Identity-and-Access-Management-Architect Dumps

Salesforce Certified Identity and Access Management Architect (SU23)

https://www.certleader.com/Identity-and-Access-Management-Architect-dumps.html
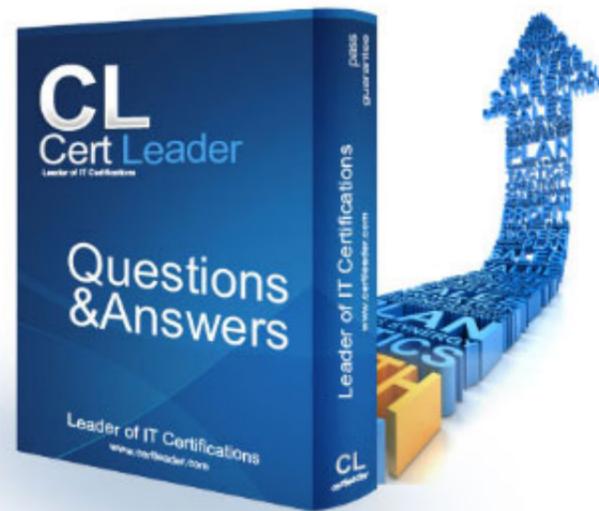
NEW QUESTION 1
Universal Containers (UC) is planning to deploy a custom mobile app that will allow users to get e-signatures from its customers on their mobile devices. The mobile app connects to Salesforce to upload the e-signature as a file attachment and uses OAuth protocol for both authentication and authorization. What is the most recommended and secure OAuth scope setting that an Architect should recommend?

A. Id
B. Web
C. Api
D. Custom_permissions

Answer: D

Explanation:
The most recommended and secure OAuth scope setting for UC's custom mobile app is custom_permissions. 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 can also be used as OAuth scopes to limit the access of an external application, such as UC's mobile app, to certain custom features or functionalities in Salesforce. By configuring custom_permissions as OAuth scopes in the connected app settings, UC can restrict the mobile app access to only the e-signature feature and protect against unauthorized or excessive access.
The other options are not recommended or secure OAuth scope settings for UC's custom mobile app. Id is an OAuth scope that allows the mobile app to access basic information about the user and their org, such as name, email, profile picture, and instance URL. This scope does not provide any access to Salesforce data or features, such as uploading e-signatures. Web is an OAuth scope that allows the mobile app to access Salesforce data and features through a browser or web-view. This scope provides full access to Salesforce data and features, which could expose sensitive information or allow unwanted actions. Api is an OAuth scope that allows the mobile app to make REST or SOAP API calls to Salesforce using the access token. This scope also provides full access to Salesforce data and features, which could compromise security and compliance. References: [OAuth Scopes], [Connected Apps], [Custom Permissions]

NEW QUESTION 2
A Salesforce customer is implementing Sales Cloud and a custom pricing application for its call center agents. An Enterprise single sign-on solution is used to authenticate and sign-in users to all applications. The customer has the following requirements:
* 1. The development team has decided to use a Canvas app to expose the pricing application to agents.
* 2. Agents should be able to access the Canvas app without needing to log in to the pricing application.
Which two options should the identity architect consider to provide support for the Canvas app to initiate login for users?
Choose 2 answers

A. Select "Enable as a Canvas Personal App" in the connected app settings.
B. Enable OAuth settings in the connected app with required OAuth scopes for the pricing application.
C. Configure the Canvas app as a connected app and set Admin-approved users as pre-authorized.
D. Enable SAML in the connected app and Security Assertion Markup Language (SAML) Initiation Method as Service Provider Initiated.

Answer: CD

Explanation:
To allow agents to access the Canvas app without needing to log in to the pricing application, the identity architect should consider two options:

> Configure the Canvas app as a connected app and set Admin-approved users as pre-authorized. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols. A Canvas app is a type of connected app that allows an external application to be embedded within Salesforce. By setting Admin-approved users as pre-authorized, the identity architect can control which users can access the Canvas app by assigning profiles or permission sets to the connected app.

> Enable SAML in the connected app and Security Assertion Markup Language (SAML) Initiation Method as Service Provider Initiated. SAML is a protocol that allows users to authenticate and authorize with an external identity provider and access Salesforce resources. By enabling SAML in the connected app, the identity architect can use Salesforce as a service provider (SP) and the pricing application as an identity provider (IdP) for single sign-on (SSO). By setting SAML Initiation Method as Service Provider Initiated, the identity architect can initiate the SSO process from Salesforce and send a SAML request to the pricing application.
References: Connected Apps, Canvas Apps, SAML Single Sign-On Settings

NEW QUESTION 3
Universal Containers (UC) wants to integrate a third-party Reward Calculation system with Salesforce to calculate Rewards. Rewards will be calculated on a schedule basis and update back into Salesforce. The integration between Salesforce and the Reward Calculation System needs to be secure. Which are two recommended practices for using OAuth flow in this scenario. choose 2 answers

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

Answer: CD

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

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

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

NEW QUESTION 4

Northern Trail Outfitters (NTO) uses Salesforce for Sales Opportunity Management. Okta was recently brought in to Just-in-Time (JIT) provision and authenticate NTO users to applications. Salesforce users also use Okta to authorize a Forecasting web application to access Salesforce records on their behalf.

Which two roles are being performed by Salesforce? Choose 2 answers

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

Answer: BD

Explanation:

Salesforce acts as an OAuth client when it uses Okta to authorize a Forecasting web application to access
Salesforce records on behalf of the user. Salesforce acts as a SAML service provider when it accepts SAML assertions from Okta to authenticate NTO users.
References: OAuth 2.0 Web Server Authentication
Flow, SAML Single Sign-On Overview

NEW QUESTION 5

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 6

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 7

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 8

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

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

Answer: C

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

NEW QUESTION 9
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 10
An identity architect has built a native mobile application and plans to integrate it with a Salesforce Identity solution. The following are the requirements for the solution:
* 1. Users should not have to login every time they use the app.
* 2. The app should be able to make calls to the Salesforce REST API.
* 3. End users should NOT see the OAuth approval page.
How should the identity architect configure the Salesforce connected app to meet the requirements?

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

Answer: A

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

NEW QUESTION 10
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 11
Universal Containers (UC) uses a home-grown Employee portal for their employees to collaborate. UC decides to use Salesforce Ideas to allow employees to post Ideas from the Employee portal. When users click on some of the links in the Employee portal, the users should be redirected to Salesforce, authenticated, and presented with the relevant pages. What OAuth flow is best suited for this scenario?

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

Answer: D

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

NEW QUESTION 14
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 18
A web service is developed that allows secure access to customer order status on the Salesforce Platform. The service connects to Salesforce through a connected app with the web server flow. The following are the required actions for the authorization flow:
* 1. User Authenticates and Authorizes Access
* 2. Request an Access Token
* 3. Salesforce Grants an Access Token
* 4. Request an Authorization Code
* 5. Salesforce Grants Authorization Code
What is the correct sequence for the authorization flow?

A. 1, 4, 5, 2, 3
B. 4, 1, 5, 2, 3
C. 2, 1, 3, 4, 5
D. 4,5,2, 3, 1

Answer: B

Explanation:
The web server flow is an OAuth 2.0 authorization code grant type, which follows this sequence of steps:
- The client app requests an authorization code from Salesforce by redirecting the user to the authorization endpoint.
- The user authenticates and authorizes access to the client app.
- Salesforce grants an authorization code and redirects the user back to the client app.
- The client app requests an access token from Salesforce by sending the authorization code to the token endpoint.
- Salesforce grants an access token and a refresh token to the client app. References: OAuth Authorization Flows, Authorize Apps with OAuth

NEW QUESTION 22
Which two are valid choices for digital certificates when setting up two-way SSL between Salesforce and an external system. Choose 2 answers

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

Answer: CD

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

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

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

NEW QUESTION 25
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 26
Northern Trail Outfitters (NTO) wants to give customers the ability to submit and manage issues with their purchases. It is important for to give its customers the ability to login with their Facebook and Twitter credentials.
Which two actions should an identity architect recommend to meet these requirements? Choose 2 answers

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

Answer: BD

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

NEW QUESTION 29
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 34
An insurance company has a connected app in its Salesforce environment that is used to integrate with a Google Workspace (formerly knot as G Suite).
An identity and access management (IAM) architect has been asked to implement automation to enable users, freeze/suspend users, disable users, and reactivate existing users in Google Workspace upon similar actions in Salesforce.
Which solution is recommended to meet this requirement?

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

Answer: A

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

NEW QUESTION 37
Universal containers (UC) has built a custom based Two-factor Authentication (2fa) system for their existing on-premise applications. Thru are now implementing salesforce and would like to enable a Two-factor login process for it, as well. What is the recommended solution an architect should consider?

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

Answer: D

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

NEW QUESTION 40
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 43
Which tool should be used to track login data, such as the average number of logins, who logged in more than the average number of times and who logged in during non-business hours?

A. Login Inspector
B. Login History
C. Login Report
D. Login Forensics

Answer: D

Explanation:
To track login data, such as the average number of logins, who logged in more than the average number of times and who logged in during non-business hours, the identity architect should use Login Forensics. Login Forensics is a tool that analyzes login data and provides insights into user behavior and login patterns. Login Forensics can help identify anomalies, risks, and trends in user login activity. Login Forensics can also generate reports and dashboards to visualize the login data. References: Login Forensics, Analyze Login Data with Login Forensics

NEW QUESTION 44
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 47
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 51
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 handler 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 55
A global company has built an external application that uses data from its Salesforce org via an OAuth 2.0 authorization flow. Upon logout, the existing Salesforce OAuth token must be invalidated.
Which action will accomplish this?

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

Answer: C

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

NEW QUESTION 58
Which two security risks can be mitigated by enabling Two-Factor Authentication (2FA) in Salesforce? Choose 2 answers

A. Users leaving laptops unattended and not logging out of Salesforce.
B. Users accessing Salesforce from a public Wi-Fi access point.
C. Users choosing passwords that are the same as their Facebook password.
D. Users creating simple-to-guess password reset questions.

Answer: BC

Explanation:
Enabling Two-Factor Authentication (2FA) in Salesforce can mitigate the security risks of users accessing Salesforce from a public Wi-Fi access point or choosing passwords that are the same as their Facebook password. 2FA is an additional layer of protection beyond your password that requires users to verify their identity with another factor, such as a mobile app, a security key, or a verification code. This can prevent unauthorized access even if the user's password is compromised

or guessed by a malicious actor. The other options are not directly related to 2FA, but rather to user behavior or password policies.

NEW QUESTION 61
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 63
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 66
A manufacturer wants to provide registration for an Internet of Things (IoT) device with limited display input or capabilities.
Which Salesforce OAuth authorization flow should be used?

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

Answer: B

Explanation:
The OAuth 2.0 Device Flow is a type of authorization flow that allows users to register an IoT device with limited display input or capabilities, such as a smart TV, a printer, or a smart speaker1. The device flow works as follows1:
- The device displays or reads out a verification code and a verification URL to the user.
- The user visits the verification URL on another device, such as a smartphone or a laptop, and enters the verification code.
- The user logs in to Salesforce and approves the device.
- The device polls Salesforce for an access token using the verification code.
- Salesforce returns an access token to the device, which can then access Salesforce APIs.
References:
- OAuth 2.0 Device Flow

NEW QUESTION 68
A multinational industrial products manufacturer is planning to implement Salesforce CRM to manage their business. They have the following requirements:
* 1. They plan to implement Partner communities to provide access to their partner network .
* 2. They have operations in multiple countries and are planning to implement multiple Salesforce orgs.
* 3. Some of their partners do business in multiple countries and will need information from multiple Salesforce communities.
* 4. They would like to provide a single login for their partners.
How should an Identity Architect solution this requirement with limited custom development?

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

Answer: A

Explanation:

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

NEW QUESTION 73
Universal Containers wants to allow its customers to log in to its Experience Cloud via a third-party authentication provider that supports only the OAuth protocol.
What should an identity architect do to fulfill this requirement?

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

Answer: B

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

NEW QUESTION 76
Universal Containers (UC) is rolling out its new Customer Identity and Access Management Solution built on top of its existing Salesforce instance. UC wants to allow customers to login using Facebook, Google, and other social sign-on providers.
How should this functionality be enabled for UC, assuming ail social sign-on providers support OpenID Connect?

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

Answer: A

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

NEW QUESTION 81
The security team at Universal containers(UC) has identified exporting reports as a high-risk action and would like to require users to be logged into salesforce with their active directory (AD) credentials when doing so. For all other uses of Salesforce, Users should be allowed to use AD credentials or salesforce credentials. What solution should be recommended to prevent exporting reports except when logged in using AD credentials while maintaining the ability to view reports when logged in with salesforce credentials?

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

Answer: B

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

NEW QUESTION 85
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 88

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

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

Answer: CD

Explanation:

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

NEW QUESTION 92

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 95

Universal Containers (UC) has built a custom token-based Two-factor authentication (2FA) system for their existing on-premise applications. They are now implementing Salesforce and would like to enable a
Two-factor login process for it, as well. What is the recommended solution as Architect should consider?

A. Use the custom 2FA system for on-premise applications and native 2FA for Salesforce.
B. Replace the custom 2FA system with an AppExchange App that supports on premise application and salesforce.
C. Use Custom Login Flows to connect to the existing custom 2FA system for use in Salesforce.
D. Replace the custom 2FA system with Salesforce 2FA for on-premise applications and Salesforce.

Answer: D

Explanation:

The recommended solution for UC to enable a two-factor login process for Salesforce and their existing
on-premise applications is to replace the custom 2FA system with Salesforce 2FA for on-premise applications and Salesforce. Salesforce 2FA is a feature that 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. Salesforce 2FA can be enabled for both Salesforce and on-premise applications by using one of the following methods:

➤ Use Salesforce Authenticator, a mobile app that generates verification codes or sends push notifications to users' devices.

➤ Use a third-party authenticator app, such as Google Authenticator or Microsoft Authenticator, that generates verification codes based on a shared secret key.

➤ Use a verification code sent by email or SMS to users' registered email address or phone number.

➤ Use a U2F security key, such as YubiKey, that plugs into users' devices and provides a physical token. By replacing the custom 2FA system with Salesforce 2FA, UC can benefit from the following advantages:

➤ Improved security and compliance by using a standard and proven 2FA solution that protects against
phishing, credential theft, and brute force attacks.

➤ Reduced complexity and cost by eliminating the need to maintain a custom 2FA system and integrating it with Salesforce.

➤ Enhanced user experience and convenience by providing multiple options for verifying identity and allowing users to remember trusted devices or browsers.
The other options are not recommended solutions for this scenario. Using the custom 2FA system for
on-premise applications and native 2FA for Salesforce would create inconsistency and confusion for users who have to use different methods of verification for

different applications. Replacing the custom 2FA system with an AppExchange app that supports on-premise applications and Salesforce would require UC to find an app that meets their specific needs and pay for its license and maintenance. Using custom login flows to connect to the existing custom 2FA system for use in Salesforce would require UC to write custom code and logic to invoke the custom 2FA system from Salesforce, which could introduce security and performance issues. References: [Two-Factor Authentication], [Salesforce Authenticator], [Third-Party Authenticator Apps], [Verification Code via Email or SMS], [U2F Security Keys], [Custom Login Flows]

NEW QUESTION 99
Universal containers (UC) wants to integrate a Web application with salesforce. The UC team has implemented the Oauth web-server Authentication flow for authentication process. Which two considerations should an architect point out to UC? Choose 2 answers

A. The web application should be hosted on a secure server.
B. The web server must be able to protect consumer privacy
C. The flow involves passing the user credentials back and forth.
D. The flow will not provide an Oauth refresh token back to the server.

Answer: AB

Explanation:
The web application should be hosted on a secure server and the web server must be able to protect consumer privacy are two considerations that an architect should point out to UC. To integrate an external web app with the Salesforce API, UC can use the OAuth 2.0 web server flow, which implements the OAuth 2.0 authorization code grant type4. With this flow, the server hosting the web app must be able to protect the connected app's identity, defined by the client ID and client secret4. The web application should be hosted on a secure server to ensure that the communication between the web app and Salesforce is encrypted and protected from unauthorized access or tampering6. The web server must be able to protect consumer privacy to comply with data protection laws and regulations, such as GDPR or CCPA . The web server should implement best practices for storing and handling user data, such as encryption, hashing, salting, and anonymization. The flow involves passing the user credentials back and forth is not a correct consideration, as the web server flow does not require the user credentials to be passed between the web app and Salesforce. Instead, it uses an authorization code that is exchanged for an access token and a refresh token4. The flow will not provide an OAuth refresh token back to the server is also not a correct consideration as the web server flow does provide a refresh token that can be used to obtain new access tokens without user interaction4. References: OAuth 2.0 Web Server Flow for Web App Integration, Secure Your Web Application, [General Data Protection Regulation (GDPR)], [California Consumer Privacy Act (CCPA)], [Data Protection Best Practices]

NEW QUESTION 104
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 105
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 107
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 109
Universal Containers wants to secure its Salesforce APIs by using an existing Security Assertion Markup Language (SAML) configuration supports the company's single sign-on process to Salesforce,
Which Salesforce OAuth authorization flow should be used?

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

Answer: A

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

NEW QUESTION 114
Universal Containers is implementing Salesforce Identity to broker authentication from its enterprise single sign-on (SSO) solution through Salesforce to third party applications using SAML.
What rote does Salesforce Identity play in its relationship with the enterprise SSO system?

A. Identity Provider (IdP)
B. Resource Server
C. Service Provider (SP)
D. Client Application

Answer: C

Explanation:
To broker authentication from its enterprise SSO solution through Salesforce to third party applications using SAML, Salesforce Identity plays the role of a Service Provider (SP). A SP is an entity that relies on an Identity Provider (IdP) to authenticate and authorize users. In this scenario, the enterprise SSO solution is the IdP, Salesforce is the SP, and the third party applications are the Resource Servers or Client Applications. The SP receives a SAML assertion from the IdP and uses it to obtain an access token from the Resource Server or Client Application. References: SAML Single Sign-On Settings, Authorize Apps with OAuth

NEW QUESTION 117
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 122
How should an Architect force user to authenticate with Two-factor Authentication (2FA) for Salesforce only when not connected to an internal company network?

A. Use Custom Login Flows with Apex to detect the user's IP address and prompt for 2FA if needed.

B. Add the list of company's network IP addresses to the Login Range list under 2FA Setup.
C. Use an Apex Trigger on the UserLogin object to detect the user's IP address and prompt for 2FA if needed.
D. Apply the "Two-factor Authentication for User Interface Logins" permission and Login IP Ranges for all Profiles.

Answer: A

Explanation:
Using Custom Login Flows with Apex is the best option to force users to authenticate with 2FA for Salesforce only when not connected to an internal company network. Custom Login Flows allow admins to customize the login process for different scenarios and user types2. Apex code can be used to detect the user's IP address and prompt for 2FA if it is not within the company's network range3. The other options are not suitable because they either do not support 2FA or do not allow conditional logic based on the user's IP address.

NEW QUESTION 124
Universal Containers would like its customers to register and log in to a portal built on Salesforce Experience Cloud. Customers should be able to use their Facebook or LinkedIn credentials for ease of use.
Which three steps should an identity architect take to implement social sign-on? Choose 3 answers

A. Register both Facebook and LinkedIn as connected apps.
B. Create authentication providers for both Facebook and LinkedIn.
C. Check "Facebook" and "LinkedIn" under Login Page Setup.
D. Enable "Federated Single Sign-On Using SAML".
E. Update the default registration handlers to create and update users.

Answer: BCE

Explanation:
To implement social sign-on for customers to register and log in to a portal built on Salesforce Experience Cloud using their Facebook or LinkedIn credentials, the identity architect should take three steps:

≫ Create authentication providers for both Facebook and LinkedIn. Authentication providers are configurations that enable users to authenticate with an external identity provider and access Salesforce resources. Salesforce provides predefined authentication providers for some common identity providers, such as Facebook and LinkedIn, which can be easily configured with minimal customization.

≫ Check "Facebook" and "LinkedIn" under Login Page Setup. Login Page Setup is a setting that allows administrators to customize the login page for Experience Cloud sites. By checking "Facebook" and "LinkedIn", the identity architect can enable social sign-on buttons for these identity providers on the login page.

≫ Update the default registration handlers to create and update users. Registration handlers are classes that implement the Auth.RegistrationHandler interface and define how to create or update users in Salesforce based on the information from the external identity provider. The identity architect can update the default registration handlers to link the user's social identity with their Salesforce identity and prevent duplicate accounts. References: Authentication Providers, Social Sign-On with Authentication Providers, Login Page Setup, Create a Custom Registration Handler

NEW QUESTION 125
Universal Containers (UC) has an existing Salesforce org configured for SP-Initiated SAML SSO with their Idp. A second Salesforce org is being introduced into the environment and the IT team would like to ensure they can use the same Idp for new org. What action should the IT team take while implementing the second org?

A. Use the same SAML Identity location as the first org.
B. Use a different Entity ID than the first org.
C. Use the same request bindings as the first org.
D. Use the Salesforce Username as the SAML Identity Type.

Answer: B

Explanation:
The Entity ID is a unique identifier for a service provider or an identity provider in SAML SSO. It is used to differentiate between different service providers or identity providers that may share the same issuer or login URL. In Salesforce, the Entity ID is automatically generated based on the organization ID and can be viewed in the Single Sign-On Settings page1. If you have a custom domain set up, you can use https:// [customDomain].my.salesforce.com as the Entity ID2. If you want to use the same IdP for two Salesforce orgs, you need to use different Entity IDs for each org, otherwise the IdP will not be able to distinguish them and may send incorrect assertions. You can also use different certificates, issuers, or login URLs for each org, but using different Entity IDs is the simplest and recommended way3.

NEW QUESTION 129
Universal containers (UC) wants to implement Delegated Authentication for a certain subset of Salesforce users. Which three items should UC take into consideration while building the Web service to handle the Delegated Authentication request? Choose 3 answers

A. The web service needs to include Source IP as a method parameter.
B. UC should whitelist all salesforce ip ranges on their corporate firewall.
C. The web service can be written using either the soap or rest protocol.
D. Delegated Authentication is enabled for the system administrator profile.
E. The return type of the Web service method should be a Boolean value

Answer: ABE

Explanation:
Delegated authentication is a feature that allows Salesforce to delegate the authentication process to an external web service. The web service needs to include the source IP address of the user as a method parameter, so that Salesforce can pass it along with the username and password. UC should whitelist all Salesforce IP ranges on their corporate firewall, so that the web service can accept requests from Salesforce. The return type of the web service method should be a Boolean value, indicating whether the authentication was successful or not. The web service can be written using either SOAP or REST protocol, but this is not a consideration for UC while building the web service. Delegated authentication is not enabled for the system administrator profile, but it can be enabled for other profiles or permission sets. References: Certification - Identity and Access Management Architect - Trailhead, [Delegated Authentication Single Sign-On], [Implementing Single Sign-On Across Multiple Organizations]

NEW QUESTION 132

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 133

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

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

Answer: B

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

NEW QUESTION 136

A global fitness equipment manufacturer uses Salesforce to manage its sales cycle. The manufacturer has a custom order fulfillment app that needs to request order data from Salesforce. The order fulfillment app needs to integrate with the Salesforce API using OAuth 2.0 protocol.
What should an identity architect use to fulfill this requirement?

A. Canvas App Integration
B. OAuth Tokens
C. Authentication Providers
D. Connected App and OAuth scopes

Answer: D

Explanation:
To integrate the order fulfillment app with the Salesforce API using OAuth 2.0 protocol, the identity architect should use a Connected App and OAuth scopes. A Connected App is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as OAuth 2.0. OAuth scopes are permissions that define the specific data that an external application can access or modify in Salesforce. To use OAuth 2.0 protocol, the identity architect needs to configure a Connected App in Salesforce and assign the appropriate OAuth scopes to it, such as "api" or "full". References: Connected Apps, OAuth Scopes

NEW QUESTION 140

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

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

Answer: AD

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

▷ Option A is correct because configuring SAML SSO settings involves specifying the identity provider details, such as the entity ID, login URL, logout URL, and certificate2.

≫ Option D is correct because setting up My Domain enables you to use a custom domain name for your Salesforce org and allows you to use SAML as an authentication method3.

≫ Option B is incorrect because creating a connected app is not necessary for SP-initiated SSO using a SAML-compliant IdP. A connected app is used for OAuth-based authentication or OpenID Connect-based authentication4.

≫ Option C is incorrect because configuring delegated authentication is not related to SP-initiated SSO using a SAML-compliant IdP. Delegated authentication is a feature that allows Salesforce to delegate user authentication to an external service, such as LDAP or Active Directory5.
References: SAML-based single sign-on: Configuration and Limitations, Configure SAML single
sign-on with an identity provider, My Domain, Create a Connected App, Configure Salesforce for Delegated Authentication

NEW QUESTION 141
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 145
Universal Containers (UC) rolling out a new Customer Identity and Access Management Solution will be built on top of their existing Salesforce instance. Several service providers have been setup and integrated with Salesforce using OpenID Connect to allow for a seamless single sign-on experience. UC has a requirement to limit user access to only a subset of service providers per customer type.
Which two steps should be done on the platform to satisfy the requirement? Choose 2 answers

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

Answer: CD

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

NEW QUESTION 149
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.
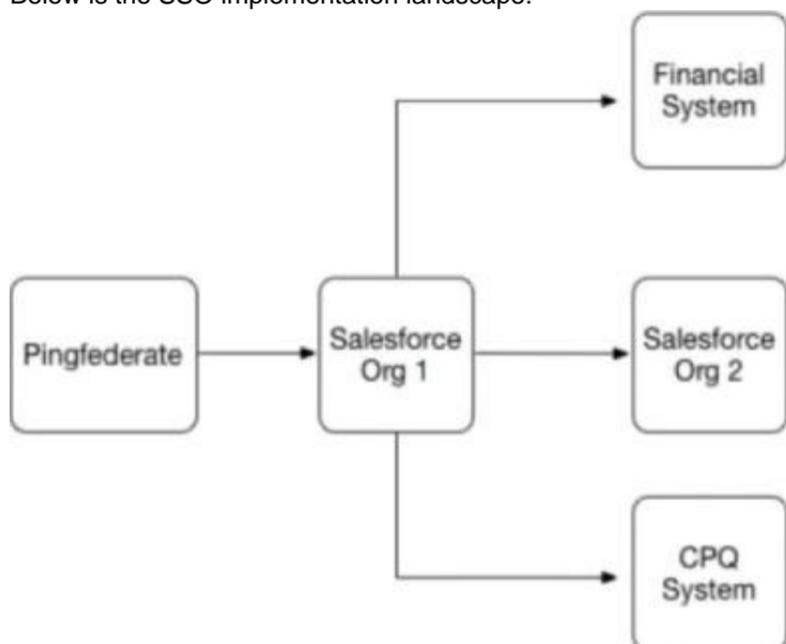
What role combination is represented by the systems in this scenario"

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 152
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 153
A client is planning to rollout multi-factor authentication (MFA) to its internal employees and wants to understand which authentication and verification methods meet the Salesforce criteria for secure authentication.
Which three functions meet the Salesforce criteria for secure mfa? Choose 3 answers

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

Answer: BCE

Explanation:
Multi-factor authentication (MFA) is a security feature that requires users to verify their identity with two or more factors when they log in to Salesforce4. Salesforce supports several types of authentication and verification methods that meet the criteria for secure MFA, such as5:
≫ Username and password + security key: A security key is a physical device that plugs into a USB port or connects wirelessly to your computer or mobile device. It generates a unique code that you use to verify your identity when you log in to Salesforce5.
≫ Third-party single sign-on with Mobile Authenticator app: Single sign-on (SSO) is an authentication method that allows users to access multiple applications with one login and one set of credentials. A mobile authenticator app is an app that generates temporary codes or sends push notifications that you use to verify your identity when you log in to Salesforce via SSO5.
≫ Lightning Login: Lightning Login is an authentication method that allows users to log in to Salesforce without entering a password. Instead, users scan a QR code with their mobile device or click an email
link that they receive when they try to log in. Then they use their fingerprint, face ID, or PIN to verify their identity on their mobile device5.
References:
≫ Multi-Factor Authentication
≫ Authentication and Verification Methods

NEW QUESTION 156
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 158
Universal Containers (UC) uses Salesforce for its customer service agents. UC has a proprietary system for order tracking which supports Security Assertion Markup Language (SAML) based single sign-on. The VP of customer service wants to ensure only active Salesforce users should be able to access the order tracking system which is only visible within Salesforce.
What should be done to fulfill the requirement? Choose 2 answers

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

Answer: AD

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

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

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

❯ [SAML Single Sign-On]

❯ [Set Up Your Domain as an Identity Provider]

❯ [Canvas Apps]

❯ [Create a Connected App for Your Canvas App]

❯ [IdP Initiated SAML Assertion POST Binding]

NEW QUESTION 162
Universal containers wants to set up SSO for a selected group of users to access external applications from salesforce through App launcher. Which three steps must be completed in salesforce to accomplish the goal?

A. Associate user profiles with the connected Apps.
B. Complete my domain and Identity provider setup.
C. Create connected apps for the external applications.
D. Complete single Sign-on settings in security controls.
E. Create named credentials for each external system.

Answer: ABC

Explanation:
To set up SSO for a selected group of users to access external applications from Salesforce through App Launcher, UC must complete the following steps in Salesforce:

❯ Associate user profiles with the connected apps. 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 Connect3. To access a connected app, users must have the appropriate permissions assigned to them, either through their profile or a permission set4. UC can associate user profiles with
the connected apps to control which users can access which apps.

❯ Complete My Domain and identity provider setup. My Domain is a feature that lets UC create a custom domain name for their Salesforce org. It is required for setting up SSO with external identity providers. An identity provider is a trusted system that authenticates users for other service providers. UC must set up an identity provider that supports SSO protocols such as SAML or OpenID Connect and configure it to communicate with Salesforce.

❯ Create connected apps for the external applications. UC must create connected apps for each external application that they want to access from Salesforce through App Launcher. A connected app defines the attributes of the external application, such as its name, logo, description, and callback URL4. It also specifies the SSO protocol and settings that are used to authenticate users and grant access tokens4.

❯ References: Learn About Connected Apps, Create a Connected App, [Set Up My Domain], Single Sign-On, [Identity Providers and Service Providers]

NEW QUESTION 165
Universal Containers (UC) would like its community users to be able to register and log in with Linkedin or Facebook Credentials. UC wants users to clearly see Facebook &Linkedin Icons when they register and login. What are the two recommended actions UC can take to achieve this Functionality? Choose 2 answers

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

Answer: AB

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

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

This action allows UC to configure Facebook and LinkedIn as authorization providers in Salesforce, which are external services that authenticate users and provide information about their identity and

attributes. By enabling these login options in the community configuration, UC can display Facebook and LinkedIn icons on the community login page and allow users to log in with their existing credentials from these services.

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

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

NEW QUESTION 166
How should an identity architect automate provisioning and deprovisioning of users into Salesforce from an external system?

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

Answer: C

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

NEW QUESTION 169
Universal containers (UC) has implemented a multi-org strategy and would like to centralize the management of their salesforce user profiles. What should the architect recommend to allow salesforce profiles to be managed from a central system of record?

A. Implement jit provisioning on the SAML IDP that will pass the profile id in each assertion.
B. Create an apex scheduled job in one org that will synchronize the other orgs profile.
C. Implement Delegated Authentication that will update the user profiles as necessary.
D. Implement an Oauthjwt flow to pass the profile credentials between systems.

Answer: A

Explanation:
To allow Salesforce profiles to be managed from a central system of record, the architect should recommend to implement JIT provisioning on the SAML IDP that will pass the profile ID in each assertion. JIT provisioning is a process that creates or updates user accounts on Salesforce based on information sent by an external identity provider (IDP) during SAML authentication. By passing the profile ID in each assertion, the IDP can control which profile is assigned to each user. Option B is not a good choice because creating an Apex scheduled job in one org that will synchronize the other orgs profile may not be scalable, reliable, or secure. Option C is not a good choice because implementing Delegated Authentication that will update the user profiles as necessary may not be feasible, as Delegated Authentication only verifies the user's credentials against an external service, but does not pass any other information to Salesforce. Option D is not a good choice because implementing an OAuth JWT flow to pass the profile credentials between systems may not be suitable, as OAuth JWT flow is used for server-to-server integration, not for user authentication.
References: Authorize Apps with OAuth, [Identity Management Concepts], [User Authentication]

NEW QUESTION 170
Universal Containers (UC) wants its closed Won opportunities to be synced to a Data Warehouse in near real time. UC has implemented Outbound Message to enable near real-time data sync. UC wants to ensure that communication between Salesforce and Target System is Secure. What Certificate is sent along with the Outbound Message?

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

Answer: A

Explanation:
The CA-Signed Certificate from the Certificate and Key Management menu is the certificate that is sent along with the outbound message. An outbound message is a SOAP message that is sent from Salesforce to an external endpoint when a workflow rule or approval process is triggered. To ensure that the communication between Salesforce and the target system is secure, the outbound message can be signed with a certificate that is generated or uploaded in the Certificate and Key Management menu. The certificate must be CA-Signed, which means that it is issued by a trusted certificate authority (CA) that verifies the identity of the sender. The other options are not valid certificates for this purpose. The default client certificate from the Develop–> API Menu is a self-signed certificate that is used for testing purposes only and does not provide adequate security. The default client certificate or a certificate from Certificate and Key Management menu is

too vague and does not specify whether the certificate is CA-Signed or self-signed. The self-signed certificates from the Certificate & Key Management menu are certificates that are generated by Salesforce without any verification by a CA, and they are not recommended for production use.
References: [Outbound Messages], [Sign Outbound Messages with a Certificate], [CA-Signed Certificates], [Default Client Certificate], [Self-Signed Certificates]

NEW QUESTION 172
Universal Containers (UC) has Active Directory (AD) as their enterprise identity store and would like to use it for Salesforce user authentication. UC expects to synchronize user data between Salesforce and AD and Assign the appropriate Profile and Permission Sets based on AD group membership. What would be the optimal way to implement SSO?

A. Use Active Directory with Reverse Proxy as the Identity Provider.
B. Use Microsoft Access control Service as the Authentication provider.
C. Use Active Directory Federation Service (ADFS) as the Identity Provider.
D. Use Salesforce Identity Connect as the Identity Provider.

Answer: D

Explanation:
The optimal way to implement SSO with Active Directory as the enterprise identity store is to use Salesforce Identity Connect as the identity provider. Salesforce Identity Connect is a software that integrates Microsoft Active Directory with Salesforce and enables single sign-on (SSO) using SAML. It also allows user data synchronization between Active Directory and Salesforce and profile and permission set assignment based on Active Directory group membership. Option A is not a good choice because using Active Directory with reverse proxy as the identity provider may not be supported by Salesforce or may require additional configuration and customization. Option B is not a good choice because using Microsoft Access Control Service as the authentication provider may not be available, as Microsoft has retired this service in 2018. Option C is not a good choice because using Active Directory Federation Service (ADFS) as the identity provider may not allow user data synchronization or profile and permission set assignment based on Active Directory group membership, unless it is combined with another tool such as Salesforce Identity Connect.
References: Salesforce Identity Connect Implementation Guide, Single Sign-On Implementation Guide

NEW QUESTION 173
Northern Trail Outfitters would like to automatically create new employee users in Salesforce with an appropriate profile that maps to its Active Directory Department.
How should an identity architect implement this requirement?

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

Answer: B

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

NEW QUESTION 176
Northern Trail Outfitters (NTO) is launching a new sportswear brand on its existing consumer portal built on Salesforce Experience Cloud. As part of the launch, emails with promotional links will be sent to existing customers to log in and claim a discount. The marketing manager would like the portal dynamically branded so that users will be directed to the brand link they clicked on; otherwise, users will view a recognizable NTO-branded page.
The campaign is launching quickly, so there is no time to procure any additional licenses. However, the development team is available to apply any required changes to the portal.
Which approach should the identity architect recommend?

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

Answer: B

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

NEW QUESTION 180
A technology enterprise is planning to implement single sign-on login for users. When users log in to the Salesforce User object custom field, data should be populated for new and existing users.
Which two steps should an identity architect recommend? Choose 2 answers

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

Answer: AB

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

NEW QUESTION 184
An Identity architect works for a multinational, multi-brand organization. As they work with the organization to understand their Customer Identity and Access Management requirements, the identity architect learns that the brand experience is different for each of the customer's sub-brands and each of these branded experiences must be carried through the login experience depending on which sub-brand the user is logging into.
Which solution should the architect recommend to support scalability and reduce maintenance costs, if the organization has more than 150 sub-brands?

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

Answer: A

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

NEW QUESTION 188
An architect has successfully configured SAML-BASED SSO for universal containers. SSO has been working for 3 months when Universal containers manually adds a batch of new users to salesforce. The new users receive an error from salesforce when trying to use SSO. Existing users are still able to successfully use SSO to access salesforce. What is the probable cause of this behaviour?

A. The administrator forgot to reset the new user's salesforce password.
B. The Federation ID field on the new user records is not correctly set
C. The my domain capability is not enabled on the new user's profile.
D. The new users do not have the SSO permission enabled on their profiles.

Answer: B

Explanation:
The Federation ID field on the new user records is not correctly set is the probable cause of this behavior. The Federation ID is an additional field contained in the Salesforce interface that allows admins to pick whatever username or username format they want to pass to Salesforce from their user directory for single sign-on. This field does not appear on the user page layout editor or on the user record page by default, and it must be populated with a unique value that matches the identity provider's assertion for each user. If the Federation ID is missing or incorrect, the SSO will fail. The administrator does not need to reset the new user's Salesforce password, as SSO bypasses the password authentication. The My Domain capability is not enabled on the new user's profile, but on the org level, so it does not affect individual users. The new users do not have the SSO permission enabled on their profiles is not a valid option, as there is no such permission in Salesforce.
References: Certification - Identity and Access Management Architect - Trailhead, Federation ID field on Us detail page is not visible, What is the purpose of Salesforce SSO by federation ID?

NEW QUESTION 190
......

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your Identity-and-Access-Management-Architect Exam with Our Prep Materials Via below:

https://www.certleader.com/Identity-and-Access-Management-Architect-dumps.html