESTION 80

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

How should the quantity of required Identity Verification Credits be estimated?

- A. Each community comes with 10,000 Identity Verification Credits per month and only customers with more than 10,000 logins a month should estimate additional SMS verifications needed.
- B. Identity Verification Credits are consumed with each SMS (text message) sent and should be estimated based on the number of login verification challenges for SMS verification users.
- C. Identity Verification Credits are consumed with each verification sent and should be estimated based on the number of logins that will incur a verification challenge.
- D. Identity Verification Credits are a direct add-on license based on the number of existing member-based or login-based Community licenses.

Answer: B

Explanation:

Identity Verification Credits are units that are consumed when Salesforce sends verification messages to users via email or SMS. To use passwordless login, customers need to receive a one-time passcode via email or SMS that they can use to log in to the customer service portal. Therefore, Identity Verification Credits are consumed with each SMS (text message) sent and should be estimated based on the number of login verification challenges for SMS verification users. Email verification does not consume Identity Verification Credits. References: Identity Verification Credits, Passwordless Login

NEW QUESTION 82

A technology enterprise is setting up an identity solution with an external vendor's wellness application for its employees. The user attributes need to be returned to the wellness application in an ID token.

Which authentication mechanism should an identity architect recommend to meet the requirements?

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

Answer: A

Explanation:

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

NEW QUESTION 83

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

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

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

Answer: D

Explanation:

Embedded Login is a feature that allows Salesforce to embed a login widget into any web page, such as a service provider's site, to enable users to log in with their Salesforce credentials. However, Embedded Login relies on third-party cookies, which can cause browser compatibility issues and require users to adjust

their browser settings. Therefore, this should be considered before recommending it as a solution on the Salesforce Platform. References: Embedded Login, Embedded Login Implementation Guide

NEW QUESTION 84

The security team at Universal containers(UC) has identified exporting reports as a high-risk action and would like to require users to be logged into salesforce with their active directory (AD) credentials when doing so. For all other uses of Salesforce, Users should be allowed to use AD credentials or salesforce credentials. What solution should be recommended to prevent exporting reports except when logged in using AD credentials while maintaining the ability to view reports when logged in with salesforce credentials?

- A. Use SAML Federated Authentication and Custom SAML jit provisioning to dynamically add or remove a permission set that grants the Export Reports permission.
- B. Use SAML Federated Authentication, treat SAML sessions as high assurance, and raise the session level required for exporting reports.
- C. Use SAML Federated Authentication and block access to reports when accesses through a standard assurance session.
- D. Use SAML Federated Authentication with a login flow to dynamically add or remove a permission set that grants the export reports permission.

Answer: B

Explanation:

Using SAML Federated Authentication, treating SAML sessions as high assurance, and raising the session level required for exporting reports is the solution that should be recommended. This solution ensures that users can only export reports when they log in using AD credentials, which provide a high level of identity verification. Users who log in using Salesforce credentials, which provide a standard level of security, can still view reports but not export them. To implement this solution, you need to configure SAML Federated Authentication with AD as the identity provider⁴, set the session security level for SAML assertions to high assurance⁵, and require high-assurance session security for exporting reports¹. This solution also avoids the complexity and overhead of creating and managing custom permission sets or login flows.

NEW QUESTION 87

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

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

Answer: CD

Explanation:

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

NEW QUESTION 92

What item should an Architect consider when designing a Delegated Authentication implementation?

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

Answer: A

Explanation:

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

NEW QUESTION 97

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

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

Answer: BD

Explanation:

The two statements that are capabilities of Identity Connect are:

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

NEW QUESTION 100

An Architect needs to advise the team that manages the Identity Provider how to differentiate Salesforce from other Service Providers. What SAML SSO setting in Salesforce provides this capability?

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

Answer: C

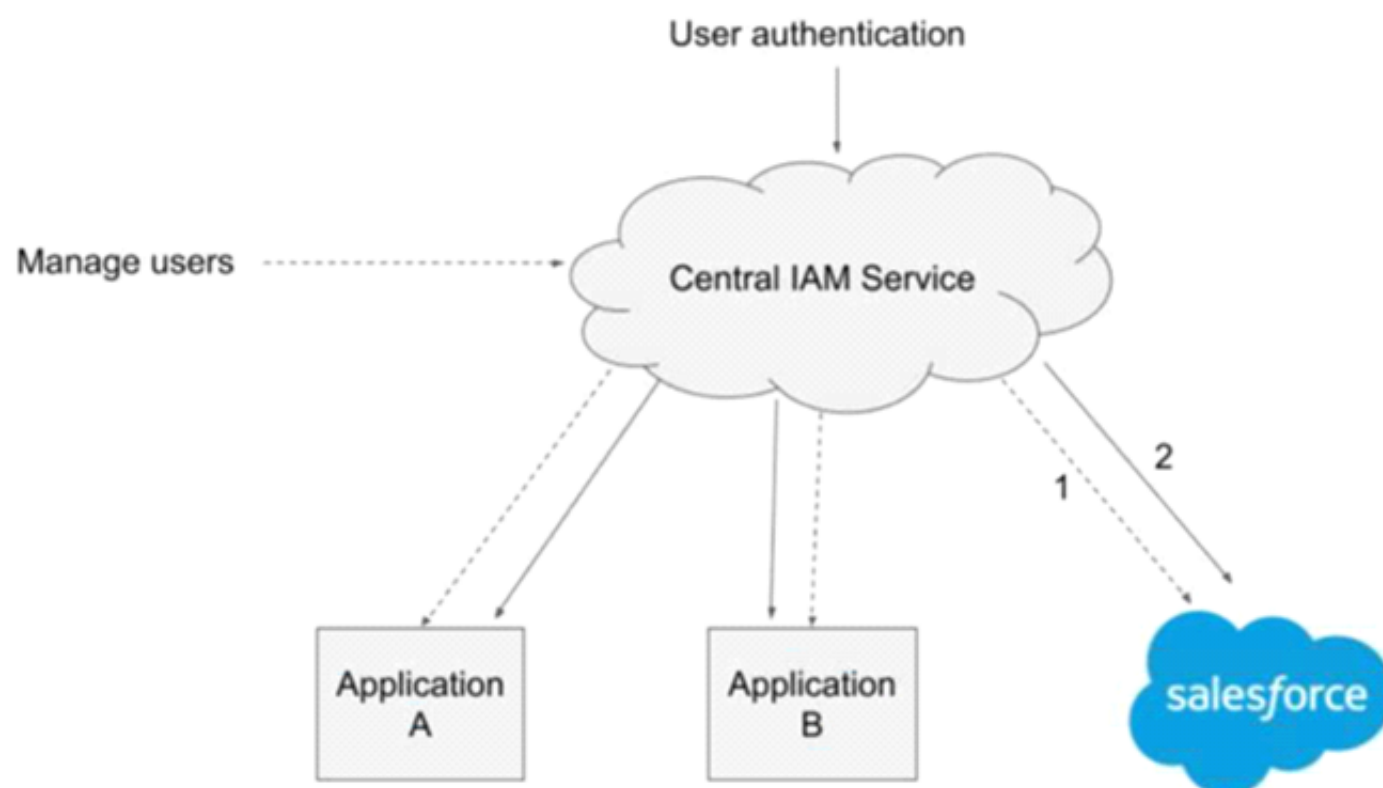
Explanation:

The Entity Id is the SAML SSO setting in Salesforce that provides the capability to differentiate Salesforce from other service providers. The Entity Id is a unique identifier for the service provider that is sent to the identity provider as part of the SSO request⁴. The identity provider uses the Entity Id to determine which service provider configuration to use and which SAML assertion to send back⁵. The other options are not valid SAML SSO settings for this purpose. The Identity Provider Login URL is the URL of the identity provider's SSO service that Salesforce redirects the user to for authentication⁴. The Issuer is the unique identifier for the identity provider that is sent by the identity provider as part of the SAML response⁴. The SAML Identity Location is the location of the user's identity in the SAML assertion, either in the Subject element or in an Attribute element⁴.

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

NEW QUESTION 101

An organization has a central cloud-based Identity and Access Management (IAM) Service for authentication and user management, which must be utilized by all applications as follows:



1 - Change of a user status in the central IAM Service triggers provisioning or deprovisioning in the integrated cloud applications.

2 - Security Assertion Markup Language single sign-on (SSO) is used to facilitate access for users authenticated at identity provider (Central IAM Service).

Which approach should an IAM architect implement on Salesforce Sales Cloud to meet the requirements?

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

Answer: A

Explanation:

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

NEW QUESTION 104

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

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

Answer: AD

Explanation:

A is correct because requiring users to provide their RSA token along with their credentials is a form of two-factor authentication. An RSA token is a hardware device that generates a one-time password (OTP) that changes every few seconds. The user needs to enter both their password and the OTP to log in to Salesforce.

D is correct because requiring users to use a biometric reader as well as their password is another form of two-factor authentication. A biometric reader is a device that scans a user's fingerprint, face, iris, or other physical characteristics to verify their identity. The user needs to provide both their password and their biometric data to log in to Salesforce.

B is incorrect because requiring users to supply their email and phone number, which gets validated, is not a form of two-factor authentication. This is a form of identity verification, which is used to confirm that the user owns the email and phone number they provided. However, this does not add an extra layer of protection beyond their password when they log in to Salesforce.

C is incorrect because requiring users to enter a second password after the first authentication is not a form of two-factor authentication. This is a form of single-factor authentication, which only relies on something the user knows (their passwords). This does not increase security against unauthorized account access.

References: 4: Multi-Factor Authentication - Salesforce 5: Salesforce Multi-Factor Authentication 6: Factor Authentication - Salesforce India 7: Customer 360 | Increase Productivity - Salesforce UK 8: Secu Salesforce Login Using Two-Factor Authentication and Salesforce ...

NEW QUESTION 105

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 110

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-m-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 112

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

Choose 2 answers

- A. Experience Builder Page

- B. lightning Experience Page
- C. Login Discovery Page
- D. Embedded Login Page

Answer: CD

Explanation:

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

NEW QUESTION 115

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 120

Universal containers(UC) wants to integrate a third-party reward calculation system with salesforce to calculate rewards. Rewards will be calculated on a schedule basis and update back into salesforce. The integration between Salesforce and the reward calculation system needs to be secure. Which are the recommended best practices for using Oauth flows in this scenario? Choose 2 answers

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

Answer: AC

Explanation:

OAuth refresh token flow and OAuth JWT bearer token flow are the recommended best practices for using OAuth flows in this scenario. These flows are suitable for server-to-server integration scenarios where the client application needs to access Salesforce resources on behalf of a user. The OAuth refresh token flow allows the client application to obtain a long-lived refresh token that can be used to request new access tokens without requiring user interaction. The OAuth JWT bearer token flow allows the client application to use a JSON Web Token (JWT) to assert its identity and request an access token. Both flows provide a secure and efficient way to integrate with Salesforce and the reward calculation system. OAuth SAML bearer assertion flow is not a recommended best practice for using OAuth flows in this scenario because it requires the client application to obtain a SAML assertion from an identity provider, which adds an extra layer of complexity and dependency. OAuth username-password flow is not a recommended best practice for using OAuth flows in this scenario because it requires the client application to store the user's credentials, which poses a security risk and does not support two-factor authentication. References: : [Which OAuth Flow to Use] : [Digging Deeper into OAuth 2.0 on Force.com] : [OAuth 2.0 JWT Bearer Token Flow] : [OAuth 2.0 SAML Bearer Assertion Flow] : [OAuth 2.0 Username-Password Flow]

NEW QUESTION 125

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

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

Answer: B

Explanation:

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

NEW QUESTION 126

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

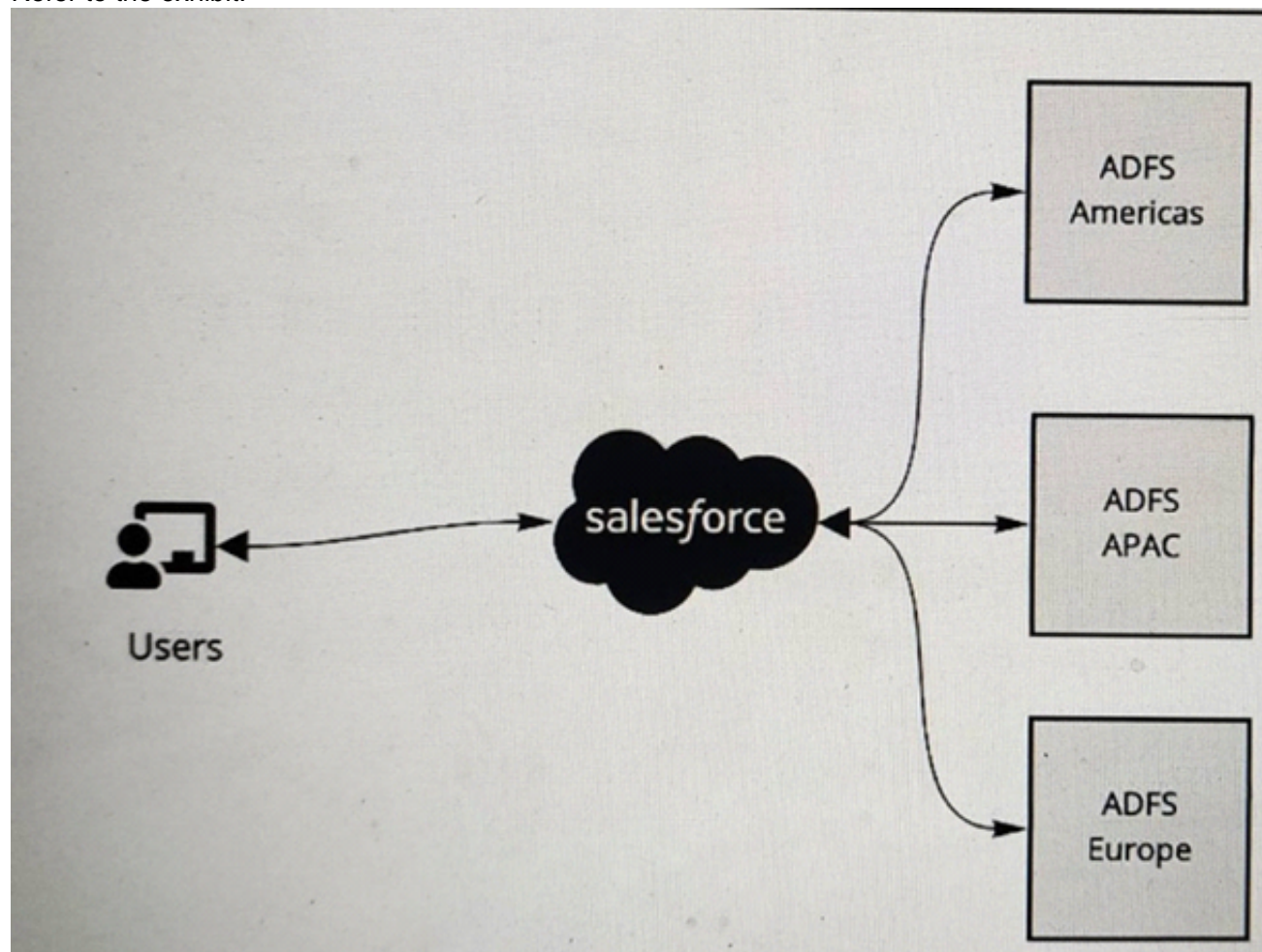
Explanation:

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 127

Refer to the exhibit.



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

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

Answer: B

Explanation:

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

NEW QUESTION 132

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 se
- 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 135

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

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

Answer: B

Explanation:

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

NEW QUESTION 136

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

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

Answer: B

Explanation:

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

NEW QUESTION 141

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

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

Answer: ACE

Explanation:

These are the steps required to enable Salesforce as a SAML Identity Provider and use the App Launcher to access external applications. According to the Salesforce documentation¹, you need to:

- Enable Salesforce as a SAML Identity Provider with My Domain².
- Create a Connected App for each external application that you want to integrate with Salesforce³.
- Add each Connected App to the App Launcher with a Start URL that points to the external application¹.

Option B is incorrect because setting up an Auth Provider is not necessary for SAML SSO. Auth Providers are used for OAuth SSO, which is a different protocol⁴. Option D is incorrect because Identity Connect is a tool for synchronizing user data between Active Directory and Salesforce, which is not related to SSO or App Launcher⁵.

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

NEW QUESTION 146

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

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

D. Identity connect is not compatible with UC's current identity environment.

Answer: A

Explanation:

Identity Connect will not support user provisioning in UC's current environment. Identity Connect is a tool that synchronizes user data between Active Directory and Salesforce, but it does not work with other identity sources such as a Custom Database⁵. Therefore, if UC wants to use Identity Connect as an Idp, they will not be able to provision users from their Custom Database to Salesforce.

Options B, C, and D are incorrect because Identity Connect does not have any limitations on the type of SAML flow or the compatibility with UC's current identity environment. Identity Connect supports both Idp-initiated and SP-initiated SAML flows⁶, and it can act as an Idp for any external service provider that supports SAML 2.07.

References: 5: Identity Connect - Salesforce 6: SAML SSO Flows - Salesforce 7: Salesforce Connect: Integration, Benefits, and Limitations

NEW QUESTION 150

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

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

Answer: AC

Explanation:

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

References: Salesforce Partner Community, Partner Community Registration Guide

NEW QUESTION 153

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

- A. Use the Identity Provider's certificate to digitally sign and Salesforce's Certificate to encrypt the payload.
- B. Use Salesforce's Certificate to digitally sign the SAML Assertion and a Mobile Device Management client on the users' mobile devices.
- C. Use the Identity provider's certificate to digitally Sign and the Identity provider's certificate to encrypt the payload.
- D. Use a custom login flow to retrieve sensitive data using an Apex callout without including the attributes in the assertion.

Answer: CD

Explanation:

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

References: [Single Sign-On Implementation Guide], [Customizing User Authentication with Login Flows]

NEW QUESTION 158

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

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

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

Answer: BD

Explanation:

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

NEW QUESTION 163

Northern Trail Outfitters is implementing a business-to-business (B2B) collaboration site using Salesforce Experience Cloud. The partners will authenticate with an existing identity provider and the solution will utilize Security Assertion Markup Language (SAML) to provide single sign-on to Salesforce. Delegated administration will be used in the Expenence Cloud site to allow the partners to administer their users' access.

How should a partner identity be provisioned in Salesforce for this solution?

- A. Create only a contact.
- B. Create a contactless user.
- C. Create a user and a related contact.
- D. Create a person account.

Answer: C

Explanation:

To provision a partner identity in Salesforce for a B2B collaboration site using SAML SSO, the identity architect should create a user and a related contact. A user record is required to authenticate and authorize the partner to access Salesforce resources. A contact record is required to associate the partner with an account, which represents the partner's organization. A contactless user or a person account are not supported for B2B collaboration sites. References: User and Contact Records for Partner Users, Create Partner Users

NEW QUESTION 168

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 169

Northern Trail Outfitters (NTO) is launching a new sportswear brand on its existing consumer portal built on Salesforce Experience Cloud. As part of the launch, emails with promotional links will be sent to existing customers to log in and claim a discount. The marketing manager would like the portal dynamically branded so that users will be directed to the brand link they clicked on; otherwise, users will view a recognizable NTO-branded page.

The campaign is launching quickly, so there is no time to procure any additional licenses. However, the development team is available to apply any required changes to the portal.

Which approach should the identity architect recommend?

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

Answer: B

Explanation:

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

NEW QUESTION 173

A technology enterprise is planning to implement single sign-on login for users. When users log in to the Salesforce User object custom field, data should be populated for new and existing users.

Which two steps should an identity architect recommend? Choose 2 answers

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

Answer: AB

Explanation:

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

NEW QUESTION 177

Universal Containers (UC) plans to use a SAML-based third-party IdP serving both of the Salesforce Partner Community and the corporate portal. UC partners will log in 65* to the corporate portal to access protected resources, including links to Salesforce resources. What would be the recommended way to configure the IdP so that seamless access can be achieved in this scenario?

- A. Set up the corporate portal as a Connected App in Salesforce and use the Web server OAuth flow.
- B. Configure SP-initiated SSO that passes the SAML token upon Salesforce resource access request.
- C. Set up the corporate portal as a Connected App in Salesforce and use the User Agent OAuth flow.
- D. Configure IdP-initiated SSO that passes the SAML token upon Salesforce resource access request.

Answer: D

Explanation:

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

NEW QUESTION 182

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 184

Universal Containers (UC) currently uses Salesforce Sales Cloud and an external billing application. Both Salesforce and the billing application are accessed several times a day to manage customers. UC would like to configure single sign-on and leverage Salesforce as the identity provider. Additionally, UC would like the billing application to be accessible from Salesforce. A redirect is acceptable.

Which two Salesforce tools should an identity architect recommend to satisfy the requirements? Choose 2 answers

- A. salesforce Canvas
- B. Identity Connect
- C. Connected Apps
- D. App Launcher

Answer: AD

Explanation:

Salesforce Canvas is a tool that allows external applications to be embedded into Salesforce as iframes, which can provide a seamless user experience. App Launcher is a feature that allows users to access connected apps from a single location in Salesforce. To enable single sign-on and use Salesforce as the identity provider, the external billing application needs to be configured as a connected app and use an OAuth 2.0 or SAML protocol. Identity Connect is not relevant for this scenario, as it is a tool for synchronizing user data between Salesforce and Active Directory. References: Salesforce Canvas Developer Guide, App Launcher, Connect Apps

NEW QUESTION 188

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

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

Answer: AD

Explanation:

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

NEW QUESTION 189

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 194

Northern Trail Outfitters (NTO) has a number of employees who do NOT need access Salesforce objects. Trie employees should sign in to a custom Benefits web app using their Salesforce credentials.

Which license should the identity architect recommend to fulfill this requirement?

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

Answer: A

Explanation:

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

NEW QUESTION 195

Universal containers (UC) has a mobile application that it wants to deploy to all of its salesforce users, including customer Community users. UC would like to minimize the administration overhead, which two items should an architect recommend? Choose 2 answers

- A. Enable the "Refresh Tokens is valid until revoked " setting in the Connected App.
- B. Enable the "Enforce Ip restrictions" settings in the connected App.
- C. Enable the "All users may self-authorize" setting in the Connected App.
- D. Enable the "High Assurance session required" setting in the Connected App.

Answer: AC

Explanation:

The two items that an architect should recommend for UC to minimize the administration overhead are:

➤ Enable the "Refresh Tokens is valid until revoked" setting in the Connected App. This setting allows the mobile app to obtain a refresh token from Salesforce when it obtains an access token. A refresh token can be used to obtain a new access token when the previous one expires or becomes invalid. By enabling this setting in the Connected App, UC can reduce the number of login prompts and authentication failures for its mobile users, as they can use the refresh token to renew their access without entering their credentials again.

➤ Enable the "All users may self-authorize" setting in the Connected App. This setting allows users to grant access to the mobile app without administrator approval. By enabling this setting in the Connected App, UC can simplify and speed up the deployment process for its mobile app, as they do not need to manually authorize each user or group of users.

The other options are not recommended items for this scenario. Enabling the "Enforce IP restrictions" setting in the Connected App would limit the mobile app access to certain IP ranges, which could prevent some users from accessing the app from different locations or networks. Enabling the "High Assurance session required" setting in the Connected App would require users to verify their identity with a second factor before accessing the mobile app, which could increase complexity and inconvenience for users. References: [Connected Apps], [Refresh Token], [All Users May Self-Authorize], [IP Restrictions for Connected Apps], [Require a Second Factor of Authentication for Connected Apps]

NEW QUESTION 196

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

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

Answer: BC

Explanation:

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

References: [Visualforce Pages], [Community Builder Pages], [Customize Password Management Features]

NEW QUESTION 197

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 199

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 200

Universal Containers (UC) uses Global Shipping (GS) as one of their shipping vendors. Regional leads of GS need access to UC's Salesforce instance for reporting damage of goods using Cases. The regional leads also need access to dashboards to keep track of regional shipping KPIs. UC internally uses a third-party cloud analytics tool for capacity planning and UC decided to provide access to this tool to a subset of GS employees. In addition to regional leads, the GS capacity planning team would benefit from access to this tool. To access the analytics tool, UC IT has set up Salesforce as the Identity provider for Internal users and would like to follow the same approach for the GS users as well. What are the most appropriate license types for GS Regional Leads and the GS Capacity Planners? Choose 2 Answers

- A. Customer Community Plus license for GS Regional Leads and External Identity for GS Capacity Planners.
- B. Customer Community Plus license for GS Regional Leads and Customer Community license for GS Capacity Planners.
- C. Identity License for GS Regional Leads and External Identity license for GS capacity Planners.
- D. Customer Community license for GS Regional Leads and Identity license for GS Capacity Planners.

Answer: AD

Explanation:

The most appropriate license types for GS regional leads and the GS capacity planners are:

- Customer Community Plus license for GS regional leads. This license type allows external users, such as customers or partners, to access standard Salesforce objects, such as cases and dashboards, and custom objects in a community. This license type also supports role hierarchy, sharing rules, and reports. This license type is suitable for GS regional leads who need to report damage of goods using cases and access dashboards to track regional shipping KPIs.
 - External Identity license for GS capacity planners. This license type allows external users to access a limited set of standard Salesforce objects, such as contacts and documents, and custom objects in a community. This license type also supports identity features, such as single sign-on (SSO) and social sign-on. This license type is suitable for GS capacity planners who need to access the third-party cloud analytics tool using Salesforce as the identity provider.
- The other options are not appropriate license types for this scenario. Customer Community license for GS capacity planners would not allow them to access the third-party cloud analytics tool using SSO, as this license type does not support identity features. Identity license for GS regional leads would not allow them to access cases and dashboards in the community, as this license type does not support standard Salesforce objects. References: [Customer Community Plus Licenses], [External Identity Licenses], [Customer Community Licenses], [Identity Licenses]

NEW QUESTION 205

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

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

Answer: C

Explanation:

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

NEW QUESTION 206

Northern Trail Outfitters wants to implement a partner community. Active community users will need to review and accept the community rules, and update key contact information for each community member before their annual partner event.

Which approach will meet this requirement?

- A. Create tasks for users who need to update their data or accept the new community rules.
- B. Create a custom landing page and email campaign asking all community members to login and verify their data.
- C. Create a login flow that conditionally prompts users who have not accepted the new community rules and who have missing or outdated information.
- D. Add a banner to the community Home page asking users to update their profile and accept the new community rules.

Answer: C

Explanation:

To meet the requirement of having active community users review and accept the community rules and update key contact information before their annual partner event, the identity architect should create a login flow that conditionally prompts users who have not accepted the new community rules and who have missing or outdated information. 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. By creating a login flow, the identity architect can check the user's status and information and display the appropriate screens for them to review and accept the community rules and update their contact information. References: Login Flows, Create a Login Flow

NEW QUESTION 209

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

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

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

Answer: AE

Explanation:

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

NEW QUESTION 213

The CIO of universal containers(UC) wants to start taking advantage of the refresh token capability for the UC applications that utilize Oauth 2.0. UC has listed an architect to analyze all of the applications that use Oauth flows to. See where refresh Tokens can be applied. Which two OAuth flows should the architect consider in their evaluation? Choose 2 answers

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

Answer: AC

Explanation:

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

NEW QUESTION 218

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

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

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

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