

Exam Questions Identity-and-Access-Management-Architect

Salesforce Certified Identity and Access Management Architect (SU23)

<https://www.2passeasy.com/dumps/Identity-and-Access-Management-Architect/>



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

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

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

Answer: CD

Explanation:

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

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

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

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

NEW QUESTION 3

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

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

Answer: BC

Explanation:

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

References: Identity Provider Overview, Connected Apps Overview, App Launcher, Single Sign-On for Desktop and Mobile Applications using SAML and OAuth

NEW QUESTION 4

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

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

Answer: C

Explanation:

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

NEW QUESTION 5

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

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

Answer: B

Explanation:

The SAML assertion OAuth flow allows a connected app to use a SAML assertion to request an OAuth access token to call Salesforce APIs. This flow provides an alternative for orgs that are currently using SAML to access Salesforce and want to access the web services API in the same way³. This flow can be used for inbound OAuth-enabled integration clients that want to use SAML-based single sign-on for authentication.

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

NEW QUESTION 6

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

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

Answer: C

Explanation:

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

NEW QUESTION 7

Universal Containers (UC) uses Salesforce as a CRM and identity provider (IdP) for their Sales Team to seamlessly login to internal portals. The IT team at UC is now evaluating Salesforce to act as an IdP for its remaining employees. Which Salesforce license is required to fulfill this requirement?

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

Answer: D

Explanation:

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

NEW QUESTION 8

Northern Trail Outfitters (NTO) believes a specific user account may have been compromised. NTO inactivated the user account and needs to perform a forensic analysis and identify signals that could indicate a breach has occurred. What should NTO's first step be in gathering signals that could indicate account compromise?

- A. Review the User record and evaluate the login and transaction history.

- B. Download the Setup Audit Trail and review all recent activities performed by the user.
- C. Download the Identity Provider Event Log and evaluate the details of activities performed by the user.
- D. Download the Login History and evaluate the details of logins performed by the user.

Answer: D

Explanation:

The Experience ID is a unique identifier for each Experience Cloud site that can be used to customize the branding and user interface based on the OAuth/Open ID or SAML flows. The Experience ID can be passed as a URL parameter to Salesforce to determine which site the user is accessing. References: Experience ID, Customize Your Experience Cloud Site Login Process

NEW QUESTION 9

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 10

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 10

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

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

Answer: D

Explanation:

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

NEW QUESTION 14

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 15

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 19

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 22

A multinational industrial products manufacturer is planning to implement Salesforce CRM to manage their business. They have the following requirements:

- * 1. They plan to implement Partner communities to provide access to their partner network.
- * 2. They have operations in multiple countries and are planning to implement multiple Salesforce orgs.
- * 3. Some of their partners do business in multiple countries and will need information from multiple Salesforce communities.
- * 4. They would like to provide a single login for their partners.

How should an Identity Architect solution this requirement with limited custom development?

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

Answer: A

Explanation:

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

NEW QUESTION 26

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 31

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

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

Answer: C

Explanation:

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

NEW QUESTION 34

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

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

Answer: BC

Explanation:

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

NEW QUESTION 38

A group of users try to access one of universal containers connected apps and receive the following error message: "Failed : Not approved for access". what is most likely to cause of the issue?

- A. The use of high assurance sessions are required for the connected App.
- B. The users do not have the correct permission set assigned to them.
- C. The connected App setting "All users may self-authorize" is enabled.
- D. The salesforce administrators gave revoked the OAuth authorization.

Answer: B

Explanation:

The users do not have the correct permission set assigned to them is the most likely cause of the issue. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect¹. Connected apps use these protocols to authorize, authenticate, and provide single sign-on (SSO) for external apps¹. To access a connected app, users must have the appropriate permissions assigned to them, either through their profile or a permission set². If the users do not have the required permissions, they will receive an error message when they try to access the connected app. The use of high assurance sessions are required for the connected app is not a valid option, as high assurance sessions are related to multi-factor authentication (MFA), not connected apps³. The connected app setting "All users may self-authorize" is enabled is not a cause of the issue, but a possible solution. This setting allows users to access the connected app without pre-approval from an administrator⁴. The Salesforce administrators have revoked the OAuth authorization is not a likely cause of the issue, as OAuth authorization is granted by the users, not the administrators⁵. Revoking OAuth authorization would also affect all users, not just a group of them.

References: Learn About Connected Apps, Create a Connected App, [Multi-Factor Authentication (MFA) for Salesforce], [Connected App Basics], OAuth Authorization Flows

NEW QUESTION 42

Universal Containers (UC) has implemented a multi-org architecture in their company. Many users have licences across multiple orgs, and they are complaining about remembering which org and credentials are tied to which business process. Which two recommendations should the Architect make to address the Complaints? Choose 2 answers

- A. Activate My Domain to Brand each org to the specific business use case.
- B. Implement SP-Initiated Single Sign-on flows to allow deep linking.
- C. Implement IdP-Initiated Single Sign-on flows to allow deep linking.
- D. Implement Delegated Authentication from each org to the LDAP provider.

Answer: AB

Explanation:

Activating My Domain allows each org to have a unique domain name that can be branded to the specific business use case². This can help users identify which

org they are logging into and avoid confusion. Implementing SP-Initiated Single Sign-on flows enables users to start from a service provider (such as Salesforce) and be redirected to an identity provider (such as Active Directory) for authentication³. This can also allow deep linking, which means users can access specific resources within the service provider after logging in⁴. These two recommendations can address the complaints of the users who have licenses across multiple orgs.

NEW QUESTION 43

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

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

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

Answer: AB

Explanation:

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

NEW QUESTION 47

Universal Containers (UC) wants to build a mobile application that will be making calls to the Salesforce REST API. UC's Salesforce implementation relies heavily on custom objects and custom Apex code. UC does not want its users to have to enter credentials every time they use the app. Which two scope values should an Architect recommend to UC? Choose 2 answers.

- A. Custom_permissions
- B. Api
- C. Refresh_token
- D. Full

Answer: BC

Explanation:

The two scope values that an architect should recommend to UC are api and refresh_token. The api scope allows the app to access the Salesforce REST API and use custom objects and custom Apex code. The refresh_token scope allows the app to obtain a refresh token that can be used to get new access tokens without requiring the user to re-enter credentials. Option A is not a good choice because the custom_permissions scope allows the app to access custom permissions in Salesforce, but it does not affect how the app can access the REST API or avoid user re-authentication. Option D is not a good choice because the full scope allows the app to access all data accessible by the user, including the web UI and the API, but it may be unnecessary or insecure for UC's requirement. References: OAuth 2.0 Web Server Authentication Flow, Digging Deeper into OAuth 2.0 on Force.com

NEW QUESTION 52

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

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

Answer: BD

Explanation:

The two role combinations that are represented by the systems in the scenario are Salesforce as the service provider and Google as the identity provider, and Salesforce as the service provider and Facebook as the identity provider. This means that Salesforce hosts the customer community app and relies on Google or Facebook to authenticate the users who log in with those options⁴. Therefore, option B and D are the correct answers. References: Salesforce as Service Provider and Identity Provider for SSO

NEW QUESTION 56

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 57

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 62

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 65

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 66

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 70

Universal Containers (UC) has an e-commerce website where customers can buy products, make payments, and manage their accounts. UC decides to build a Customer Community on Salesforce and wants to allow the customers to access the community from their accounts without logging in again. UC decides to implement an SP-initiated SSO using a SAML-compliant Idp. In this scenario where Salesforce is the Service Provider, which two activities must be performed in Salesforce to make SP-initiated SSO work? Choose 2 answers

- A. Configure SAML SSO settings.
- B. Create a Connected App.
- C. Configure Delegated Authentication.
- D. Set up My Domain.

Answer: AD

Explanation:

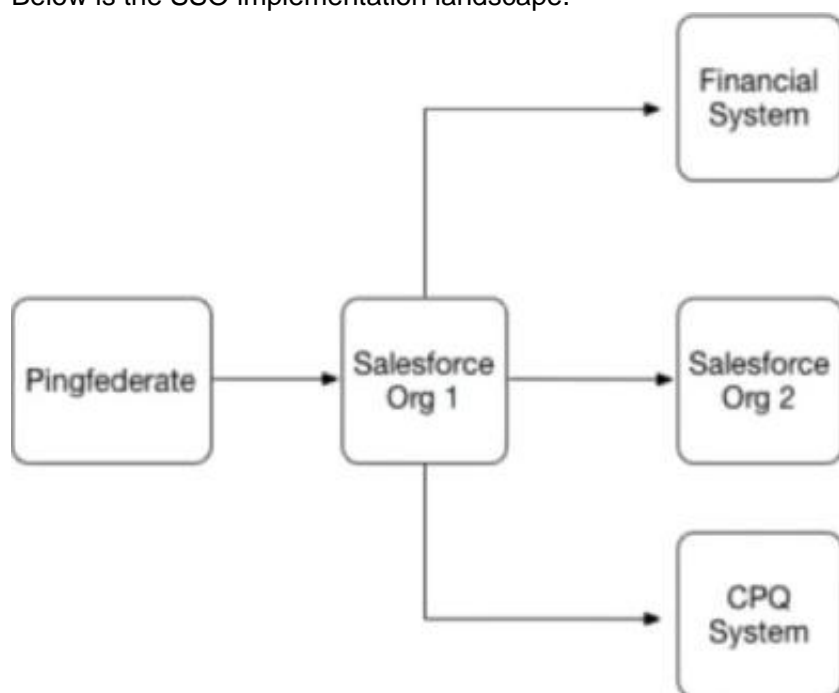
To enable SP-initiated SSO with Salesforce as the Service Provider, two steps are required in Salesforce:

- Option A is correct because configuring SAML SSO settings involves specifying the identity provider details, such as the entity ID, login URL, logout URL, and certificate².
- Option D is correct because setting up My Domain enables you to use a custom domain name for your Salesforce org and allows you to use SAML as an authentication method³.
- Option B is incorrect because creating a connected app is not necessary for SP-initiated SSO using a SAML-compliant IdP. A connected app is used for OAuth-based authentication or OpenID Connect-based authentication⁴.
- Option C is incorrect because configuring delegated authentication is not related to SP-initiated SSO using a SAML-compliant IdP. Delegated authentication is a feature that allows Salesforce to delegate user authentication to an external service, such as LDAP or Active Directory⁵.

References: SAML-based single sign-on: Configuration and Limitations, Configure SAML single sign-on with an identity provider, My Domain, Create a Connected App, Configure Salesforce for Delegated Authentication

NEW QUESTION 75

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



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

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

Answer: B

Explanation:

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

answer is B.

References:

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

NEW QUESTION 76

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 79

Northern Trail Outfitters recently acquired a company. Each company will retain its Identity Provider (IdP). Both companies rely extensively on Salesforce processes that send emails to users to take specific actions in Salesforce.

How should the combined company's employees collaborate in a single Salesforce org, yet authenticate to the appropriate IdP?

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

Answer: D

Explanation:

To allow employees to collaborate in a single Salesforce org, yet authenticate to the appropriate IdP, the identity architect should enable each IdP as a login option in the MyDomain Authentication Service settings. Users will then click on the appropriate IdP button. MyDomain is a feature that allows administrators to customize the Salesforce login URL with a unique domain name. Authentication Service is a setting that allows administrators to enable different authentication options for users, such as social sign-on or single

sign-on with an external IdP. By enabling each IdP as a login option in the MyDomain Authentication Service settings, the identity architect can provide a user-friendly and secure way for employees to log in to Salesforce using their preferred IdP. References: MyDomain, Authentication Service

NEW QUESTION 82

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

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

Answer: C

Explanation:

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

NEW QUESTION 87

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 90

Northern Trail Outfitters would like to automatically create new employee users in Salesforce with an appropriate profile that maps to its Active Directory Department.

How should an identity architect implement this requirement?

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

Answer: B

Explanation:

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

NEW QUESTION 91

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 93

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 94

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 99

A consumer products company uses Salesforce to maintain consumer information, including orders. The company implemented a portal solution using Salesforce Experience Cloud for its consumers where the consumers can log in using their credentials. The company is considering allowing users to login with their Facebook or LinkedIn credentials. Once enabled, what role will Salesforce play?

- A. Facebook and LinkedIn will be the SPs.
- B. Salesforce will be the service provider (SP).
- C. Salesforce will be the identity provider (IdP).
- D. Facebook and LinkedIn will act as the IdPs and SPs.

Answer: B

Explanation:

To allow users to login with their Facebook or LinkedIn credentials, Salesforce will play the role of a service provider (SP). A SP is an entity that relies on an identity provider (IdP) to authenticate and authorize users. In this scenario, Facebook and LinkedIn are the IdPs, and Salesforce is the SP. The SP receives a token from the IdP and uses it to access Salesforce resources. The other options are not correct for this scenario. References: Service Provider, Social Sign-On with Authentication Providers

NEW QUESTION 103

Universal containers (UC) is concerned that having a self-registration page will provide a means for "bots" or unintended audiences to create user records, thereby consuming licences and adding dirty data. Which two actions should UC take to prevent unauthorised form submissions during the self-registration process? Choose 2 answers

- A. Use open-ended security questions and complex password requirements
- B. Primarily use lookup and picklist fields on the self registration page.
- C. Require a captcha at the end of the self-registration process.
- D. Use hidden fields populated via java script events in the self-registration page.

Answer: CD

Explanation:

To prevent unauthorized form submissions during the self-registration process, UC should require a captcha at the end of the self-registration process and use hidden fields populated via JavaScript events in the self-registration page. These methods will help to verify that the user is a human and not a bot, and also to validate the user's input against some predefined values. Option A is not a good choice because open-ended security questions and complex password requirements may frustrate the user and reduce the conversion rate. Option B is not a good choice because lookup and picklist fields may not prevent bots from submitting the form, as they can be easily automated or bypassed.

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

NEW QUESTION 105

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 108

Universal Containers is using OpenID Connect to enable a connection from their new mobile app to its production Salesforce org. What should be done to enable the retrieval of the access token status for the OpenID Connect connection?

- A. Query using OpenID Connect discovery endpoint.
- B. A Leverage OpenID Connect Token Introspection.
- C. Create a custom OAuth scope.
- D. Enable cross-origin resource sharing (CORS) for the /services/oauth2/token endpoint.

Answer: B

Explanation:

According to the Salesforce documentation¹, OpenID Connect Token Introspection allows all OAuth connected apps to check the current state of an OAuth 2.0 access or refresh token. The resource server or connected apps send the client app's client ID and secret to the authorization server, initiating an OAuth authorization flow. As part of this flow, the authorization server validates, or introspects, the client app's access token. If the access token is current and valid, the client app is granted access.

NEW QUESTION 111

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 112

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

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

Answer: A

Explanation:

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

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

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

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

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

NEW QUESTION 115

Universal Containers (UC) wants to use Salesforce for sales orders and a legacy of system for order fulfillment. The legacy system must update the status of orders in 65* Salesforce in real time as they are fulfilled. UC decides to use OAuth for connecting the legacy system to Salesforce. What OAuth flow should be considered that doesn't require storing credentials, client secret or refresh tokens?

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

Answer: B

Explanation:

The JWT Bearer Token flow is an OAuth flow in which an external app (also called client or consumer app) sends a signed JSON string to Salesforce called JWT to obtain an access token. The access token can then be used by the external app to read & write data in Salesforce¹. This flow does not require storing credentials, client secret or refresh tokens, as the JWT is self-contained and includes information about the app and the user². The other flows require either user interaction (Web Server flow and User Agent flow) or storing credentials (Username-Password flow)³.

References: Salesforce OAuth : JWT Bearer Flow, Accessing Salesforce with JWT OAuth Flow, OAuth Authorization Flows - Salesforce

NEW QUESTION 118

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

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

Answer: C

Explanation:

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

NEW QUESTION 123

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

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

Answer: B

Explanation:

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

NEW QUESTION 128

Northern Trail Outfitters (NTO) has an existing custom business-to-consumer (B2C) website that does NOT support single sign-on standards, such as Security Assertion Markup Language (SAML) or OAuth. NTO wants to use Salesforce Identity to register and authenticate new customers on the website.
Which two Salesforce features should an identity architect use in order to provide username/password authentication for the website? Choose 2 answers

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

Answer: BD

Explanation:

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

NEW QUESTION 133

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

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

Answer: AD

Explanation:

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

- Enable My Domain and select "Prevent login from <https://login.salesforce.com>". My Domain is a feature that allows administrators to customize the Salesforce login URL with a unique domain name. By preventing login from the standard login URL, administrators can enforce SSO and restrict users from logging in with their Salesforce credentials.
- Assign user "is Single Sign-on Enabled" permission via profile or permission set. This permission allows users to log in to Salesforce using SSO. Users who do not have this permission will not be able to access Salesforce even if they have valid Salesforce credentials. References: My Domain, User Permissions for Single Sign-On

NEW QUESTION 135

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

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

Answer: AC

Explanation:

Relaxing the IP restriction in the connected app settings for the Salesforce1 mobile app and relaxing the IP restriction with a second factor in the connected app settings for Salesforce1 mobile app are two options that an architect should recommend. These options allow UC employees to access the Salesforce1 mobile app from any location, while still maintaining some level of security. Relaxing the IP restriction means that users can log in to the connected app from outside the trusted IP ranges defined in their profiles¹. Adding a second factor means that users need to provide an additional verification method, such as a verification code or a security key, to access the app². Using a login flow to bypass IP range restriction for the mobile app is not a recommended option because it can create a complex and inconsistent user experience³. Removing existing restrictions on IP ranges for all types of user access is not a recommended option because it can expose UC's data and applications to unauthorized access⁴. References: 1: Restrict Access to Trusted IP Ranges for a Connected App 2: Require Multi-Factor Authentication for Connected Apps 3: [Custom Login Flows] 4: [Restrict Login Access by IP Address]

NEW QUESTION 138

Under which scenario Web Server flow will be used?

- A. Used for web applications when server-side code needs to interact with APIs.
- B. Used for server-side components when page needs to be rendered.
- C. Used for mobile applications and testing legacy Integrations.
- D. Used for verifying Access protected resources.

Answer: A

Explanation:

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

NEW QUESTION 142

An administrator created a connected app for a custom web application in Salesforce which needs to be visible as a tile in App Launcher. The tile for the custom web application is missing in the app launcher for all users in Salesforce. The administrator requested assistance from an identity architect to resolve the issue. Which two reasons are the source of the issue? Choose 2 answers

- A. StartURL for the connected app is not set in Connected App settings.
- B. OAuth scope does not include "openid".
- C. Session Policy is set as 'High Assurance Session required' for this connected app.
- D. The connected app is not set in the App menu as 'Visible in App Launcher'.

Answer: AD

Explanation:

The StartURL for the connected app is required to specify the landing page for the app. The connected app must also be set as visible in the App Launcher to appear as a tile for users. References: Connected App Basics, Manage Connected Apps

NEW QUESTION 143

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

NTO has asked an identity architect to identify which Salesforce security configurations can map to AD permissions.

Which three Salesforce permissions are available to map to AD permissions? Choose 3 answers

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

Answer: ACE

Explanation:

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

NEW QUESTION 144

When designing a multi-branded Customer Identity and Access Management solution on the Salesforce Platform, how should an identity architect ensure a specific brand experience in Salesforce is presented?

- A. The Experience ID, which can be included in OAuth/Open ID flows and Security Assertion Markup Language (SAML) flows as a URL parameter.
- B. Provide a brand picker that the end user can use to select its sub-brand when they arrive on Salesforce.
- C. Add a custom parameter to the service provider's OAuth/SAML call and implement logic on its login page to apply branding based on the parameters value.

D. The Audience ID, which can be set in a shared cookie.

Answer: A

Explanation:

Configuring an authentication provider to delegate authentication to the LDAP directory ensures that users can only log in to Salesforce if they are active in the LDAP directory. This prevents terminated employees from accessing Salesforce with their old credentials. References: Authentication Providers, Delegated Authentication Single Sign-On

NEW QUESTION 149

A farming enterprise offers smart farming technology to its farmer customers, which includes a variety of sensors for livestock tracking, pest monitoring, climate monitoring etc. They plan to store all the data in Salesforce. They would also like to ensure timely maintenance of the Installed sensors. They have engaged a salesforce Architect to propose an appropriate way to generate sensor Information In Salesforce.

Which OAuth flow should the architect recommend?

- A. OAuth 2.0 Asset Token Flow
- B. OAuth 2.0 Device Authentication Row
- C. OAuth 2.0 JWT Bearer Token Flow
- D. OAuth 2.0 SAML Bearer Assertion Flow

Answer: A

Explanation:

To generate sensor information in Salesforce, the architect should recommend OAuth 2.0 Asset Token Flow. OAuth 2.0 Asset Token Flow is a protocol that allows devices, such as sensors, to obtain an access token from Salesforce by using a certificate instead of an authorization code. The access token can be used to access Salesforce APIs and send data to Salesforce. OAuth 2.0 Asset Token Flow is designed for devices that do not have a user interface or a web browser.

References: OAuth 2.0 Asset Token Flow, Authorize Apps with OAuth

NEW QUESTION 150

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

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

Answer: C

Explanation:

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

NEW QUESTION 152

Universal Containers (UC) has decided to replace the homegrown customer portal with Salesforce Experience Cloud. UC will continue to use its third-party single sign-on (SSO) solution that stores all of its customer and partner credentials.

The first time a customer logs in to the Experience Cloud site through SSO, a user record needs to be created automatically.

Which solution should an identity architect recommend in order to automatically provision users in Salesforce upon login?

- A. Just-in-Time (JIT) provisioning
- B. Custom middleware and web services
- C. Custom login flow and Apex handler
- D. Third-party AppExchange solution

Answer: A

Explanation:

Just-in-Time (JIT) provisioning is a feature that allows Salesforce to create or update user records on the fly when users log in through an external identity provider. This eliminates the need for manual or batch user provisioning in Salesforce. References: Just-in-Time Provisioning for SAML and OpenID Connect, Identity 101: Design Patterns for Access Management

NEW QUESTION 153

Universal Containers (UC) built an integration for their employees to post, view, and vote for ideas in Salesforce from an internal Company portal. When ideas are posted in Salesforce, links to the ideas are created in the company portal pages as part of the integration process. The Company portal connects to Salesforce using OAuth. Everything is working fine, except when users click on links to existing ideas, they are always taken to the Ideas home page rather than the specific idea, after authorization. Which OAuth URL parameter can be used to retain the original requested page so that a user can be redirected correctly after OAuth authorization?

- A. Redirect_uri
- B. State
- C. Scope

D. Callback_uri

Answer: A

Explanation:

Threedirect_uri parameter is used to specify the URL that the user should be redirected to after OAuth authorization¹. The redirect_uri should match the one that was registered with the OAuth client application². By using the redirect_uri parameter, the user can be redirected to the original requested page instead of the Ideas home page.

NEW QUESTION 154

Northern Trail Outfitters (NTO) is planning to roll out a partner portal for its distributors using Experience Cloud. NTO would like to use an external identity provider (IdP) and for partners to register for access to the portal. Each partner should be allowed to register only once to avoid duplicate accounts with Salesforce. What should a identity architect recommend to create partners?

- A. On successful creation of Partners using Self Registration page in Experience Cloud, create identity in Ping.
- B. Create a custom page in Experience Cloud to self register partner with Experience Cloud and Ping identity store.
- C. Create a custom web page in the Portal and create users in the IdP and Experience Cloud using published APIs.
- D. Allow partners to register through the IdP and create partner users in Salesforce through an API.

Answer: B

Explanation:

To create partners using an external identity provider (IdP) and avoid duplicate accounts with Salesforce, the identity architect should recommend creating a custom page in Experience Cloud to self register partner with Experience Cloud and Ping identity store. Ping is an IdP that supports OpenID Connect protocol, which allows users to sign in with an external identity provider and access Salesforce resources. By creating a custom page in Experience Cloud, the identity architect can use a custom registration handler to link the partner's Ping identity with their Salesforce identity and prevent duplicate accounts. The custom page can also provide a seamless user experience for the partners. References: OpenID Connect Authentication Providers, Social Sign-On with OpenID Connect, Create a Custom Registration Handler

NEW QUESTION 156

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual Identity-and-Access-Management-Architect Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the Identity-and-Access-Management-Architect Product From:

<https://www.2passeasy.com/dumps/Identity-and-Access-Management-Architect/>

Money Back Guarantee

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