Exam Questions Identity-and-Access-Management-Architect

Salesforce Certified Identity and Access Management Architect (SU23)

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

NEW QUESTION 1
Universal containers(UC) has implemented SAML-BASED single Sign-on for their salesforce application and is planning to provide access to salesforce on mobile devices using the salesforce1 mobile app. UC wants to ensure that single Sign-on is used for accessing the salesforce1 mobile app. Which two recommendations should the architect make? Choose 2 answers

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

Answer: BD

Explanation:
To use SAML SSO for accessing the Salesforce1 mobile app, the architect should recommend configuring the embedded web browser to use the My Domain URL and configuring the Salesforce1 app to use the My Domain URL4. Using the My Domain URL allows Salesforce to identify the identity provider and initiate the SSO process5. Using the existing SAML SSO flow along with user agent flow or web server flow is not necessary because Salesforce Mobile Applications only work with service provider initiated setups46. Therefore, option B and D are the correct answers.
References: Salesforce Mobile Application Single Sign-On overview, SAML SSO with Salesforce as the Service Provider, Single Sign-On

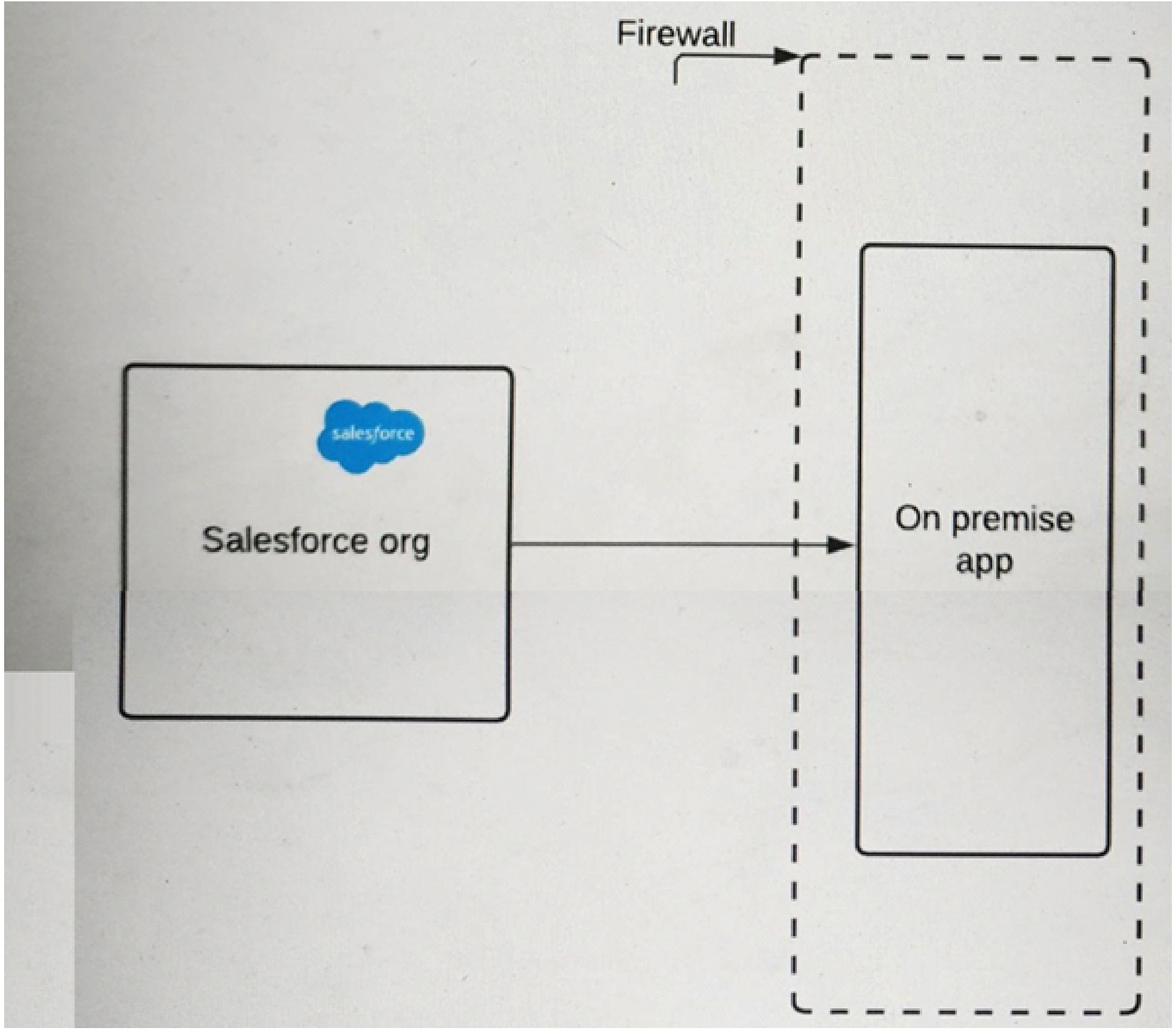
NEW QUESTION 2
In a typical SSL setup involving a trusted party and trusting party, what consideration should an Architect take into account when using digital certificates?

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

Answer: D

Explanation:
D is correct because using a self-signed certificate leads to higher maintenance for the trusting party, which is the client or browser that connects to the server. The trusting party needs to add the self-signed certificate to their truststore, which is a repository of trusted certificates, in order to establish a secure connection with the server. Otherwise, the trusting party will see a warning message or an error when accessing the server.
A is incorrect because using a self-signed certificate leads to higher maintenance for the trusted party, not lower. The trusted party needs to maintain multiple self-signed certificates from different servers in their truststore.
B is incorrect because using a self-signed certificate does not make the trusted party act as the trusted CA (Certificate Authority). The trusted CA is the entity that issues and validates certificates for servers. The trusted party only needs to trust the CA’s root certificate, which is usually pre-installed in their truststore.
C is incorrect because using a self-signed certificate leads to higher maintenance for the trusting party, not lower. The trusting party still needs to maintain a trusted CA cert in their truststore, which is the self-signed certificate itself.
References: 1: SSL Certificate Installation Instructions & Tutorials - DigiCert 2: How To Install an SSL Certificate from a Commercial … - DigitalOcean 3: Setup SSL CSR Creation and SSL Certificate Installatio
- DigiCert

NEW QUESTION 3
A pharmaceutical company has an on-premise application (see illustration) that it wants to integrate with Salesforce.



The IT director wants to ensure that requests must include a certificate with a trusted certificate chain to access the company's on-premise application endpoint.

What should an Identity architect do to meet this requirement?

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

Answer: C

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

NEW QUESTION 4
Universal containers want to build a custom mobile app connecting to salesforce using Oauth, and would like to restrict the types of resources mobile users can access. What Oauth feature of Salesforce should be used to achieve the goal?

A. Access Tokens
B. Mobile pins
C. Refresh Tokens
D. Scopes

Answer: D

Explanation:
The OAuth feature of Salesforce that should be used to restrict the types of resources mobile users can access is scopes. Scopes are parameters that specify the level of access that the mobile app requests from Salesforce when it obtains an OAuth token. Scopes can be used to limit the access to certain resources or actions, such as API calls, full access, web access, or refresh token. By configuring scopes in the connected app settings, Universal Containers can control what the mobile app can do with the OAuth token and protect against unauthorized or excessive access.
References: [OAuth Scopes], [Connected Apps], [OAuth Authorization Flows]

NEW QUESTION 5
Universal Containers is considering using Delegated Authentication as the sole means of Authenticating of Salesforce users. A Salesforce Architect has been brought in to assist with the implementation. What two risks Should the Architect point out? Choose 2 answers

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

Answer: BC

Explanation:
The two risks that the architect should point out for using delegated authentication as the sole means of authenticating Salesforce users are:
➢ UC will be required to develop and support a custom SOAP web service. Delegated authentication is a feature that allows Salesforce to delegate the authentication process to an external service by making a SOAP callout to a web service that verifies the user's credentials. This feature requires UC to develop and support a custom SOAP web service that can accept and validate the user's username and password, and return a boolean value to indicate whether the authentication is successful or not. This could increase complexity and cost for UC, as they need to write custom code and maintain the web service.
➢ Salesforce users will be locked out of Salesforce if the web service goes down. Delegated authentication relies on the availability and performance of the external web service that handles the authentication requests from Salesforce. If the web service goes down or becomes slow, Salesforce users will not be able to log in or access Salesforce, as they will receive an error message or a timeout response. This could cause disruption and frustration for UC's business operations and user satisfaction.
The other options are not valid risks for using delegated authentication. Delegated authentication can be enabled or disabled for individual users or groups of users by using permission sets or profiles, not for the entire Salesforce org. The web service does not need to reside on a public cloud service, such as Heroku, as it can be hosted on any platform that supports SOAP services and can communicate with Salesforce. References: [Delegated Authentication], [Enable 'Delegated Authentication'], [Troubleshoot Delegated Authentication]

NEW QUESTION 6
Universal Containers (UC) wants to integrate a third-party Reward Calculation system with Salesforce to calculate Rewards. Rewards will be calculated on a schedule basis and update back into Salesforce. The integration between Salesforce and the Reward Calculation System needs to be secure. Which are two recommended practices for using OAuth flow in this scenario. choose 2 answers

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

Answer: CD

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

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

> OAuth JWT Bearer Token Flow, which allows the client app to use a JSON Web Token (JWT) signed by a private key to request an access token from Salesforce. This flow does not require any user interaction or consent, and uses a certificate to verify the identity of the client app.
Verified References: [OAuth 2.0 SAML Bearer Assertion Flow for Server-to-Server Integration], [OAuth 2.0 JWT Bearer Token Flow for Server-to-Server Integration]

NEW QUESTION 7
A large consumer company is planning to create a community and will requ.re login through the customers social identity. The following requirements must be met:
* 1. The customer should be able to login with any of their social identities, however salesforce should only have one user per customer.
* 2. Once the customer has been identified with a social identity, they should not be required to authonze Salesforce.
* 3. The customers personal details from the social sign on need to be captured when the customer logs into Salesforce using their social Identity.
* 3. If the customer modifies their personal details in the social site, the changes should be updated in Salesforce.
Which two options allow the Identity Architect to fulfill the requirements? Choose 2 answers

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

Answer: BD

Explanation:
To allow customers to log in to the community with any of their social identities, such as Facebook, Google, or Twitter, the identity architect needs to use authentication providers for social sign-on. Authentication providers are configurations that enable users to authenticate with an external identity provider and access Salesforce resources. To ensure that Salesforce has only one user per customer, regardless of how many social identities they have, the identity architect needs to use the custom registration handler to link social identities to Salesforce identities. The custom registration handler is a class that implements the Auth.RegistrationHandler interface and defines how to create or update users in Salesforce based on the information from the external identity provider. The custom registration handler can also be used to insert or update personal details of the customers when they log in to Salesforce using their social identity.
References: Authentication Providers, Social Sign-On with Authentication Providers, Create a Custom Registration Handler

NEW QUESTION 8
A global company's Salesforce Identity Architect is reviewing its Salesforce production org login history and is seeing some intermittent Security Assertion Markup Language (SAML SSO) 'Replay Detected and Assertion Invalid' login errors.
Which two issues would cause these errors?
Choose 2 answers

A. The subject element is missing from the assertion sent to salesforce.
B. The certificate loaded into SSO configuration does not match the certificate used by the IdP.
C. The current time setting of the company's identity provider (IdP) and Salesforce platform is out of sync by more than eight minutes.
D. The assertion sent to 5alesforce contains an assertion ID previously used.

Answer: CD

Explanation:
A SAML SSO ‘Replay Detected and Assertion Invalid’ error occurs when Salesforce detects that the same assertion has been used more than once within the validity period. This can happen if the assertion ID is reused by the IdP or if the assertion is resent by the user. Another possible cause is that the time settings of the IdP and Salesforce are not synchronized, which can result in an assertion being valid for a shorter or longer period than expected. References: SAML Single Sign-On Settings, Troubleshoot SAML Single Sign-On

NEW QUESTION 9
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 10
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 10
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 14
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 19
Universal containers (UC) has implemented SAML SSO to enable seamless access across multiple applications. UC has regional salesforce orgs and wants it's users to be able to access them from their main Salesforce org seamless. Which action should an architect recommend?

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

Answer: B

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

NEW QUESTION 23
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 28
Universal Containers (UC) employees have Salesforce access from restricted IP ranges only, to protect against unauthorized access. UC wants to roll out the Salesforce1 mobile app and make it accessible from any location. Which two options should an Architect recommend? Choose 2 answers

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

Answer: AC

Explanation:
The two options that an architect should recommend for UC to roll out the Salesforce1 mobile app and make it accessible from any location are:
➢ Relax the IP restriction with a second factor in the Connected App settings for Salesforce1 mobile app.
This option allows UC to enable two-factor authentication (2FA) for the Salesforce1 mobile app, which requires users to verify their identity with a second factor, such as a verification code or a mobile app, after entering their username and password. By enabling 2FA in the Connected App settings, UC can relax the IP restriction for the Salesforce1 mobile app, as users can access it from any location as long as they provide the second factor.
➢ Relax the IP restrictions in the Connected App settings for the Salesforce1 mobile app. This option allows UC to disable or modify the IP restriction for the Salesforce1 mobile app in the Connected App settings, which control how users can access a connected app, such as Salesforce1. By relaxing the IP restrictions, UC can allow users to access the Salesforce1 mobile app from any location without requiring 2FA.
The other options are not recommended for this scenario. Removing existing restrictions on IP ranges for all types of user access would compromise security and compliance, as it would expose Salesforce to unauthorized access from any location. Using Login Flow to bypass IP range restriction for the mobile app would require custom code and logic, which could introduce complexity and errors. References: [Connected Apps], [Two-Factor Authentication], [Require a Second Factor of Authentication for Connected Apps], [IP Restrictions for Connected Apps], [Login Flows]

NEW QUESTION 32
Universal containers wants salesforce inbound Oauth-enabled integration clients to use SAML-BASED single Sign-on for authentication. What Oauth flow would be recommended in this scenario?

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

Answer: B

Explanation:
The SAML assertion OAuth flow allows a connected app to use a SAML assertion to request an OAuth access token to call Salesforce APIs. This flow provides an alternative for orgs that are currently using SAML to access Salesforce and want to access the web services API in the same way3. This flow can be used for inbound OAuth-enabled integration clients that want to use SAML-based single sign-on for authentication.
References: OAuth 2.0 SAML Bearer Assertion Flow for Previously Authorized Apps, Access Data with AP
Integration, Error ‘Invalid assertion’ in OAuth 2.0 SAML Bearer Flow

NEW QUESTION 35
A third-party app provider would like to have users provisioned via a service endpoint before users access their app from Salesforce.
What should an identity architect recommend to configure the requirement with limited changes to the third-party app?

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

Answer: A

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

NEW QUESTION 38
An identity architect has built a native mobile application and plans to integrate it with a Salesforce Identity solution. The following are the requirements for the solution:
* 1. Users should not have to login every time they use the app.
* 2. The app should be able to make calls to the Salesforce REST API.
* 3. End users should NOT see the OAuth approval page.
How should the identity architect configure the Salesforce connected app to meet the requirements?

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

Answer: A

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

NEW QUESTION 41
A service provider (SP) supports both Security Assertion Markup Language (SAML) and OpenID Connect (OIDC).
When integrating this SP with Salesforce, which use case is the determining factor when choosing OIDC or SAML?

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

Answer: B

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

NEW QUESTION 45
An Architect has configured a SAML-based SSO integration between Salesforce and an external Identity provider and is ready to test it. When the Architect attempts to log in to Salesforce using SSO, the Architect receives a SAML error. Which two optimal actions should the Architect take to troubleshoot the issue?

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

Answer: BC

Explanation:
these are the optimal actions to troubleshoot a SAML error. According to the Salesforce documentation1, yo can use the following methods to debug a SAML error:
> Use a browser that has an add-on/extension that can inspect SAML. This will allow you to see the SAML request and response messages and identify any issues with the SAML assertion or the SAML response2.
> Paste the SAML Assertion Validator in Salesforce. This is a tool that helps you validate the last SAML operation on your organization and shows you any errors or warnings with the SAML assertion or the SAML response1.
Option A is incorrect because the Callback URL is not related to SAML SSO. The Callback URL is used for OAuth SSO, which is a different protocol3. Option D is incorrect because using the browser’s Development tools to view the Salesforce page’s markup will not help you debug a SAML error. The page’s markup does not contain any information about the SAML request or response4.
References: 1: SAML Login Errors - Salesforce 2: How to Troubleshoot a Single Sign-On Error | Salesfo Ben 3: Identity Providers and Service Providers - Salesforce 4: Single Sign-On - Salesforce

NEW QUESTION 49
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 UC1 Choose 2 answers

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

Answer: CD

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

NEW QUESTION 52
Universal Containers (UC) is building a customer community and will allow customers to authenticate using Facebook credentials. The First time the user authenticating using Facebook, UC would like a customer account created automatically in their accounting system. The accounting system has a web service

accessible to Salesforce for the creation of accounts. How can the Architect meet these requirements?

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

Answer: C

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

NEW QUESTION 54
Northern Trail Outfitters (NTO) wants its customers to use phone numbers to log in to their new digital portal, which was designed and built using Salesforce Experience Cloud. In order to access the portal, the user will need to do the following:
* 1. Enter a phone number and/or email address
* 2. Enter a verification code that is to be sent via email or text.
What is the recommended approach to fulfill this requirement?

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

Answer: A

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

NEW QUESTION 58
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 59
Universal Containers (UC) uses Salesforce as a CRM and identity provider (IdP) for their Sales Team to seamlessly login to intemaJ portals. The IT team at UC is now evaluating Salesforce to act as an IdP for its remaining employees.
Which Salesforce license is required to fulfill this requirement?

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

Answer: D

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

NEW QUESTION 64
How should an Architect automatically redirect users to the login page of the external Identity provider when using an SP-Initiated SAML flow with Salesforce as a Service Provider?

A. Use visualforce as the landing page for My Domain to redirect users to the Identity Provider login Page.
B. Enable the Redirect to the Identity Provider setting under Authentication Services on the My domainConfiguration.
C. Remove the Login page from the list of Authentication Services on the My Domain configuration.
D. Set the Identity Provider as default and enable the Redirect to the Identity Provider setting on the SAML Configuration.

Answer: D

Explanation:
Setting the Identity Provider as default and enabling the Redirect to the Identity Provider setting on the SAML Configuration will automatically redirect users to the login page of the external Identity Provider when using an SP-Initiated SAML flow with Salesforce as a Service Provider1. Option A is incorrect because Visualforce is not a supported method for redirecting users to the Identity Provider login page2. Option B is incorrect because enabling the Redirect to the Identity Provider setting under Authentication Services on the My Domain Configuration will only redirect users to the Identity Provider login page when using an IdP-Initiated SAML flow3. Option C is incorrect because removing the Login page from the list of Authentication Services on the My Domain configuration will not affect the SP-Initiated SAML flow, and may cause other issues with authentication4.
References: SAML SSO Flows, Set up a Service Provider initiated login flow, Configure SAML single sign-on with an identity provider, SAML Identity Provider Configuration Settings

NEW QUESTION 65
Northern Trail Outfitters (NTO) believes a specific user account may have been compromised. NTO inactivated the user account and needs U perform a forensic analysis and identify signals that could Indicate a breach has occurred.
What should NTO's first step be in gathering signals that could indicate account compromise?

A. Review the User record and evaluate the login and transaction history.
B. Download the Setup Audit Trail and review all recent activities performed by the user.
C. Download the Identity Provider Event Log and evaluate the details of activities performed by the user.
D. Download the Login History and evaluate the details of logins performed by the user.

Answer: D

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

NEW QUESTION 70
An architect needs to advise the team that manages the identity provider how to differentiate salesforce from other service providers. What SAML SSO setting in salesforce provides this capability?

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

Answer: A

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

NEW QUESTION 71
Universal containers (UC) has an e-commerce website while customers can buy products, make payments, and manage their accounts. UC decides to build a customer Community on Salesforce and wants to allow the customers to access the community for their accounts without logging in again. UC decides to implement ansp-Initiated SSO using a SAML-BASED complaint IDP. In this scenario where salesforce is the service provider, which two activities must be performed in salesforce to make sp-Initiated SSO work? Choose 2 answers

A. Configure SAML SSO settings.
B. Configure Delegated Authentication
C. Create a connected App
D. Set up my domain

Answer: AD

Explanation:
To enable SP-initiated SSO using a SAML-based identity provider, UC needs to configure SAML SSO settings in Salesforce and set up a custom domain using My Domain feature. This allows UC to specify the identity provider information, such as the issuer, entity ID, certificate, and SAML assertion attributes. Delegated authentication is a different mechanism that allows Salesforce to delegate the authentication process to an external web service. A connected app is not required for SP-initiated SSO, but it is used for

IDP-initiated SSO or OAuth flows. References: Certification - Identity and Access Management Architect - Trailhead, [Set Up My Domain], [Configure SAML Settings for Single Sign-On]

NEW QUESTION 72
A group of users try to access one of Universal Containers' Connected Apps and receive the following error message: " Failed: Not approved for access." What is the most likely cause of this issue?

A. The Connected App settings "All users may self-authorize" is enabled.
B. The Salesforce Administrators have revoked the OAuth authorization.
C. The Users do not have the correct permission set assigned to them.
D. The User of High Assurance sessions are required for the Connected App.

Answer: C

Explanation:
The underlying mechanisms that the UC Architect must ensure are part of the product are Just-in-Time (JIT) provisioning and deprovisioning. JIT provisioning is a process that creates or updates user accounts in Salesforce when users log in with SAML single sign-on (SSO)6. JIT deprovisioning is a process that disables or deletes user accounts in Salesforce when users are removed from the identity provider (IdP). Both of these processes enable automated provisioning and deprovisioning of users without requiring manual intervention or synchronization. The other options are not valid mechanisms for provisioning and deprovisioning. SOAP API is an application programming interface that allows developers to create, retrieve, update, or delete records in Salesforce. However, SOAP API does not support JIT provisioning or deprovisioning, and requires custom code to implement. Provisioning API is not a standard term for Salesforce, and there is no such API that supports both provisioning and deprovisioning.
References: Just-in-Time Provisioning for SAML, [Just-in-Time Deprovisioning], [SOAP API Developer

NEW QUESTION 75
Universal containers (UC) uses a legacy Employee portal for their employees to collaborate and post their ideas. UC decides to use salesforce ideas for voting and better tracking purposes. To avoid provisioning users on Salesforce, UC decides to push ideas posted on the Employee portal to salesforce through API. UC decides to use an API user using Oauth Username - password flow for the connection. How can the connection to salesforce be restricted only to the employee portal server?

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

Answer: A

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

NEW QUESTION 79
What are three capabilities of Delegated Authentication? Choose 3 answers

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

Answer: BCE

Explanation:
The three capabilities of delegated authentication are:

- It can connect to SOAP services. Delegated authentication is a feature that allows Salesforce to delegate the authentication process to an external service by making a SOAP callout to a web service that verifies the user’s credentials. This feature enables Salesforce to integrate with existing identity stores or authentication methods that support SOAP services.
- It can be assigned by permission sets. Permission sets are collections of settings and permissions that give users access to various tools and functions in Salesforce. Permission sets can be used to assign delegated authentication to users by enabling the “Is Single Sign-on Enabled” permission. This permission allows users to log in with delegated authentication instead of their Salesforce username and password.
- It can connect to REST services. REST services are web services that use HTTP methods to access or manipulate resources on a server. REST services can be used for delegated authentication by creating a custom login page that makes a REST callout to an external service that verifies the user’s credentials. This approach requires custom code and configuration, but it provides more flexibility and control over the authentication process.

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

NEW QUESTION 83
Universal Containers has multiple Salesforce instances where users receive emails from different instances. Users should be logged into the correct Salesforce instance authenticated by their IdP when clicking on an email link to a Salesforce record.

What should be enabled in Salesforce as a prerequisite?

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

Answer: A

Explanation:
My Domain is a feature that allows you to personalize your Salesforce org with a subdomain within the Salesforce domain. For example, instead of using a generic URL like https://na30.salesforce.com, you can use a custom URL like https://somethingReallycool.my.salesforce.com10. My Domain should be enabled in Salesforce as a prerequisite for the following reasons:

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

References:

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

NEW QUESTION 85
A university is planning to set up an identity solution for its alumni. A third-party identity provider will be used for single sign-on Salesforce will be the system of records. Users are getting error messages when logging in.
Which Salesforce feature should be used to debug the issue?

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

Answer: D

NEW QUESTION 89
Universal Container's (UC) is using Salesforce Experience Cloud site for its container wholesale business. The identity architect wants to an authentication provider for the new site.
Which two options should be utilized in creating an authentication provider? Choose 2 answers

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

Answer: AB

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

- A custom registration handler, which is a class that implements the Auth.RegistrationHandler interface and defines how to create or update users in Salesforce based on the information from the external identity provider.
- A custom error URL, which is a URL that users are redirected to when an error occurs during the authentication process. References: Authentication Providers, Create an Authentication Provider

NEW QUESTION 91
Northern Trail Outfitters (NTO) uses the Customer 360 Platform implemented on Salesforce Experience Cloud. The development team in charge has learned of a contactless user feature, which can reduce the overhead of managing customers and partners by creating users without contact information.
What is the potential impact to the architecture if NTO decides to implement this feature?

A. Custom registration handler is needed to correctly assign External Identity or Community license for the newly registered contactless user.
B. If contactless user is upgraded to Community license, the contact record is automatically created and linked to the user record, but not associated with an Account.
C. Contactless user feature is available only with the External Identity license, which can restrict the Experience Cloud functionality available to the user.
D. Passwordless authentication cannot be supported because the mobile phone receiving one-time password (OTP) needs to match the number on the contact record.

Answer: B

Explanation:
According to the Salesforce documentation3, contactless user feature allows creating users without contact information, such as email address or phone number. This reduces the overhead of managing customers and partners who don’t need or want to provide their contact information. However, if a contactless user is upgraded to a Community license, a contact record is automatically created and linked to the user record, but not associated with an account. This can impact the architecture of NTO’s Customer 360 Platform, as they may need to associate contacts with accounts for reporting or other purposes.

NEW QUESTION 95

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 98
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 100
Containers (UC) has implemented SAML-based single Sign-on for their Salesforce application and is planning to provide access to Salesforce on mobile devices using the Salesforce1 mobile app. UC wants to ensure that Single Sign-on is used for accessing the Salesforce1 mobile App. Which two recommendations should the Architect make? Choose 2 Answers

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

Answer: BC

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

NEW QUESTION 103
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 107
A technology enterprise is setting up an identity solution with an external vendors wellness application for its employees. The user attributes need to be returned to the wellness application in an ID token.
Which authentication mechanism should an identity architect recommend to meet the requirements?

A. OpenID Connect
B. User Agent Flow
C. JWT Bearer Token Flow

D. Web Server Flow

Answer: A

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

NEW QUESTION 111
The executive sponsor for an organization has asked if Salesforce supports the ability to embed a login widget into its service providers in order to create a more seamless user experience.
What should be used and considered before recommending it as a solution on the Salesforce Platform?

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

Answer: D

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

NEW QUESTION 114
Universal Containers (UC) wants its users to access Salesforce and other SSO-enabled applications from a custom web page that UC magnets. UC wants its users to use the same set of credentials to access each of the applications. what SAML SSO flow should an Architect recommend for UC?

A. SP-Initiated with Deep Linking
B. SP-Initiated
C. IdP-Initiated
D. User-Agent

Answer: C

Explanation:
The SAML SSO flow that an architect should recommend for UC is IdP-initiated. IdP-initiated SSO is a process that allows users to start at the IdP site, such as UC’s custom web page, and then be redirected to Salesforce or other SPs with a SAML assertion that contains information about the user’s identity and attributes. This flow enables UC to provide a single point of entry for its users to access multiple applications with the same credentials, as they do not need to enter their username and password again for each application. This flow also simplifies the configuration and maintenance of SSO, as UC does not need to create or manage deep links or URLs for each application.
The other options are not valid SAML SSO flows for this scenario. SP-initiated with deep linking is a process that allows users to start at a specific resource on the SP site, such as a report or dashboard, and then be redirected to the IdP for authentication and back to the resource with a SAML assertion. This flow is not suitable for UC’s scenario, as they want their users to start at their custom web page, not at a specific resource on Salesforce or other SPs. SP-initiated is a process that allows users to start at the SP site, such as Salesforce or other applications, and then be redirected to the IdP for authentication and back to the SP site with a SAML assertion. This flow is not suitable for UC’s scenario, as they want their users to start at their custom web page, not at each application separately. User-agent is not a standard term for SAML SSO, but it could refer to user-agent flow, which is an OAuth authorization flow that allows users to obtain an access token from Salesforce by using a browser or web-view. This flow is not suitable for UC’s scenario, as it does not use SAML or IdP for authentication.
References: [SAML Single Sign-On], [IdP-Initiated Login], [SP-Initiated Login], [Deep Linking], [OAuth User-Agent Flow]

NEW QUESTION 116
Universal containers (UC) is successfully using Delegated Authentication for their salesforce users. The service supporting Delegated Authentication is written in Java. UC has a new CIO that is requiring all company Web services be RESR-ful and written in. NET. Which two considerations should the UC Architect provide to the new CIO? Choose 2 answers

A. Delegated Authentication will not work with a.net service.
B. Delegated Authentication will continue to work with rest services.
C. Delegated Authentication will continue to work with a.net service.
D. Delegated Authentication will not work with rest services.

Answer: CD

Explanation:
Delegated Authentication will continue to work with a .NET service as long as it is wrapped in a web service that Salesforce can consume1. Delegated Authentication will not work with REST services because it requires a SOAP-based web service23. Therefore, option C and D are the correct answers.
References: Salesforce Documentation, DEV Community, Salesforce Developer Community

NEW QUESTION 119
Universal Containers (UC) is looking to build a Canvas app and wants to use the corresponding Connected App to control where the app is visible. Which two options are correct in regards to where the app can be made visible under the Connected App setting for the Canvas app? Choose 2 answers

A. As part of the body of a Salesforce Knowledge article.

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

Answer: CD

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

NEW QUESTION 121
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 125
What item should an Architect consider when designing a Delegated Authentication implementation?

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

Answer: A

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

NEW QUESTION 128
Northern Trail Outfitters (NTO) is planning to implement a community for its customers using Salesforce Experience Cloud. Customers are not able to self-register. NTO would like to have customers set their own passwords when provided access to the community.
Which two recommendations should an identity architect make to fulfill this requirement? Choose 2 answers

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

Answer: CD

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

NEW QUESTION 130
A group of users try to access one of universal containers connected apps and receive the following error message: "Failed : Not approved for access". what is

most likely to cause of the issue?

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

Answer: B

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

NEW QUESTION 134
Universal Containers (UC) has implemented a multi-org architecture in their company. Many users have licences across multiple orgs, and they are complaining about remembering which org and credentials are tied to which business process. Which two recommendations should the Architect make to address the Complaints? Choose 2 answers

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

Answer: AB

Explanation:
Activating My Domain allows each org to have a unique domain name that can be branded to the specific business use case2. This can help users identify which org they are logging into and avoid confusion. Implementing SP-Initiated Single Sign-on flows enables users to start from a service provider (such as Salesforce) and be redirected to an identity provider (such as Active Directory) for authentication3. This can also allow deep linking, which means users can access specific resources within the service provider after logging in4. These two recommendations can address the complaints of the users who have licenses across multiple orgs.

NEW QUESTION 135
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 140
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 145
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 148
A security architect is rolling out a new multi-factor authentication (MFA) mandate, where all employees must go through a secure authentication process before accessing Salesforce. There are multiple Identity Providers (IdP) in place and the architect is considering how the "Authentication Method Reference" field (AMR) in the Login History can help.
Which two considerations should the architect keep in mind? Choose 2 answers

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

Answer: AB

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

NEW QUESTION 152
After a recent audit, universal containers was advised to implement Two-factor Authentication for all of their critical systems, including salesforce. Which two actions should UC consider to meet this requirement? Choose 2 answers

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

Answer: AD

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

NEW QUESTION 156
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 161
Universal Containers (UC) is using Active Directory as its corporate identity provider and Salesforce as its CRM for customer care agents, who use SAML based sign sign-on to login to Salesforce. The default agent profile does not include the Manage User permission. UC wants to dynamically update the agent role and permission sets.
Which two mechanisms are used to provision agents with the appropriate permissions? Choose 2 answers

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

Answer: BD

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

- Use Login Flow in System Context to update role and permission sets. A Login Flow is a custom post-authentication process that can be used to add additional screens or logic after a user logs in to Salesforce. A System Context is a mode that allows a Login Flow to run as an administrator user with full access to Salesforce data and metadata. By using a Login Flow in System Context, the identity architect can update the agent role and permission sets based on the information from Active Directory or other criteria.
- Use SAML Just-in-Time (JIT) handler class run as an admin user to update role and permission sets. A SAML JIT handler class is a class that implements the Auth.SamlJitHandler interface and defines how to handle SAML assertions for Just-in-Time (JIT) provisioning. JIT provisioning is a feature that allows Salesforce to create or update user records on the fly when users log in through an external identity provider. By using a SAML JIT handler class run as an admin user, the identity architect can update the agent role and permission sets based on the information from the SAML assertion. References: Login Flows, SAML Just-in-Time Provisioning, Auth.SamlJitHandler Interface

NEW QUESTION 164
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 169
Universal containers (UC) has implemented SAML -based single Sign-on for their salesforce application. UC is using PingFederate as the Identity provider. To access salesforce, Users usually navigate to a bookmarked link to my domain URL. What type of single Sign-on is this?

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

Answer: A

Explanation:
The type of single sign-on that UC is using is SP-initiated, which means that the service provider (Salesforce) initiates the SSO process by sending a SAML request to the identity provider (PingFederate) when the user navigates to the My Domain URL3. Therefore, option A is the correct answer. References: SAML SSO with Salesforce as the Service Provider

NEW QUESTION 173
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

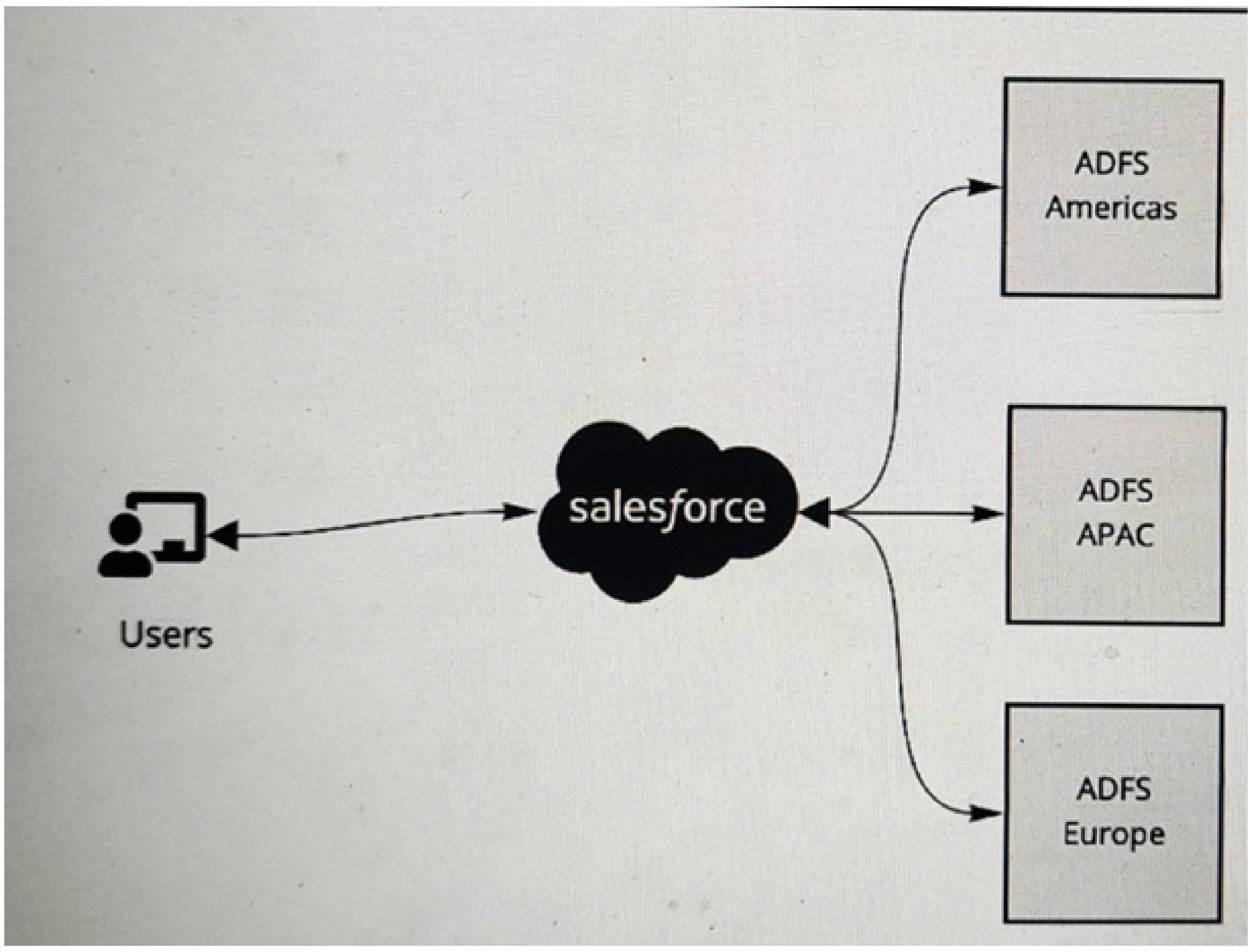
Answer: AC

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 178

Refer to the exhibit.



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

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

Answer: B

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

NEW QUESTION 180

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

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

Answer: C

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

NEW QUESTION 181

Universal Containers (UC) has an existing e-commerce platform and is implementing a new customer community. They do not want to force customers to register on both applications due to concern over the customers experience. It is expected that 25% of the e-commerce customers will utilize the customer community .
The e-commerce platform is capable of generating SAML responses and has an existing
REST-ful API capable of managing users. How should UC create the identities of its e-commerce users with the customer community?

A. Use SAML JIT in the Customer Community to create users when a user tries to login to the community from the e-commerce site.
B. Use the e-commerce REST API to create users when a user self-register on the customer community and use SAML to allow SSO.
C. Use a nightly batch ETL job to sync users between the Customer Community and the e-commerce platform and use SAML to allow SSO.
D. Use the standard Salesforce API to create users in the Community When a User is Created in the e-Commerce platform and use SAML to allow SSO.

Answer: A

Explanation:
The best option for UC to create the identities of its e-commerce users with the customer community is to use SAML JIT in the customer community to create users when a user tries to login to the community from the e-commerce site. SAML JIT (Just-in-Time) is a feature that allows Salesforce to create or update user accounts based on the information provided in a SAML assertion from an identity provider (IdP). This feature enables UC to avoid duplicating user registration on both applications and provide a seamless single sign-on (SSO) experience for its customers. The other options are not optimal for this scenario. Using the e-commerce REST API to create users when a user self-registers on the customer community would require the user to register twice, once on the e-commerce site and once on the customer community, which would degrade the customer experience. Using a nightly batch ETL job to sync users between the customer community and the e-c ommerce platform would introduce a delay in user creation and synchronization, which could cause errors or inconsistencies. Using the standard Salesforce API to create users in the community when a user is created in the e-commerce platform would require UC to write custom code and maintain API integration, which could increase complexity and cost. References: [Just-in-Time Provisioning for SAML], [Single Sign-On], [SAML SSO Flows]

NEW QUESTION 182
Universal Containers (UC) wants to implement SAML SSO for their internal of Salesforce users using a third-party IdP. After some evaluation, UC decides NOT to 65« set up My Domain for their Salesforce org. How does that decision impact their SSO implementation?

A. IdP-initiated SSO will NOT work.
B. Neither SP- nor IdP-initiated SSO will work.
C. Either SP- or IdP-initiated SSO will work.
D. SP-initiated SSO will NOT work

Answer: D

Explanation:
This is because without My Domain, Salesforce will not know in advance what Identity Provider (IdP) to use for SSO, since it does not even know yet what Organization the user is trying to log in to1. SP-initiated SSO is the scenario where the user starts with a Salesforce link (login page, deep link, Outlook Sync URL, etc.) and then gets redirected to the IdP for authentication2. Without My Domain, SP-initiated SSO requires that the user do an IdP-initiated SSO at least once first so that Salesforce can set a cookie in their browser identifying the IdP1. The other options are not correct for this question because:
- IdP-initiated SSO will work without My Domain, as long as the user starts SSO at the IdP and sends the identity information to Salesforce along with SAML protocol information that identifies the Organization and the IdP2.
- Neither SP- nor IdP-initiated SSO will not work is false, as explained above.
- Either SP- or IdP-initiated SSO will work is false, as explained above.

References: Considerations for setting up My Domain and SSO - Salesforce, SAML SSO with Salesforce as the Service Provider

NEW QUESTION 187
Universal containers (UC) would like to enable SAML-BASED SSO for a salesforce partner community. UC has an existing ldap identity store and a third-party portal. They would like to use the existing portal as the primary site these users' access, but also want to allow seamless access to the partner community. What SSO flow should an architect recommend?

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

Answer: B

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

NEW QUESTION 191
Universal Containers allows employees to use a mobile device to access Salesforce for daily operations using a hybrid mobile app. This app uses Mobile software development kits (SDK), leverages refresh token to regenerate access token when required and is distributed as a private app.
The chief security officer is rolling out an org wide compliance policy to enforce re-verification of devices if an employee has not logged in from that device in the last week.
Which connected app setting should be leveraged to comply with this policy change?

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

Answer: B

Explanation:
Refresh Token Policy - Expire the refresh token if it has not been used for 7 days is the connected app setting that should be leveraged to comply with the policy

change. This setting ensures that users have to re-verify their devices if they have not logged in from that device in the last week. The other settings are either not relevant or not effective for this scenario. References: Connected App Basics, OAuth 2.0 Refresh Token Flow

NEW QUESTION 192
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 194
Universal containers(UC) has decided to build a new, highly sensitive application on Force.com platform. The security team at UC has decided that they want users to provide a fingerprint in addition to username/Password to authenticate to this application. How can an architect support fingerprint as a form of identification for salesforce Authentication?

A. Use salesforce Two-factor Authentication with callouts to a third-party fingerprint scanning application.
B. Use Delegated Authentication with callouts to a third-party fingerprint scanning application.
C. Use an AppExchange product that does fingerprint scanning with native salesforce identity confirmation.
D. Use custom login flows with callouts to a third-party fingerprint scanning application.

Answer: D

Explanation:
D is correct because using custom login flows with callouts to a third-party fingerprint scanning application allows UC to support fingerprints as a form of identification for Salesforce authentication. Custom login flows allow UC to implement custom logic and UI elements for authentication, such as calling an external web service that performs fingerprint scanning and verification. A is incorrect because using Salesforce two-factor authentication with callouts to a third-party fingerprint scanning application does not support fingerprints as a form of identification for Salesforce authentication. Salesforce two-factor authentication requires users to enter a verification code or use an app like Salesforce Authenticator, not a fingerprint. B is incorrect because using delegated authentication with callouts to a third-party fingerprint scanning application does not support fingerprints as a form of identification for Salesforce authentication. Delegated authentication requires users to enter their username and password, not a fingerprint. C is incorrect because using an AppExchange product that does fingerprint scanning with native Salesforce identity confirmation does not support fingerprints as a form of identification for Salesforce authentication. AppExchange products are third-party applications that integrate with Salesforce, not native Salesforce features. Verified References: [Custom Login Flows],
[Two-Factor Authentication], [Delegated Authentication], [AppExchange]

NEW QUESTION 198
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 OpenlD 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

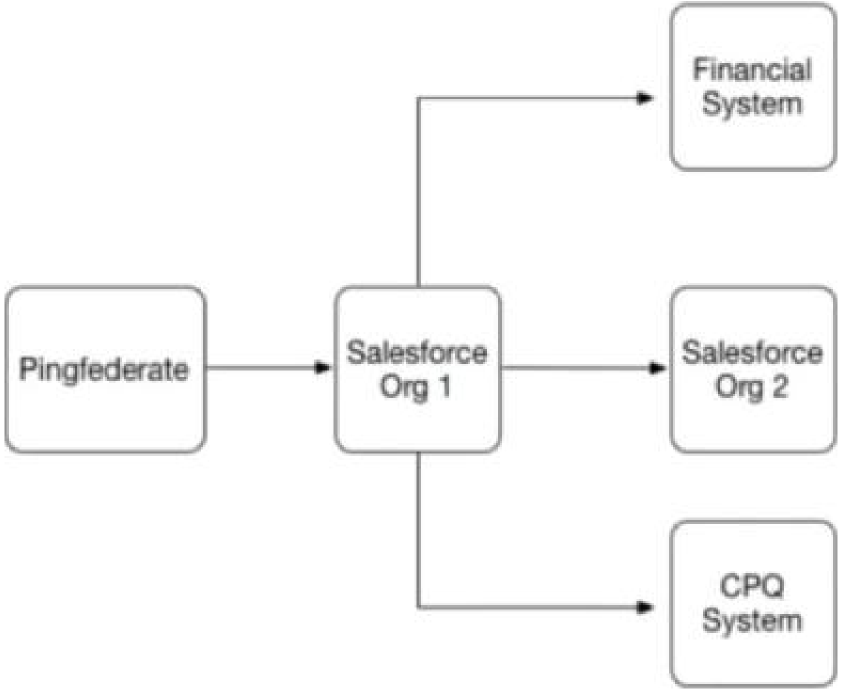
NEW QUESTION 199
Universal containers (UC) would like to enable self - registration for their salesforce partner community users. UC wants to capture some custom data elements from the partner user, and based on these data elements, wants to assign the appropriate profile and account values. Which two 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 201
Universal Containers (UC) has implemented SAML-based Single Sign-On to provide seamless access to its Salesforce Orgs, financial system, and CPQ system. Below is the SSO implementation landscape.



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

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

Answer: B

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

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

NEW QUESTION 205
Universal Containers (UC) is considering a Customer 360 initiative to gain a single source of the truth for its customer data across disparate systems and services.
UC wants to understand the primary benefits of Customer 360 Identity and how it contributes ato successful Customer 360 Truth project.
What are two are key benefits of Customer 360 Identity as it relates to Customer 360? Choose 2 answers

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

Answer: BC

Explanation:
Customer 360 Identity is a cloud-based identity service that provides a single, trusted identity for customers across all your digital properties and applications2. Customer 360 Identity has several benefits that relate to Customer 360, such as3:

- Customer 360 Identity enables an organization to build a single login for each of its customers, giving the organization an understanding of the user's login activity across all its digital properties and applications. This helps to create a unified customer profile and deliver personalized experiences based on user preferences and behaviors3.
- Customer 360 Identity supports multiple brands so you can deliver centralized identity services and correlation of user activity, even if it spans multiple corporate brands and user experiences. This helps to maintain brand consistency and loyalty while providing seamless access to your products and services3.

References:

- Customer 360 Identity
- Customer 360 Identity Benefits

NEW QUESTION 208
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 209
Northern Trail Outfitters (NTO) wants to give customers the ability to submit and manage issues with their purchases. It is important for NTO to give its customers the ability to login with their Amazon credentials.
What should an identity architect recommend to meet these requirements?

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

Answer: C

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

NEW QUESTION 212
Universal Containers wants to implement Single Sign-on for a Salesforce org using an external Identity Provider and corporate identity store.
What type of authentication flow is required to support deep linking'

A. Web Server OAuth SSO flow
B. Service-Provider-Initiated SSO
C. Identity-Provider-initiated SSO
D. StartURL on Identity Provider

Answer: B

Explanation:
Single sign-on (SSO) is an authentication method that enables users to access multiple applications with one login and one set of credentials4. There are two types of SSO flows that can be used with Salesforce as the service provider (SP) and an external identity provider (IdP)5:

- Service-provider-initiated SSO: The user requests a resource from the SP, such as a Salesforce URL. The SP redirects the user to the IdP for authentication. The IdP authenticates the user and sends a SAML response to the SP. The SP validates the SAML response and grants access to the user5. This type of SSO flow supports deep linking, which means that the user can access a specific page within Salesforce without logging in again6.
- Identity-provider-initiated SSO: The user logs in to the IdP and selects an app from a list of available apps. The IdP sends a SAML response to the SP. The SP validates the SAML response and grants access to the user5. This type of SSO flow does not support deep linking, which means that the user can only access the default landing page of Salesforce6.

References:

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

NEW QUESTION 213
Universal Containers (UC) has a Customer Community that uses Facebook for of authentication. UC would like to ensure that changes in the Facebook profile are 65. reflected on the appropriate Customer Community user. How can this requirement be met?

A. Use SAML Just-In-Time Provisioning between Facebook and Salesforce.
B. Use information in the Signed Request that is received from Facebook.
C. Develop a scheduled job that calls out to Facebook on a nightly basis.
D. Use the update User () method on the Registration Handler class.

Answer: D

Explanation:
The update User() method on the Registration Handler class is used to update the Salesforce user record with information from the Facebook profile, such as name, email, and photo1. This method is invoked every time a user logs in to Salesforce using Facebook credentials2. The other options are not suitable for this requirement because:

- SAML Just-In-Time Provisioning is used to create or update users in Salesforce based on SAML assertions from an identity provider3. Facebook does not support SAML as an identity provider.

- The Signed Request is a parameter that contains information about the user who is logging in to Salesforce via Facebook. It does not contain the user’s profile information, such as name, email, or photo.
- A scheduled job that calls out to Facebook on a nightly basis would not reflect the changes in the Facebook profile in real time, as the requirement states. It would also require storing the user’s Facebook access token and making API calls to Facebook, which could be inefficient and insecure. References: Set Up Social Sign-On, Configure a Facebook Authentication Provider, SAML Just-in-Time Provisioning, [Facebook as a SAML Identity Provider], [Facebook Login for Apps - Signed Request], [Facebook Login for Apps - Access Tokens], [Facebook Graph API - User]

NEW QUESTION 215

......