Salesforce

Exam Questions Identity-and-Access-Management-Architect

Salesforce Certified Identity and Access Management Architect (SU23)

NEW QUESTION 1
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 2
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 3
Universal Containers (UC) has a strict requirement to authenticate users to Salesforce using their mainframe credentials. The mainframe user store cannot be accessed from a SAML provider. UC would also like to have users in Salesforce created on the fly if they provide accurate mainframe credentials.
How can the Architect meet these requirements?

A. Use a Salesforce Login Flow to call out to a web service and create the user on the fly.
B. Use the SOAP API to create the user when created on the mainframe; implement Delegated Authentication.
C. Implement Just-In-Time Provisioning on the mainframe to create the user on the fly.
D. Implement OAuth User-Agent Flow on the mainframe; use a Registration Handler to create the user on the fly.

Answer: C

Explanation:
The best way to meet the requirements of UC is to implement Just-In-Time Provisioning on the mainframe to create the user on the fly. According to the Salesforce documentation, "Just-in-time provisioning lets you create or update user accounts on the fly when users log in to Salesforce using single sign-on (SSO)." This way, UC can authenticate users to Salesforce using their mainframe credentials and also create or update their user accounts in Salesforce without using a SAML provider. Therefore, option C is the correct answer.
References: [Just-in-Time Provisioning]

NEW QUESTION 4
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 5
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 6
Containers (UC) uses an internal system for recruiting and would like to have the candidates' info available in the Salesforce automatically when they are selected. UC decides to use OAuth to connect to Salesforce from the recruiting system and would like to do the authentication using digital certificates. Which two OAuth flows should be considered to meet the requirement? Choose 2 answers

A. JWT Bearer Token flow
B. Refresh Token flow
C. SAML Bearer Assertion flow
D. Web Service flow

Answer: AC

Explanation:
JWT Bearer Token flow and SAML Bearer Assertion flow are two OAuth flows that can be used to authenticate to Salesforce using digital certificates. JWT Bearer Token flow allows a connected app to request an access token from Salesforce by using a JSON Web Token (JWT) that is signed with a digital certificate. SAML Bearer Assertion flow allows a connected app to request an access token from Salesforce by using a SAML assertion that is signed with a digital certificate. These two flows can meet the requirement of UC to use OAuth and digital certificates to connect to Salesforce from the recruiting system.

NEW QUESTION 7
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. Thi feature allows Salesforce to create or update user accounts based on the information provided by the external authentication service3.

References:

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

NEW QUESTION 8
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 9
Universal Containers (UC) uses a home-grown Employee portal for their employees to collaborate. UC decides to use Salesforce Ideas to allow employees to post Ideas from the Employee portal. When users click on some of the links in the Employee portal, the users should be redirected to Salesforce, authenticated, and presented with the relevant pages. What OAuth flow is best suited for this scenario?

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

Answer: D

Explanation:
The best OAuth flow for this scenario is the web server flow. The web server flow is an OAuth authorization flow that allows a web application, such as UC's employee portal, to obtain an access token and a refresh token from Salesforce after the user grants permission. The web application can then use the access token to access Salesforce data and features, such as posting ideas, and use the refresh token to obtain a new access token when the previous one expires or becomes invalid. This flow is suitable for UC's scenario because it allows users to be redirected to Salesforce, authenticated, and presented with the relevant pages when they click on some of the links in the employee portal. This flow also provides a secure and seamless user experience by using a confidential client secret that is stored on the web server and not exposed to the browser.
The other options are not valid OAuth flows for this scenario. The web application flow is not a standard term for OAuth, but it could refer to the user-agent flow, which is an OAuth authorization flow that allows a browser or web-view, such as a mobile app or a desktop app, to obtain an access token from Salesforce by using a script or a pop-up window. This flow is not suitable for UC's scenario, as it does not use a web server or a client secret, and it does not provide a refresh token. The SAML bearer assertion flow is an OAuth authorization flow that allows an external application to obtain an access token from Salesforce by using a SAML assertion from an identity provider (IdP) that verifies the user's identity. This flow is not suitable for UC's scenario, as it does not involve user interaction or redirection to Salesforce. The user-agent flow is an OAuth authorization flow that allows a browser or web-view, such as a mobile app or a desktop app, to obtain an access token from Salesforce by using a script or a pop-up window. This flow is not suitable for UC's scenario, as it does not use a web server or a client secret, and it does not provide a refresh token. References: [OAuth Authorization Flows], [OAuth 2.0 Web Server Flow for Web App Integration], [OAuth 2.0 User-Agent Flow for Desktop Apps], [OAuth 2.0 SAML Bearer Assertion Flow for Server-to-Server Integration]

NEW QUESTION 10
Which two capabilities does My Domain enable in the context of a SAML SSO configuration? Choose 2 answers

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

Answer: BC

Explanation:
These are two capabilities that My Domain enables in the context of a SAML SSO configuration. My Domain is a feature that lets you customize your Salesforce domain name and login page1. Resource deep linking is the ability to access a specific page or resource within Salesforce directly from a link, without having to navigate through the app2. SSO from Salesforce Mobile App is the ability to log in to the Salesforce Mobile App using your SSO credentials, without having to enter your username and password3. My Domain enables these capabilities by allowing you to specify your identity provider (IdP) and SSO settings for your unique domain name, and by providing a custom login URL that can be used for deep linking and mobile app login1. The other options are not correct for this question because:

- App Launcher is a feature that lets you access all your connected apps from one place in Salesforce. It does not require My Domain or SAML SSO to work, although it can be enhanced by using them.
- Login Forensics is a feature that analyzes login behavior and identifies anomalous or suspicious logins.

It does not require My Domain or SAML SSO to work, although it can be used with them.
References: My Domain, Deep Linking into Salesforce, Salesforce Mobile App Basics, [App Launc [Login Forensics]

NEW QUESTION 10
Which two are valid choices for digital certificates when setting up two-way SSL between Salesforce and an external system. Choose 2 answers

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

Answer: CD

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

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

This option is more secure and reliable, but requires Salesforce to trust the CA that signed the external system’s certificate implicitly.
References: Know more about all the SSL certificates that are supported by Salesforce, two way ssl. How to

NEW QUESTION 15
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 18
Sales users at Universal containers use salesforce for Opportunity management. Marketing uses a third-party application called Nest for Lead nurturing that is accessed using username/password. The VP of sales wants to open up access to nest for all sales uses to provide them access to lead history and would like SSO for better adoption. Salesforce is already setup for SSO and uses Delegated Authentication. Nest can accept username/Password or SAML-based Authentication. IT teams have received multiple password-related issues for nest and have decided to set up SSO access for Nest for Marketing users as well. The CIO does not want to invest in a new IDP solution and is considering using Salesforce for this purpose. Which are appropriate license type choices for sales and marketing users, giving salesforce is using Delegated Authentication? Choose 2 answers

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

Answer: AD

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

- Salesforce license for sales users. This license type allows internal users, such as employees, to access standard and custom Salesforce objects and features, such as opportunities and reports. This license type also supports delegated authentication, which is a feature that allows Salesforce to delegate the authentication process to an external service by making a SOAP callout to a web service that verifies the user’s credentials. This license type is suitable for sales users who use Salesforce for opportunity management and need to log in with delegated authentication.
- Platform license for marketing users. This license type allows internal users to access custom Salesforce objects and features, such as custom apps and tabs. This license type also supports delegated authentication and single sign-on (SSO), which are features that allow users to log in with an external identity provider (IdP) or service provider (SP). This license type is suitable for marketing users who use a third-party application called Nest for lead nurturing and need to log in with SSO using Salesforce as the IdP or SP.

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

NEW QUESTION 23
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 27
An architect needs to set up a Facebook Authentication provider as login option for a salesforce customer Community. What portion of the authentication provider setup associates a Facebook user with a salesforce user?

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

Answer: D

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

NEW QUESTION 29
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 33
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 Identit
Provider

NEW QUESTION 35
Northern Trail Outfitters (NTO) is setting up Salesforce to authenticate users with an external identity provider. The NTO Salesforce Administrator is having trouble getting things setup.
What should an identity architect use to show which part of the login assertion is fading?

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

Answer: D

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

NEW QUESTION 39
Universal Containers built a custom mobile app for their field reps to create orders in Salesforce. OAuth is used for authenticating mobile users. The app is built in such a way that when a user session expires after Initial login, a new access token is obtained automatically without forcing the user to log in again. While that

improved the field reps' productivity, UC realized that they need a "logout" feature.
What should the logout function perform in this scenario, where user sessions are refreshed automatically?

A. Invoke the revocation URL and pass the refresh token.
B. Clear out the client Id to stop auto session refresh.
C. Invoke the revocation URL and pass the access token.
D. Clear out all the tokens to stop auto session refresh.

Answer: A

Explanation:
The refresh token is used to obtain a new access token when the previous one expires. To revoke the user session, the logout function should invoke the revocation URL and pass the refresh token as a parameter. This will invalidate both the refresh token and the access token, and prevent the user from accessing Salesforce without logging in again2.
References:

- Certification Exam Guide
- Revoke OAuth Tokens

NEW QUESTION 44
IT security at Unversal Containers (UC) us concerned about recent phishing scams targeting its users and wants to add additional layers of login protection. What should an Architect recommend to address the issue?

A. Use the Salesforce Authenticator mobile app with two-step verification
B. Lock sessions to the IP address from which they originated.
C. Increase Password complexity requirements in Salesforce.
D. Implement Single Sign-on using a corporate Identity store.

Answer: A

Explanation:
The Salesforce Authenticator mobile app adds an extra layer of security for online accounts with two-factor authentication. It allows users to respond to push notifications or use location services to verify their logins and other account activity1. This can help prevent phishing scams and unauthorized access.
References: Salesforce Authenticator, Salesforce Authenticator: Mobile App Security Features, Salesforce Authenticator

NEW QUESTION 47
A public sector agency is setting up an identity solution for its citizens using a Community built on Experience Cloud and requires the new user registration functionality to capture first name, last name, and phone number. The phone number will be used for identity verification.
Which feature should an identity architect recommend to meet the requirements?

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

Answer: D

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

NEW QUESTION 48
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 50
Universal Containers (UC) is building a custom Innovation platform on their Salesforce instance. The Innovation platform will be written completely in Apex and Visualforce and will use custom objects to store the Data. UC would like all users to be able to access the system without having to log in with Salesforce credentials. UC will utilize a third-party idp using SAML SSO. What is the optimal Salesforce licence type for all of the UC employees?

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

Answer: D

Explanation:
The optimal Salesforce license type for all of the UC employees who will access the custom Innovation platform without logging in with Salesforce credentials is the Salesforce Platform license. The Salesforce Platform license allows users to access custom applications built on the Lightning Platform, such as Apex and Visualforce, and use standard objects such as accounts, contacts, reports, dashboards, and custom tabs. It also supports SSO with a third-party identity provider using SAML. Option A is not a good choice because the Identity license is designed for users who need to access Salesforce Identity features, such as identity provider, social sign-on, and user provisioning, but not for users who need to access custom applications. Option B is not a good choice because the Salesforce license is designed for users who need full access to standard CRM and Lightning Platform features, such as leads, opportunities, campaigns, forecasts, and contracts, but it may be unnecessary or expensive for users who only need to access custom applications. Option C is not a good choice because the External Identity license is designed for users who are external to the organization, such as customers or partners, but not for users who are internal employees.
References: Salesforce Help: User License Types, [Salesforce Help: Single Sign-On for Desktop and Mobile Applications using SAML and OAuth]

NEW QUESTION 51
An identity architect is setting up an integration between Salesforce and a third-party system. The third-party system needs to authenticate to Salesforce and then make API calls against the REST API.
One of the requirements is that the solution needs to ensure the third party service providers connected app in Salesforce mini need for end user interaction and maximizes security.
Which OAuth flow should be used to fulfill the requirement?

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

Answer: A

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

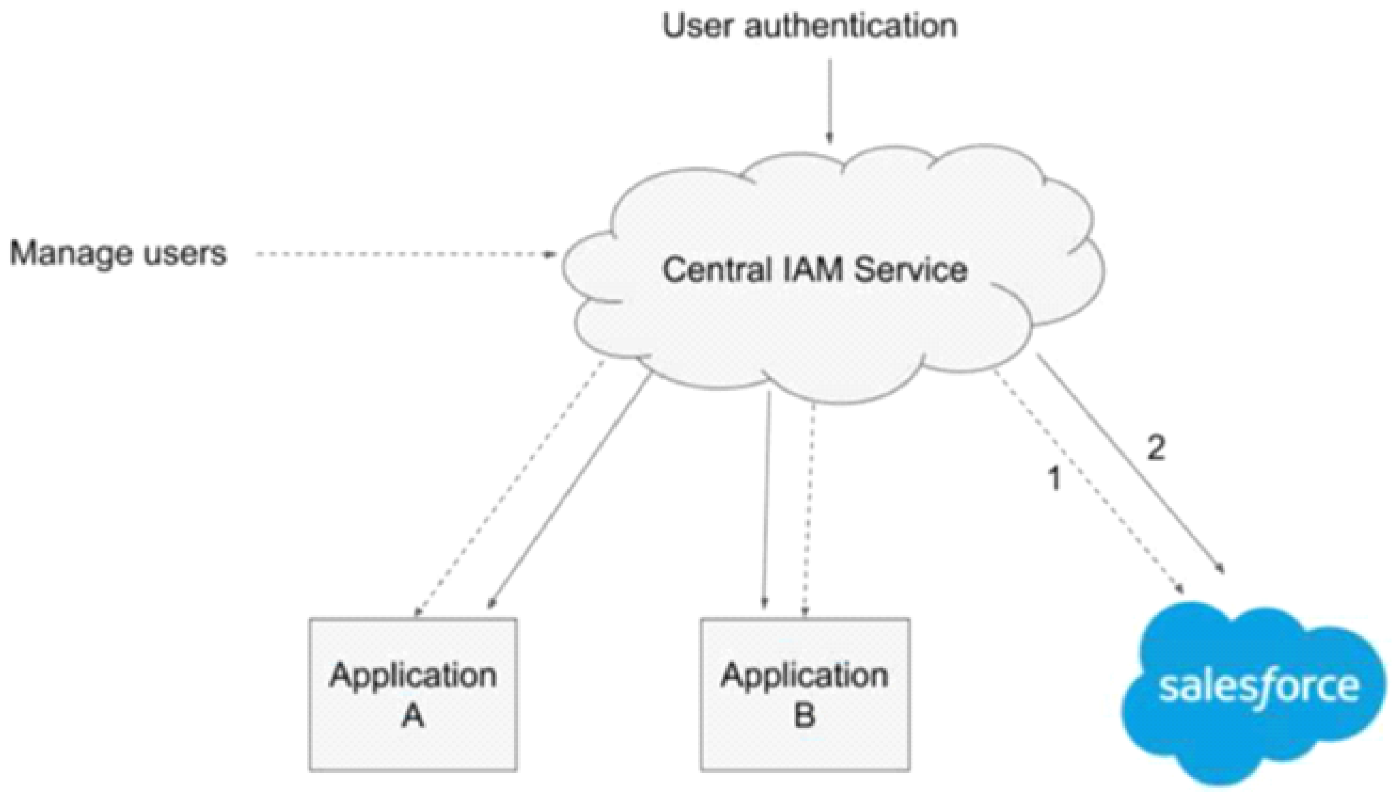
NEW QUESTION 52
An Architect needs to advise the team that manages the Identity Provider how to differentiate Salesforce from other Service Providers. What SAML SSO setting in Salesforce provides this capability?

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 53
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 57
Universal Containers (UC) has five Salesforce orgs (UC1, UC2, UC3, UC4, UC5). of Every user that is in UC2, UC3, UC4, and UC5 is also in UC1, however not all users 65* have access to every org. Universal Containers would like to simplify the authentication process such that all Salesforce users need to remember one set of credentials. UC would like to achieve this with the least impact to cost and maintenance. What approach should an Architect recommend to UC?

A. Purchase a third-party Identity Provider for all five Salesforce orgs to use and set up JIT user provisioning on all other orgs.
B. Purchase a third-party Identity Provider for all five Salesforce orgs to use, but don't set up JIT user provisioning for other orgs.
C. Configure UC1 as the Identity Provider to the other four Salesforce orgs and set up JIT user provisioning on all other orgs.
D. Configure UC1 as the Identity Provider to the other four Salesforce orgs, but don't set up JIT user provisioning for other orgs.

Answer: C

Explanation:
The best approach to simplify the authentication process and reduce cost and maintenance is to configure UC1 as the Identity Provider to the other four Salesforce orgs and set up JIT user provisioning on all other
orgs. This way, users can log in to any of the five orgs using their UC1 credentials, and their user accounts wil be automatically created or updated in the other orgs based on the information from UC11. This eliminates the need to purchase a third-party Identity Provider or manually provision users in advance. The other options are not optimal for this requirement because:
> Purchasing a third-party Identity Provider for all five Salesforce orgs would incur additional cost and maintenance, and would not leverage the existing user base in UC1.
> Not setting up JIT user provisioning for other orgs would require manually creating or updating user accounts in each org, which would be time-consuming and error-prone. References: Salesforce as an Identity Provider, Identity Providers and Service Providers, Just-in-Time Provisioning for SAML

NEW QUESTION 62
A global fitness equipment manufacturer is planning to sell fitness tracking devices and has the following requirements:
1) Customer purchases the device.
2) Customer registers the device using their mobile app.
3) A case should automatically be created in Salesforce and associated with the customer’s account in cases where the device registers issues with tracking.
Which OAuth flow should be used to meet these requirements?

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

Answer: A

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

NEW QUESTION 63
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 68
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 73
Universal Containers wants to secure its Salesforce APIs by using an existing Security Assertion Markup Language (SAML) configuration supports the company's single sign-on process to Salesforce,
Which Salesforce OAuth authorization flow should be used?

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

Answer: A

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

NEW QUESTION 74
Universal Containers (UC) has an existing web application that it would like to access from Salesforce without requiring users to re-authenticate. The web application is owned UC and the UC team that is responsible for it is willing to add new javascript code and/or libraries to the application. What implementation should an Architect recommend to UC?

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

Answer: A

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

NEW QUESTION 77
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 81
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 resourse 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 82
Universal Containers (UC) has a mobile application for its employees that uses data from Salesforce as well as uses Salesforce for Authentication purposes. UC wants its mobile users to only enter their credentials the first time they run the app. The application has been live for a little over 6 months, and all of the users who were part of the initial launch are complaining that they have to re-authenticate. UC has also recently changed the URI Scheme associated with the mobile app. What should the Architect at UC first investigate?Universal Containers (UC) has a mobile application for its employees that uses data from Salesforce as well as uses Salesforce for Authentication purposes. UC wants its mobile users to only enter their credentials the first time they run the app. The application has been live for a little over 6 months, and all of the users who were part of the initial launch are complaining that they have to re-authenticate. UC has also recently changed the URI Scheme associated with the mobile app. What should the Architect at UC first investigate?

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

Answer: A

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

NEW QUESTION 86
Northern Trail Outfitters manages application functional permissions centrally as Active Directory groups. The CRM_Superllser and CRM_Reportmg_SuperUser groups should respectively give the user the SuperUser and Reportmg_SuperUser permission set in Salesforce. Salesforce is the service provider to a Security Assertion Markup Language (SAML) identity provider.
Mow should an identity architect ensure the Active Directory groups are reflected correctly when a user accesses Salesforce?

A. Use the Apex Just-in-Time handler to query standard SAML attributes and set permission sets.

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

Answer: B

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

NEW QUESTION 89
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 93
Universal Containers (UC) rolling out a new Customer Identity and Access Management Solution will be built on top of their existing Salesforce instance.
Several service providers have been setup and integrated with Salesforce using OpenID Connect to allow for a seamless single sign-on experience. UC has a requirement to limit user access to only a subset of service providers per customer type.
Which two steps should be done on the platform to satisfy the requirement? Choose 2 answers

A. Manage which connected apps a user has access to by assigning authentication providers to the user's profile.
B. Assign the connected app to the customer community, and enable the users profile in the Community settings.
C. Use Profiles and Permission Sets to assign user access to Admin Pre-Approved Connected Apps.
D. Set each of the Connected App access settings to Admin Pre-Approved.

Answer: CD

Explanation:
To limit user access to only a subset of service providers per customer type, the identity architect should use Profiles and Permission Sets to assign user access to Admin Pre-Approved Connected Apps. Connected apps are frameworks that enable external applications to integrate with Salesforce using APIs and standard protocols, such as OpenID Connect. By setting each of the Connected App access settings to Admin Pre-Approved, the identity architect can control which users can access which connected apps by assigning profiles or permission sets to the connected apps. The other options are not relevant for this scenario. References: Connected Apps, Manage Connected Apps

NEW QUESTION 94
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 95
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 97
An identity architect is implementing a mobile-first Consumer Identity Access Management (CIAM) for external users. User authentication is the only requirement. The users email or mobile phone number should be supported as a username.
Which two licenses are needed to meet this requirement? Choose 2 answers

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

Answer: AD

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

NEW QUESTION 100
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 companys' employees collaborate in a single Salesforce org, yet authenticate to the appropriate IdP?

A. Configure unique MyDomains for each company and have generated links use the appropriate MyDomam in the URL.
B. Have generated links append a querystnng 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 102
Universal Containers (UC) would like its community users to be able to register and log in with Linkedin or Facebook Credentials. UC wants users to clearly see Facebook &Linkedin Icons when they register and login. What are the two recommended actions UC can take to achieve this Functionality? Choose 2 answers

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

Answer: AB

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

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

This action allows UC to configure Facebook and LinkedIn as authorization providers in Salesforce, which are external services that authenticate users and provide information about their identity and
attributes. By enabling these login options in the community configuration, UC can display Facebook and LinkedIn icons on the community login page and allow users to log in with their existing credentials from these services.

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

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

NEW QUESTION 107
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 111
Universal containers (UC) has decided to use identity connect as it's identity provider. UC uses active directory(AD) and has a team that is very familiar and comfortable with managing ad groups. UC would like to use AD groups to help configure salesforce users. Which three actions can AD groups control through identity connect? Choose 3 answers

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

Answer: ACE

Explanation:
AD groups can control public group assignment, role assignment, and permission set assignment through Identity Connect. Identity Connect is a tool that integrates Microsoft Active Directory (AD) user accounts with Salesforce user records1. It allows Salesforce admins to leverage the existing user data and group memberships in AD to automate user provisioning and deprovisioning in Salesforce. Identity Connect can map AD groups to Salesforce public groups, roles, and permission sets, and assign them to users based on their group membership2. This way, AD groups can control the access level and visibility of users in Salesforce. AD groups cannot control granting report folder access or custom permission assignment through Identity Connect. These are not supported features of Identity Connect. Report folder access is controlled by the folder sharing settings in Salesforce. Custom permission assignment is controlled by the custom permission settings in Salesforce. References: Get to Know Identity Connect, Map Your Data, [Folder Sharing], [Custom Permissions]

NEW QUESTION 116
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 121
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 124
An identity architect has been asked to recommend a solution that allows administrators to configure personalized alert messages to users before they land on the Experience Cloud site (formerly known as Community) homepage.
What is recommended to fulfill this requirement with the least amount of customization?

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

Answer: B

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

NEW QUESTION 129
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 134
Northern Trail Outfitters want to allow its consumer to self-register on it 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 139
A real estate company wants to provide its customers a digital space to design their interior decoration options. To simplify the registration to gain access to the community site (built in Experience Cloud), the CTO has requested that the IT/Development team provide the option for customers to use their existing social-media credentials to register and access.
The IT lead has approached the Salesforce Identity and Access Management (IAM) architect for technical direction on implementing the social sign-on (for Facebook, Twitter, and a new provider that supports standard OpenID Connect (OIDC)).
Which two recommendations should the Salesforce IAM architect make to the IT Lead? Choose 2 answers

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

Answer: BD

Explanation:
Authentication provider configuration and Apex coding skills are two recommendations that the Salesforce IAM architect should make to the IT Lead. Authentication providers are used to configure social sign-on providers, such as Facebook, Twitter, and any OpenID Connect compliant provider. Apex coding skills are needed for registration handlers, which are custom classes that create and update users based on social sign-on data. References: Authentication Providers, Registration Handlers

NEW QUESTION 141
Universal Container's (UC) identity architect needs to recommend a license type for their new Experience Cloud site that will be used by external partners (delivery providers) for reviewing and updating their accounts, downloading files provided by UC and obtaining scheduled pickup dates from their calendar.
UC is using their Salesforce production org as the identity provider for these users and the expected number of individual users is 2.5 million with 13.5 million unique logins per month.
Which of the following license types should be used to meet the requirement?

A. External Apps License
B. Partner Community License
C. Partner Community Login License
D. Customer Community plus Login License

Answer: C

Explanation:
Partner Community Login License is the best option for UC’s use case, as it allows external partners to access Experience Cloud sites and Salesforce data with a pay-per-login model. The other license types are either too expensive or not suitable for partner users. References: Experience Cloud User Licenses, Salesforce Experience Cloud Pricing

NEW QUESTION 146
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 151
Universal Containers (UC) implemented SSO to a third-party system for their Salesforce users to access the App Launcher. UC enabled “User Provisioning” on the Connected App so that changes to user accounts can be synched between Salesforce and the third-party system. However, UC quickly notices that changes to user roles in Salesforce are not getting synched to the third-party system. What is the most likely reason for this behavior?

A. User Provisioning for Connected Apps does not support role sync.
B. Required operation(s) was not mapped in User Provisioning Settings.
C. The Approval queue for User Provisioning Requests is unmonitored.
D. Salesforce roles have more than three levels in the role hierarchy.

Answer: B

Explanation:
User Provisioning for Connected Apps supports role sync, but the required operation(s) must be mapped in User Provisioning Settings. According to the

Salesforce documentation1, “To provision roles, map the Role operation to a field in the connected app. The field must contain the role’s unique name.”
Therefore, option B is the correct answer.
References: Salesforce Documentation

NEW QUESTION 153
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 154
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.

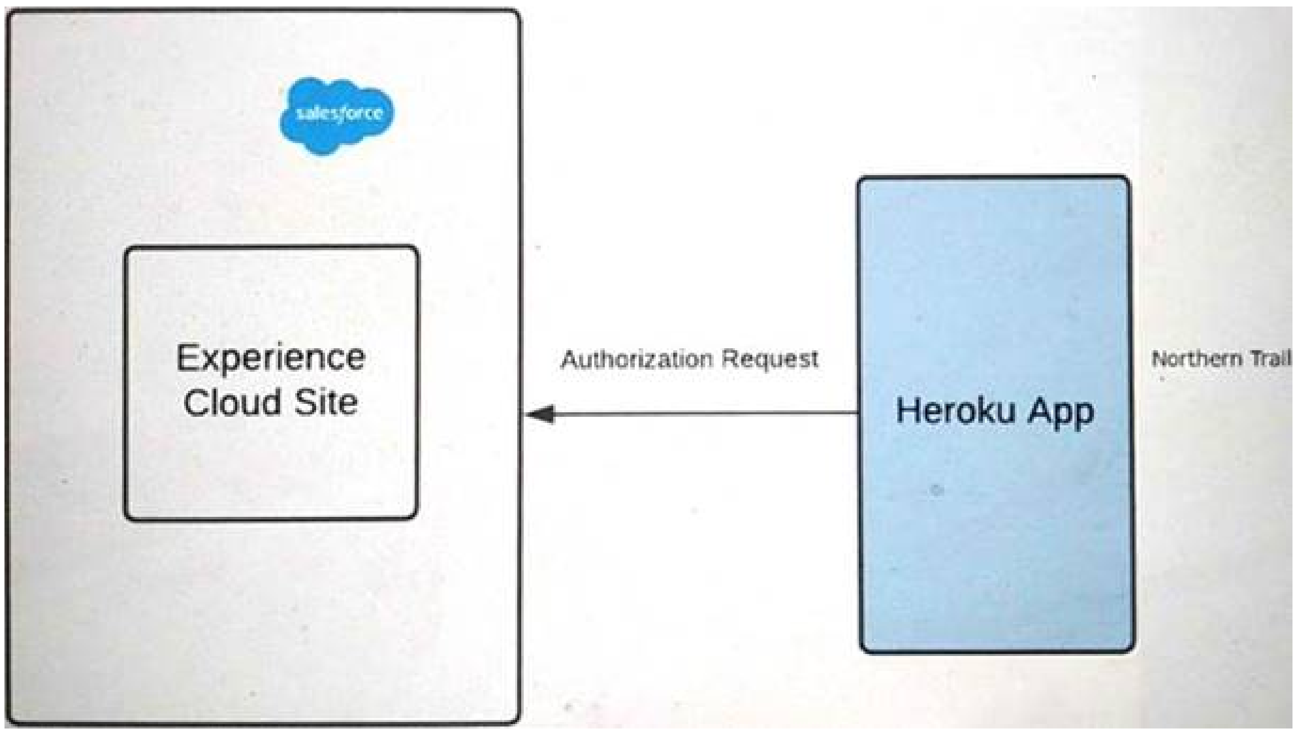
NEW QUESTION 155
universal container plans to develop a custom mobile app for the sales team that will use salesforce for authentication and access management. The mobile app access needs to be restricted to only the sales team. What would be the recommended solution to grant mobile app access to sales users?

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

Answer: B

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

NEW QUESTION 156
Refer to the exhibit.



Outfitters (NTO) is using Experience Cloud as an Identity for its application on Heroku. The application on Heroku should be able to handle two brands, Northern Trail Shoes and Northern Trail Shirts.
A user should select either of the two brands in Heroku before logging into the community. The app then performs Authorization using OAuth2.0 with the Salesforce Experience Cloud site.
NTO wants to make sure it renders login page images dynamically based on the user's brand preference selected in Heroku before Authorization.
what should an identity architect do to fulfill the above requirements?

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

Answer: D

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

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

References:

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

NEW QUESTION 161
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 163
Universal Containers (UC) has implemented SAML-based SSO solution for use with their multi-org Salesforce implementation, utilizing one of the the orgs as the

Identity Provider. One user is reporting that they can log in to the Identity Provider org but get a generic SAML error message when accessing the other orgs. Which two considerations should the architect review to troubleshoot the issue? Choose 2 answers

A. The Federation ID must be a valid Salesforce Username
B. The Federation ID must is case sensitive
C. The Federation ID must be in the form of an email address.
D. The Federation ID must be populated on the user record.

Answer: BD

Explanation:
The Federation ID is a field on the user object that is used to link a Salesforce user with an external identity provider. When using SAML SSO, Salesforce matches the Federation ID value with the NameID element in the SAML assertion to identify the user. To troubleshoot the issue of getting a generic SAML error message when accessing the other orgs, the architect should review the following considerations:

- The Federation ID must be case sensitive, which means that the value in the user record must match exactly with the value in the SAML assertion. For example, if the Federation ID is “John.Doe”, then “john.doe” or “JOHN.DOE” will not work.

- The Federation ID must be populated on the user record, which means that the user must have a value for this field in each org that they want to access via SSO. If the Federation ID is blank or missing, then Salesforce will not be able to match the user with the SAML assertion.

NEW QUESTION 166
architect is troubleshooting some SAML-based SSO errors during testing. The Architect confirmed that all of the Salesforce SSO settings are correct. Which two issues outside of the Salesforce SSO settings are most likely contributing to the SSO errors the Architect is encountering? Choose 2 Answers

A. The Identity Provider is also used to SSO into five other applications.
B. The clock on the Identity Provider server is twenty minutes behind Salesforce.
C. The Issuer Certificate from the Identity Provider expired two weeks ago.
D. The default language for the Identity Provider and Salesforce are Different.

Answer: BC

Explanation:
The two issues outside of the Salesforce SSO settings that are most likely contributing to the SSO errors are the clock on the identity provider server being twenty minutes behind Salesforce and the issuer certificate from the identity provider expiring two weeks ago. These issues can cause SAML assertion errors, which prevent the user from logging in with SSO. A SAML assertion is an XML document that contains information about the user’s identity and attributes, and it is signed by the identity provider and sent to Salesforce as part of the SSO process4. If the clock on the identity provider server is not synchronized with Salesforce, the SAML assertion may be rejected as invalid or expired, as it has a time limit for validity5. If the issuer certificate from the identity provider is expired, the SAML assertion may not be verified by Salesforce, as it relies on the certificate to validate the signature6. The other options are not likely issues that cause SSO errors. The identity provider being used to SSO into five other applications does not affect its ability to SSO into Salesforce, as long as it supports multiple service providers and has a separate configuration for each one7. The default language for the identity provider and Salesforce being different does not affect the SSO process, as it does not impact the SAML assertion or its validation.
References: SAML Login Errors, Troubleshoot SAML Assertion Errors, SAML SSO with Salesforce as th Service Provider, Single Sign-On, [How to Troubleshoot a Single Sign-On Error]

NEW QUESTION 170
Universal Containers (UC) is building an integration between Salesforce and a legacy web application using the canvas framework. The security for UC has determined that a signed request from Salesforce is not an adequate authentication solution for the Third-Party app. Which two options should the Architect consider for authenticating the third-party app using the canvas framework? Choose 2 Answers

A. Utilize the SAML Single Sign-on flow to allow the third-party to authenticate itself against UC's IdP.
B. Utilize Authorization Providers to allow the third-party application to authenticate itself against Salesforce as the Idp.
C. Utilize Canvas OAuth flow to allow the third-party application to authenticate itself against Salesforce as the Idp.
D. Create a registration handler Apex class to allow the third-party application to authenticate itself against Salesforce as the Idp.

Answer: AC

Explanation:
The Canvas framework supports OAuth 2.0 for authorization1. There are two OAuth flows that can be used to authenticate the third-party app using the canvas framework: User-Agent OAuth Flow and Web Server OAuth Flow2. The User-Agent OAuth Flow uses the Canvas JavaScript SDK to obtain an OAuth token by using the login function in the SDK2. The Web Server OAuth Flow redirects the user to the Salesforce OAuth authorization endpoint and then obtains an OAuth access token by making a POST request to the Salesforce OAuth token endpoint2. Both of these flows allow the third-party app to authenticate itself against Salesforce as the IdP. The SAML Single Sign-on flow can also be used to allow the third-party app to authenticate itself against UC’s IdP, which is another option for authentication3.
References: OAuth Authorization, Mastering Salesforce Canvas Apps, Integrate third-party applications vi Canvas App

NEW QUESTION 175
Northern Trail Outfitters (NTO) uses a Security Assertion Markup Language (SAML)-based Identity Provider (idP) to authenticate employees to all systems. The IdP authenticates users against a Lightweight Directory Access Protocol (LDAP) directory and has access to user information. NTO wants to minimize Salesforce license usage since only a small percentage of users need Salesforce.
What is recommended to ensure new employees have immediate access to Salesforce using their current IdP?

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

Answer: C

Explanation:
Just-in-Time (JIT) provisioning is a feature that allows Salesforce to create or update user records on the fly when users log in through an external identity

provider, such as a SAML-based IdP. This eliminates the need for manual or batch user provisioning in Salesforce and minimizes license usage. To use JIT provisioning, the identity architect needs to configure the SAML settings in Salesforce and include the user attributes in the SAML assertion sent by the IdP.
References: Just-in-Time Provisioning for SAML and OpenID Connect, Identity 101: Design Patterns for Access Management

NEW QUESTION 176
What information does the 'Relaystate' parameter contain in sp-Initiated Single Sign-on?

A. Reference to a URL redirect parameter at the identity provider.
B. Reference to a URL redirect parameter at the service provider.
C. Reference to the login address URL of the service provider.
D. Reference to the login address URL of the identity Provider.

Answer: B

Explanation:
The ‘Relaystate’ parameter is an HTTP parameter that can be included as part of the SAML request and SAML response. In an SP-initiated sign-in flow, the SP can set the RelayState parameter in the SAML request with additional information about the request, such as the URL of the resource that the user is trying to access.
The IDP should just relay it back in the SAML response without any modification or inspection. Therefore, the ‘Relaystate’ parameter contains a reference to a URL redirect parameter at the service provider123.
References: 1: single sign on - What is exactly RelayState parameter used in SSO (Ex. SAML)? - Stack
Overflow 2: java - How to send current URL as relay state while sending authentication request to IDP - Stack Overflow 3: Understanding SAML | Okta Developer

NEW QUESTION 181
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 182
Universal Containers uses Salesforce as an identity provider and Concur as the Employee Expense management system. The HR director wants to ensure Concur accounts for employees are created only after the apocopate approval in the Salesforce org.
Which three steps should the identity architect use to implement this requirement? Choose 3 answers

A. Create an approval process for a custom object associated with the provisioning flow.
B. Create a connected app for Concur in Salesforce.
C. Enable User Provisioning for the connected app.
D. Create an approval process for user object associated with the provisioning flow.
E. Create an approval process for UserProvisionlngRequest object associated with the provisioning flow.

Answer: BCE

Explanation:
User provisioning is a feature that allows Salesforce to create, update, or deactivate user accounts on a
third-party system, such as Concur, based on user assignments in Salesforce1. To implement user provisioning for Concur with an approval process, the identity architect should use the following steps2:

- Create a connected app for Concur in Salesforce. A connected app is an application that integrates with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect3. To create a connected app for Concur, you need to provide the basic information, such as the app name, logo URL, contact email, and API name. You also need to enable SAML and configure the SAML settings, such as the entity ID, ACS URL, and subject type4.
- Enable User Provisioning for the connected app. This step allows you to configure the user provisioning settings for the connected app, such as the provisioning API endpoint URL, the client ID and client secret, the mapping of user attributes, and the linkage rules5. You can also choose to require an approval process for user provisioning requests by selecting the Approval Required option6.
- Create an approval process for UserProvisioningRequest object associated with the provisioning flow. A UserProvisioningRequest object represents a user provisioning request that is sent to or received from a third-party system7. An approval process specifies the steps necessary for a record to be approved and who must approve it at each step8. To create an approval process for UserProvisioningRequest object, you need to define the approval steps, assignees, actions, criteria, and email alerts9.

References:

- User Provisioning for Connected Apps
- Tutorial: Configure Salesforce for automatic user provisioning
- Connected Apps
- Create a Connected App
- Enable User Provisioning for a Connected App
- Require Approvals for User Provisioning Requests

UserProvisioningRequest
- Approval Processes
- Create an Approval Process

NEW QUESTION 187
A company wants to provide its employees with a custom mobile app that accesses Salesforce. Users are required to download the internal native IOS mobile app from corporate intranet on their mobile device. The app allows flexibility to access other non-Salesforce internal applications once users authenticate with Salesforce. The apps self-authorize, and users are permitted to use the apps once they have logged into Salesforce.
How should an identity architect meet the above requirements with the privately distributed mobile app?

A. Use connected app with OAuth and Security Assertion Markup Language (SAML) to access other non-Salesforce internal apps.
B. Configure Mobile App settings in connected app and Salesforce as identity provider for non-Salesforce internal apps.
C. Use Salesforce as an identity provider (IdP) to access the mobile app and use the external IdP for other non-Salesforce internal apps.
D. Create a new hybrid mobile app and use the connected app with OAuth to authenticate users for Salesforce and non-Salesforce internal apps.

Answer: B

Explanation:
Configuring Mobile App settings in connected app and Salesforce as identity provider for non-Salesforce internal apps is the best way to meet the requirements with the privately distributed mobile app. The Mobile App settings allow users to download the app from a private URL and use it with Salesforce credentials. The identity provider settings allow users to access other internal apps with SSO using Salesforce as the IdP. The other options are either not feasible or not optimal for this use case. References: Mobile App Settings, Single Sign-On for Desktop and Mobile Applications using SAML and OAuth

NEW QUESTION 190
Universal Containers (UC) wants to build a few applications that leverage the Salesforce REST API. UC has asked its Architect to describe how the API calls will be authenticated to a specific user. Which two mechanisms can the Architect provide? Choose 2 Answers

A. Authentication Token
B. Session ID
C. Refresh Token
D. Access Token

Answer: CD

Explanation:
These are the mechanisms that the Salesforce REST API uses for authentication. According to the Salesforce documentation1, the REST API requires an access token obtained by authentication. The access token is a session credential that represents the authorization of a specific application to access specific parts of a user's data2. The access token is valid for a limited time and can be refreshed using a refresh token. A refresh token is a credential that represents the authorization of an application to refresh an expired access token2.
Option A is incorrect because an authentication token is not used by the Salesforce REST API. An authentication token is an email security feature that appends a unique string of characters to your password when you log in from an unrecognized device or IP address3. Option B is incorrect because a session ID is not used by the Salesforce REST API. A session ID is a unique identifier for a user's session that can be used for SOAP API calls4.
References: 1: Step Two: Set Up Authentication | REST API Developer Guide | Salesforce Developers 2: Salesforce REST APIs with Heroku - Trailhead 3: Authentication Token - Salesforce 4: Session ID - Salesforce

NEW QUESTION 195
Universal containers (UC) uses a home-grown employee portal for their employees to collaborate. UC decides to use salesforce ideas to allow the employees to post ideas from the employee portal. When clicking some links in the employee portal, the users should be redirected to salesforce, authenticated, and presented with relevant pages. What scope should be requested when using the Oauth token to meet this requirement?

A. Web
B. Full
C. API
D. Visualforce

Answer: A

Explanation:
The web scope should be requested when using the OAuth token to meet this requirement. The web scope
allows the user to log in to Salesforce and access the web UI. This is suitable for scenarios where the user is redirected from an external portal to Salesforce and needs to see the relevant pages. Option B is not a good choice because the full scope allows access to all data accessible by the user, including the web UI and the API. This may be unnecessary or insecure for this requirement. Option C is not a good choice because the API scope allows access to the Salesforce API only, not the web UI. This may not meet the requirement of presenting the user with relevant pages. Option D is not a good choice because the visualforce scope allows access to Visualforce pages only, not the entire web UI. This may limit the user's experience and functionality.
References: OAuth 2.0 Web Server Authentication Flow, Digging Deeper into OAuth 2.0 on Force.com

NEW QUESTION 200
which three are features of federated Single Sign-on solutions? Choose 3 answers

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

Answer: ABD

Explanation:

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

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

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

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

NEW QUESTION 204

An Identity and Access Management (IAM) Architect is recommending Identity Connect to integrate Microsoft Active Directory (AD) with Salesforce for user provisioning, deprovisioning and single sign-on (SSO).
Which feature of Identity Connect is applicable for this scenario?

A. When Identity Connect is in place, if a user is deprovisioned in an on-premise AD, the user's Salesforce session Is revoked Immediately.
B. If the number of provisioned users exceeds Salesforce license allowances, identity Connect will start disabling the existingSalesforce users in First-in, First-out (FIFO) fashion.
C. Identity Connect can be deployed as a managed package on salesforce org, leveraging High Availability of Salesforce Platform out-of-the-box.
D. When configured, Identity Connect acts as an identity provider to both Active Directory and Salesforce, thus providing SSO as a default feature.

Answer: A

Explanation:
Identity Connect is a tool that synchronizes user data between Microsoft Active Directory and Salesforce. It allows user provisioning, deprovisioning, and single sign-on (SSO) between multiple Active Directory domains and a single Salesforce org. One of the features of Identity Connect is that it can revoke the user's Salesforce session immediately when the user is deprovisioned in an on-premise Active Directory. This can enhance security and compliance by preventing unauthorized access to Salesforce resources. References: Identity Connect Implementation Guide, Identity Connect Overview

NEW QUESTION 205

......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

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

* Identity-and-Access-Management-Architect Questions and Answers Updated Frequently

* Identity-and-Access-Management-Architect Practice Questions Verified by Expert Senior Certified Staff

* Identity-and-Access-Management-Architect Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* Identity-and-Access-Management-Architect Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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