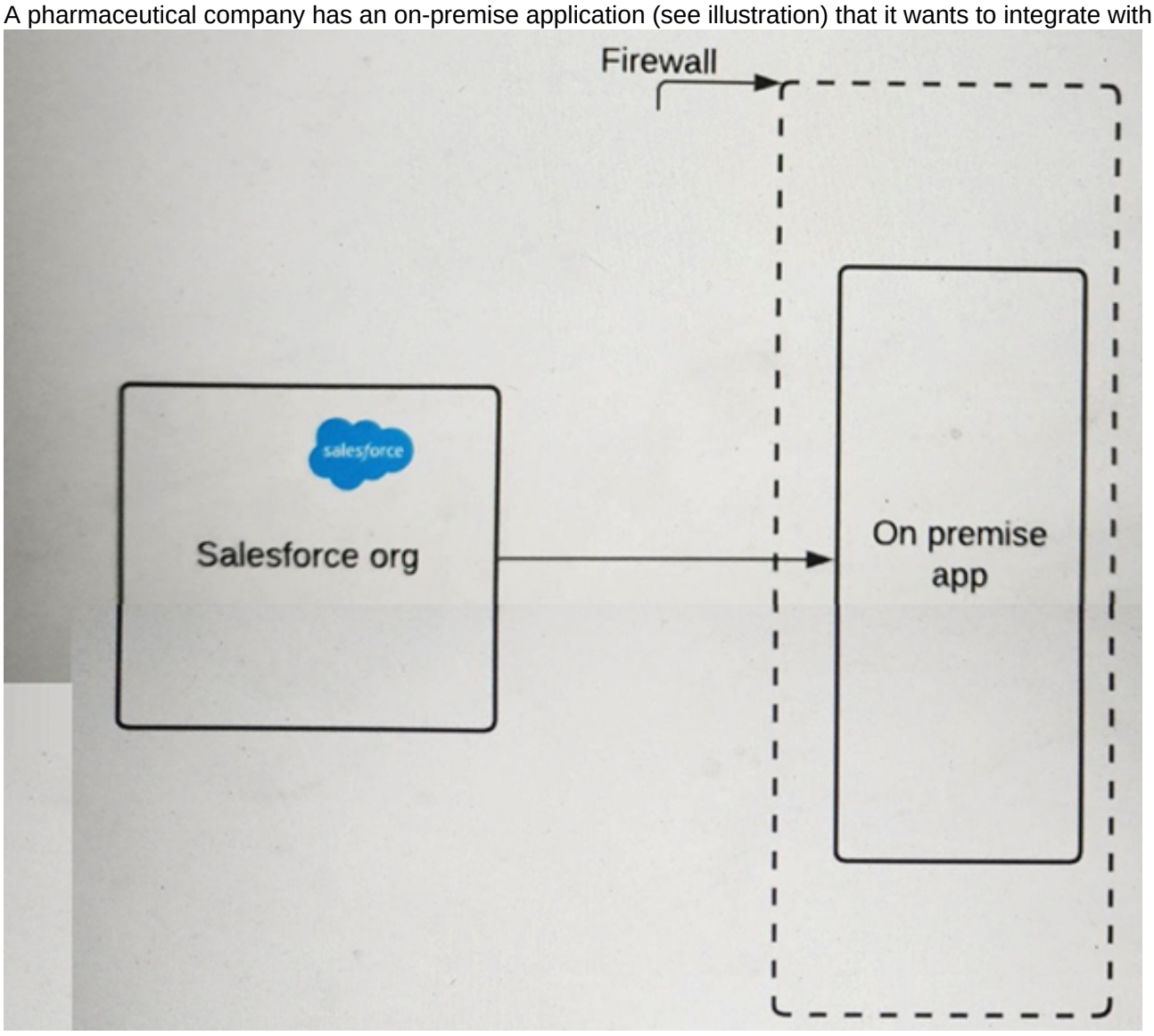
Exam Questions Identity-and-Access-Management-Architect

Salesforce Certified Identity and Access Management Architect (SU23)

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

NEW QUESTION 1
A pharmaceutical company has an on-premise application (see illustration) that it wants to integrate with Salesforce.



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

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

Answer: C

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

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

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

Answer: BD

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

NEW QUESTION 4
A global company's Salesforce Identity Architect is reviewing its Salesforce production org login history and is seeing some intermittent Security Assertion Markup Language (SAML SSO) 'Replay Detected and Assertion Invalid' login errors.
Which two issues would cause these errors?
Choose 2 answers

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

Answer: CD

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

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

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

Answer: AC

Explanation:

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

NEW QUESTION 7
A third-party app provider would like to have users provisioned via a service endpoint before users access their app from Salesforce.
What should an identity architect recommend to configure the requirement with limited changes to the third-party app?

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

Answer: A

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

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

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

Answer: D

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

NEW QUESTION 10
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 10
Northern Trail Outfitters (NTO) wants its customers to use phone numbers to log in to their new digital portal, which was designed and built using Salesforce Experience Cloud. In order to access the portal, the user will need to do the following:
* 1. Enter a phone number and/or email address
* 2. Enter a verification code that is to be sent via email or text.
What is the recommended approach to fulfill this requirement?

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

Answer: A

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

NEW QUESTION 13
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 16
A group of users try to access one of Universal Containers' Connected Apps and receive the following error message: " Failed: Not approved for access." What is the most likely cause of this issue?

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

Answer: C

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

References: Just-in-Time Provisioning for SAML, [Just-in-Time Deprovisioning], [SOAP API Developer

NEW QUESTION 21
Universal containers (UC) wants users to authenticate into their salesforce org using credentials stored in a custom identity store. UC does not want to purchase or use a third-party Identity provider. Additionally, UC is extremely wary of social media and does not consider it to be trust worthy. Which two options should an architect recommend to UC? Choose 2 answers

A. Use a professional social media such as LinkedIn as an Authentication provider
B. Build a custom web page that uses the identity store and calls frontdoor.jsp
C. Build a custom Web service that is supported by Delegated Authentication.
D. Implement the Openid protocol and configure an authentication provider

Answer: CD

Explanation:
The two options that an architect should recommend to UC are to build a custom web service that is supported by delegated authentication and to implement the OpenID protocol and configure an authentication provider. Delegated authentication is a feature that allows Salesforce to delegate user authentication to an external service instead of using Salesforce credentials3. A custom web service can be built to use the credentials stored in the custom identity store and validate them against Salesforce using SOAP or REST API3. OpenID is an open standard protocol that allows users to authenticate with various web services using an existing account4. An authentication provider can be configured in Salesforce to use OpenID and connect with the custom identity store5.
References: Delegated Authentication, OpenID, Authentication Providers

NEW QUESTION 22
Sales users at Universal containers use salesforce for Opportunity management. Marketing uses a third-party application called Nest for Lead nurturing that is accessed using username/password. The VP of sales wants to open up access to nest for all sales uses to provide them access to lead history and would like SSO for better adoption. Salesforce is already setup for SSO and uses Delegated Authentication. Nest can accept username/Password or SAML-based Authentication. IT teams have received multiple password-related issues for nest and have decided to set up SSO access for Nest for Marketing users as well. The CIO does not want to invest in a new IDP solution and is considering using Salesforce for this purpose. Which are appropriate license type choices for sales and marketing users, giving salesforce is using Delegated Authentication? Choose 2 answers

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

Answer: AD

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

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

NEW QUESTION 26
Northern Trail Outfitters would like to use a portal built on Salesforce Experience Cloud for customer self-service. Guests of the portal be able to self-register, but be unable to automatically be assigned to a contact record until verified. External Identity licenses have been purchased for the project.
After registered guests complete an onboarding process, a flow will create the appropriate account and contact records for the user.
Which three steps should an identity architect follow to implement the outlined requirements? Choose 3 answers

A. Enable "Allow customers and partners to self-register".
B. Select the "Configurable Self-Reg Page" option under Login & Registration.
C. Set jp an external login page and call Salesforce APIs for user creation.
D. Customize the self-registration Apex handler to temporarily associate the user to a shared single contact record.
E. Customize me self-registration Apex handler to create only the user record.

Answer: ABE

Explanation:
Enabling "Allow customers and partners to self-register" allows guests to create their own user accounts in the portal. Selecting the "Configurable Self-Reg Page" option allows the administrator to customize the
self-registration page to capture the required fields. Customizing the self-registration Apex handler to create
only the user record prevents the automatic creation of a contact record until verification. References: Enable Self-Registration, Customize Self-Registration

NEW QUESTION 31
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 34
An architect needs to set up a Facebook Authentication provider as login option for a salesforce customer Community. What portion of the authentication provider setup associates a Facebook user with a salesforce user?

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

Answer: D

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

NEW QUESTION 36
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 37
A financial services company uses Salesforce and has a compliance requirement to track information about devices from which users log in. Also, a Salesforce Security Administrator needs to have the ability to revoke the device from which users log in.
What should be used to fulfill this requirement?

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

Answer: B

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

Users

NEW QUESTION 38
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 41
Universal Container's (UC) is using Salesforce Experience Cloud site for its container wholesale business. The identity architect wants to an authentication provider for the new site.
Which two options should be utilized in creating an authentication provider? Choose 2 answers

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

Answer: AB

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

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

NEW QUESTION 43
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 46
IT security at Unversal Containers (UC) us concerned about recent phishing scams targeting its users and wants to add additional layers of login protection. What should an Architect recommend to address the issue?

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

Answer: A

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

NEW QUESTION 51
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 54
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 58
Universal Containers (UC) wants its users to access Salesforce and other SSO-enabled applications from a custom web page that UC magnets. UC wants its users to use the same set of credentials to access each of the applications. what SAML SSO flow should an Architect recommend for UC?

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

Answer: C

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

NEW QUESTION 59
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 61

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

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

Answer: C

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

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

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

Answer: C

Explanation:
The best approach to simplify the authentication process and reduce cost and maintenance is to configure UC1 as the Identity Provider to the other four Salesforce orgs and set up JIT user provisioning on all other
orgs. This way, users can log in to any of the five orgs using their UC1 credentials, and their user accounts wil be automatically created or updated in the other orgs based on the information from UC11. This eliminates the need to purchase a third-party Identity Provider or manually provision users in advance. The other options are not optimal for this requirement because:

- Purchasing a third-party Identity Provider for all five Salesforce orgs would incur additional cost and maintenance, and would not leverage the existing user base in UC1.
- Not setting up JIT user provisioning for other orgs would require manually creating or updating user accounts in each org, which would be time-consuming and error-prone. References: Salesforce as an Identity Provider, Identity Providers and Service Providers, Just-in-Time Provisioning for SAML

NEW QUESTION 69
Universal Containers (UC) wants to build a mobile application that twill be making calls to the Salesforce REST API. UC's Salesforce implementation relies heavily on custom objects and custom Apex code. UC does not want its users to have to enter credentials every time they use the app. Which two scope values should an Architect recommend to UC? Choose 2 answers.

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

Answer: BC

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

NEW QUESTION 70
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 74
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 79
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 80
Universal containers (UC) has implemented SAML -based single Sign-on for their salesforce application. UC is using PingFederate as the Identity provider. To access salesforce, Users usually navigate to a bookmarked link to my domain URL. What type of single Sign-on is this?

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

Answer: A

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

NEW QUESTION 82
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 86
Universal Containers (UC) wants to implement SAML SSO for their internal of Salesforce users using a third-party IdP. After some evaluation, UC decides NOT to 65« set up My Domain for their Salesforce org. How does that decision impact their SSO implementation?

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

Answer: D

Explanation:
This is because without My Domain, Salesforce will not know in advance what Identity Provider (IdP) to use for SSO, since it does not even know yet what Organization the user is trying to log in to1. SP-initiated SSO is the scenario where the user starts with a Salesforce link (login page, deep link, Outlook Sync URL, etc.) and then gets redirected to the IdP for authentication2. Without My Domain, SP-initiated SSO requires that the user do an IdP-initiated SSO at least once first so that Salesforce can set a cookie in their browser identifying the IdP1. The other options are not correct for this question because:

- IdP-initiated SSO will work without My Domain, as long as the user starts SSO at the IdP and sends the identity information to Salesforce along with SAML protocol information that identifies the Organization and the IdP2.
- Neither SP- nor IdP-initiated SSO will not work is false, as explained above.
- Either SP- or IdP-initiated SSO will work is false, as explained above.

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

NEW QUESTION 91
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 95
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 97
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 102
Universal containers (UC) would like to enable self - registration for their salesforce partner community users. UC wants to capture some custom data elements from the partner user, and based on these data elements, wants to assign the appropriate profile and account values. Which two actions should the architect recommend to UC? Choose 2 answers

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

Answer: AC

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

NEW QUESTION 105
A global company is using the Salesforce Platform as an Identity Provider and needs to integrate a third-party application with its Experience Cloud customer portal.
Which two features should be utilized to provide users with login and identity services for the third-party application?
Choose 2 answers

A. Use the App Launcher with single sign-on (SSO).
B. External a Data source with Named Principal identity type.
C. Use a connected app.
D. Use Delegated Authentication.

Answer: AC

Explanation:
Using the App Launcher with SSO and using a connected app are two features that can be utilized to provide users with login and identity services for the third-party application. The App Launcher allows users to access multiple apps from one location with SSO. The connected app allows users to authorize access to the third-party application using OAuth 2.0. The other options are either not relevant or not applicable for this use case. References: App Launcher, Connected Apps

NEW QUESTION 109
Universal Containers (UC) wants to build a custom mobile app for their field reps to create orders in salesforce. After the first time the users log in, they must be able to access salesforce upon opening the mobile app without being prompted to log in again. What Oauth flows should be considered to support this requirement?

A. Web Server flow with a Refresh Token.
B. Mobile Agent flow with a Bearer Token.
C. User Agent flow with a Refresh Token.
D. SAML Assertion flow with a Bearer Token.

Answer: AC

Explanation:

The OAuth 2.0 user-agent flow and the OAuth 2.0 web server flow are both suitable for building a custom mobile app that can access Salesforce data without prompting the user to log in again1. Both of these flows use a refresh token that can be used to obtain a new access token when the previous one expires2. The user-agent flow uses the Canvas JavaScript SDK to obtain an OAuth token by using the login function in the SDK2. The web server flow redirects the user to the Salesforce OAuth authorization endpoint and then obtains an OAuth access token by making a POST request to the Salesforce OAuth token endpoint2. The mobile agent flow and the SAML assertion flow are not valid OAuth flows for Salesforce3.
References: OAuth Authorization Flows, Mastering Salesforce Canvas Apps, Access Data with API Integration

NEW QUESTION 110
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 111
Northern Trail Outfitters is implementing a business-to-business (B2B) collaboration site using Salesforce Experience Cloud. The partners will authenticate with an existing identity provider and the solution will utilize Security Assertion Markup Language (SAML) to provide single sign-on to Salesforce. Delegated administration will be used in the Expenence Cloud site to allow the partners to administer their users' access.
How should a partner identity be provisioned in Salesforce for this solution?

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

Answer: C

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

NEW QUESTION 112
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 113

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

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

Answer: ACE

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

NEW QUESTION 116
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 119
Universal Containers is creating a mobile application that will be secured by Salesforce Identity using the OAuth 2.0 user-agent flow. Application users will authenticate using username and password. They should not be forced to approve API access in the mobile app or reauthenticate for 3 months.
Which two connected app options need to be configured to fulfill this use case?
Choose 2 answers

A. Set Permitted Users to "Admin approved users are pre-authorized".
B. Set Permitted Users to "All users may self-authorize".
C. Set the Session Timeout value to 3 months.
D. Set the Refresh Token Policy to expire refresh token after 3 months.

Answer: BD

Explanation:
To fulfill the use case of creating a mobile application that will be secured by Salesforce Identity using the OAuth 2.0 user-agent flow, where users will authenticate using username and password and not be forced to approve API access or reauthenticate for 3 months, the identity architect should configure two connected app options:

- Set Permitted Users to “All users may self-authorize”. Permitted Users is a setting that controls how users can access a connected app. By setting it to “All users may self-authorize”, the identity architect can allow users to access the connected app without requiring administrator approval or API access confirmation.
- Set the Refresh Token Policy to expire refresh token after 3 months. Refresh Token Policy is a setting that controls how long a refresh token can be used to obtain a new access token without requiring user authentication. By setting it to expire refresh token after 3 months, the identity architect can allow users to access the connected app for 3 months without reauthenticating, as long as they use the app at least once every 90 days. References: Connected Apps, OAuth 2.0 User-Agent Flow

NEW QUESTION 121
Universal Containers (UC) currently uses Salesforce Sales Cloud and an external billing application. Both Salesforce and the billing application are accessed several times a day to manage customers. UC would like to configure single sign-on and leverage Salesforce as the identity provider. Additionally, UC would like the billing application to be accessible from Salesforce. A redirect is acceptable.
Which two Salesforce tools should an identity architect recommend to satisfy the requirements? Choose 2 answers

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

Answer: AD

Explanation:

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

NEW QUESTION 122
Universal containers (UC) wants to implement a partner community. As part of their implementation, UC would like to modify both the Forgot password and change password experience with custom branding for their partner community users. Which 2 actions should an architect recommend to UC? Choose 2 answers

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

Answer: BC

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

NEW QUESTION 125
Northern Trail Outfitters want to allow its consumer to self-register on it business-to-consumer (B2C) portal that is built on Experience Cloud. The identity architect has recommended to use Person Accounts.
Which three steps need to be configured to enable self-registration using person accounts? Choose 3 answers

A. Enable access to person and business account record types under Public Access Settings.
B. Contact Salesforce Support to enable business accounts.
C. Under Login and Registration settings, ensure that the default account field is empty.
D. Contact Salesforce Support to enable person accounts.
E. Set organization-wide default sharing for Contact to Public Read Only.

Answer: ACD

Explanation:
To enable self-registration using person accounts for consumers on a B2C portal built on Experience Cloud, the identity architect should configure three steps:

- Enable access to person and business account record types under Public Access Settings. Public Access Settings are settings that control the access level and permissions for guest users on Experience Cloud sites. By enabling access to person and business account record types, the identity architect can allow guest users to create person accounts or business accounts when they self-register on the portal.
- Under Login and Registration settings, ensure that the default account field is empty. Login and Registration settings are settings that control the login and registration options for Experience Cloud sites. By ensuring that the default account field is empty, the identity architect can prevent guest users from being associated with a default account when they self-register on the portal.
- Contact Salesforce Support to enable person accounts. Person accounts are a type of account that combines an individual consumer with an account record. Person accounts are not enabled by default in Salesforce orgs and require contacting Salesforce Support to enable them. References: Public Access Settings, Login and Registration Settings, Person Accounts

NEW QUESTION 126
Universal Containers is implementing a new Experience Cloud site and the identity architect wants to use dynamic branding features as of the login process.
Which two options should the identity architect recommend to support dynamic branding for the site? Choose 2 answers

A. To use dynamic branding, the community must be built with the Visuaiforce + Salesforce Tabs template.
B. To use dynamic branding, the community must be built with the Customer Account Portal template.
C. An experience ID (expid) or placeholder parameter must be used in the URL to represent the brand.
D. An external content management system (CMS) must be used for dynamic branding on Experience Cloud sites.

Answer: BC

Explanation:
Dynamic branding is a feature that allows Experience Cloud sites to display different branding elements, such as logos, colors, or images, based on the user's profile or preferences. To use dynamic branding, the community must be built with the Customer Account Portal template, which supports this feature. An experience ID (expid) or placeholder parameter must be used in the URL to represent the brand and trigger the dynamic branding logic.
References: Dynamic Branding for Experience Cloud Sites, Create a Customer Account Portal

NEW QUESTION 130
Universal containers (UC) does my domain enable in the context of a SAML SSO configuration? Choose 2 answers

A. Resource deep linking
B. App launcher
C. SSO from salesforce1 mobile app.
D. Login forensics

Answer: AC

Explanation:
Enabling My Domain in the context of a SAML SSO configuration enables resource deep linking and SSO from Salesforce1 mobile app. Resource deep linking allows users to access specific records or pages after logging in with SSO5. SSO from Salesforce1 mobile app requires using the My Domain URL as the login server4. Enabling My Domain does not affect the app launcher or login forensics features. Therefore, option A and C are the correct answers. References: Salesforce Mobile Application Single Sign-On overview, SAML SSO with Salesforce as the Service Provider, Single Sign-On, Considerations for setting up My Domain and SSO

NEW QUESTION 134
Universal Containers is creating a mobile application that will be secured by Salesforce Identity using the OAuth 2.0 user-agent flow (this flow uses the OAuth 2.0 implicit grant type).
Which three OAuth concepts apply to this flow? Choose 3 answers

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

Answer: AE

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

NEW QUESTION 136
Universal Container's (UC) identity architect needs to recommend a license type for their new Experience Cloud site that will be used by external partners (delivery providers) for reviewing and updating their accounts, downloading files provided by UC and obtaining scheduled pickup dates from their calendar.
UC is using their Salesforce production org as the identity provider for these users and the expected number of individual users is 2.5 million with 13.5 million unique logins per month.
Which of the following license types should be used to meet the requirement?

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

Answer: C

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

NEW QUESTION 138
Universal Containers is using OpenID Connect to enable a connection from their new mobile app to its production Salesforce org.
What should be done to enable the retrieval of the access token status for the OpenID Connect connection?

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

Answer: B

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

NEW QUESTION 139
The CIO of universal containers(UC) wants to start taking advantage of the refresh token capability for the UC applications that utilize Oauth 2.0. UC has listed an architect to analyze all of the applications that use Oauth flows to. See where refresh Tokens can be applied. Which two OAuth flows should the architect consider in their evaluation? Choose 2 answers

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

Answer: AC

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

NEW QUESTION 144
Universal Containers (UC) uses middleware to integrate multiple systems with Salesforce. UC has a strict, new requirement that usernames and passwords cannot be stored in any UC system. How can UC's middleware authenticate to Salesforce while adhering to this requirement?

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

Answer: A

Explanation:
A is correct because creating a connected app that supports the JWT Bearer Token OAuth Flow allows the middleware to authenticate to Salesforce without storing usernames and passwords. The JWT Bearer Token OAuth Flow uses a certificate and a private key to sign a JSON Web Token (JWT) that contains information about the user identity and requested access. The middleware sends the JWT to Salesforce, which verifies it using the certificate and grants an access token2.
B is incorrect because creating a connected app that supports the Refresh Token OAuth Flow requires storing usernames and passwords in the middleware. The Refresh Token OAuth Flow uses a username-password authentication flow to obtain an access token and a refresh token. The middleware can use the refresh token to obtain new access tokens without user interaction, but it still needs to store the username and password for the initial authentication3.
C is incorrect because creating a connected app that supports the Web Server OAuth Flow requires user interaction to authenticate to Salesforce. The Web Server OAuth Flow redirects the user to a Salesforce login page, where they enter their credentials and grant access to the middleware. The middleware then receives an authorization code that it can exchange for an access token and a refresh token4.
D is incorrect because creating a connected app that supports the User-Agent OAuth Flow also requires user interaction to authenticate to Salesforce. The User-Agent OAuth Flow is similar to the Web Server OAuth Flow, except that it does not return a refresh token. The middleware can only use the access token until it expires5.
References: 2: Accessing Salesforce with JWT OAuth Flow 3: OAuth Authorization Flows - Salesforce 4: OAuth Authorization Flows - Salesforce 5: OAuth Authorization Flows - Salesforce

NEW QUESTION 146
Universal Containers (UC) wants to use Salesforce for sales orders and a legacy of system for order fulfillment. The legacy system must update the status of orders in 65* Salesforce in real time as they are fulfilled. UC decides to use OAuth for connecting the legacy system to Salesforce. What OAuth flow should be considered that doesn't require storing credentials, client secret or refresh tokens?

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

Answer: B

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

NEW QUESTION 147
Northern Trail Outfitters (NTO) leverages Microsoft Active Directory (AD) for management of employee usernames, passwords, permissions, and asset access. NTO also owns a third-party single sign-on (SSO) solution. The third-party party SSO solution is used for all corporate applications, including Salesforce.
NTO has asked an architect to explore Salesforce Identity Connect for automatic provisioning and deprovisioning of users in Salesforce.
What role does identity Connect play in the outlined requirements?

A. Service Provider
B. Single Sign-On
C. Identity Provider
D. User Management

Answer: D

Explanation:
Salesforce Identity Connect is a tool that synchronizes user data between Microsoft Active Directory and Salesforce. It allows automatic provisioning and deprovisioning of users in Salesforce based on the changes made in Active Directory. Therefore, Identity Connect plays the role of user management in the outlined requirements. References: Identity Connect Implementation Guide, Identity Connect Overview

NEW QUESTION 152
Universal Containers (UC) is setting up delegated authentication to allow employees to log in using their corporate credentials. UC's security team is concerned about the risks of exposing the corporate login service on the internet and has asked that a reliable trust mechanism be put in place between the login service and Salesforce.
What mechanism should an Architect put in place to enable a trusted connection between the login service and Salesforce?

A. Require the use of Salesforce security tokens on passwords.
B. Enforce mutual authentication between systems using SSL.
C. Include Client Id and Client Secret in the login header callout.
D. Set up a proxy service for the login service in the DMZ.

Answer: B

Explanation:
To enable a trusted connection between the login service and Salesforce, an architect should enforce mutual authentication between systems using SSL. Mutual

authentication, also known as two-way SSL or client certificate authentication, is a process in which both parties in a communication exchange certificates to verify their identities7. This mechanism ensures that only authorized systems can access each other's resources and prevents unauthorized access or spoofing attacks8. To use mutual authentication with delegated authentication you need to do the following steps9:

- Generate a self-signed certificate in Salesforce and download it.
- Import the certificate into your login service's truststore.
- Configure your login service to require client certificates for incoming requests.
- Generate a certificate for your login service and export it.
- Import the certificate into Salesforce's certificate and key management tool.
- Enable mutual authentication for your login service's endpoint URL in Salesforce. References:
- Mutual Authentication
- Mutual Authentication Overview
- Set Up Mutual Authentication

NEW QUESTION 154
Which three are capabilities of SAML-based Federated authentication? Choose 3 answers

A. Trust relationships between Identity Provider and Service Provider are required.
B. SAML tokens can be in XML or JSON format and can be used interchangeably.
C. Web applications with no passwords are more secure and stronger against attacks.
D. Access tokens are used to access resources on the server once the user is authenticated.
E. Centralized federation provides single point of access, control and auditing.

Answer: ACE

Explanation:
A is correct because SAML-based Federated authentication requires trust relationships between the IdP and the SP. The IdP issues a SAML assertion that contains information about the user's identity and attributes. The SP validates the assertion and grants access to the user.
C is correct because web applications that use SAML-based Federated authentication do not require passwords for users to log in. Instead, they rely on the IdP to authenticate the users and provide a secure token. This eliminates the risk of password breaches and phishing attacks.
E is correct because centralized federation provides a single point of access, control, and auditing for web applications that use SAML-based Federated authentication. Users can access multiple applications with one login, administrators can manage user access from one place, and auditors can monitor user activity across applications.
B is incorrect because SAML tokens are always in XML format. They cannot be used interchangeably with JSON tokens, which are used by OAuth or OpenID Connect protocols.
D is incorrect because access tokens are not used by SAML-based Federated authentication. Access tokens are used by OAuth or OpenID Connect protocols to access resources on the server once the user is authenticated.
References: : [Single Sign-On Implementation Guide Developer Documentation] : [Identity 101: Design Patterns for Access Management Salesforce Developers YouTube] : Certification - Identity and Access Management Architect - Trailhead : OAuth Authorization Flows Trailblazer Community Documentation : User Authentication Module - Trailhead

NEW QUESTION 159
Universal Containers (UC) has implemented SAML-based SSO solution for use with their multi-org Salesforce implementation, utilizing one of the the orgs as the Identity Provider. One user is reporting that they can log in to the Identity Provider org but get a generic SAML error message when accessing the other orgs.
Which two considerations should the architect review to troubleshoot the issue? Choose 2 answers

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

Answer: BD

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

- The Federation ID must be case sensitive, which means that the value in the user record must match exactly with the value in the SAML assertion. For example, if the Federation ID is "John.Doe", then "john.doe" or "JOHN.DOE" will not work.
- The Federation ID must be populated on the user record, which means that the user must have a value for this field in each org that they want to access via SSO. If the Federation ID is blank or missing, then Salesforce will not be able to match the user with the SAML assertion.

NEW QUESTION 164
Northern Trail Outfitters mar ages functional group permissions in a custom security application supported by a relational database and a REST service layer. Group permissions are mapped as permission sets in Salesforce.
Which action should an identity architect use to ensure functional group permissions are reflected as permission set assignments?

A. Use a Login Flow to query SAML attributes and set permission sets.
B. Use a Login Flow with invocable Apex to callout to the security application and set permission sets.
C. Use the Apex Just-in-Time (JIT) handler to query the Security Assertion markup Language (SAML) attributes and set permission sets.
D. Use the Apex JIT handler to callout to the security application and set permission sets

Answer: B

Explanation:
Using a Login Flow with invocable Apex to callout to the security application and set permission sets allows the identity architect to dynamically assign or remove permission sets based on the functional group permissions in the custom security application. This ensures that the permission set assignments are consistent

with the group permissions. References: Login Flows, Invocable Apex

NEW QUESTION 165
Northern Trail Outfitters (NTO) recently purchased Salesforce Identity Connect to streamline user provisioning across Microsoft Active Directory (AD) and Salesforce Sales Cloud.
NTO has asked an identity architect to identify which salesforce security configurations can map to AD permissions.
Which three Salesforce permissions are available to map to AD permissions? Choose 3 answers

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

Answer: ACE

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

NEW QUESTION 169
Universal Containers uses Salesforce as an identity provider and Concur as the Employee Expense management system. The HR director wants to ensure Concur accounts for employees are created only after the apocopate approval in the Salesforce org.
Which three steps should the identity architect use to implement this requirement? Choose 3 answers

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

Answer: BCE

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

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

References:

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

NEW QUESTION 171
A company wants to provide its employees with a custom mobile app that accesses Salesforce. Users are required to download the internal native IOS mobile app from corporate intranet on their mobile device. The app allows flexibility to access other non-Salesforce internal applications once users authenticate with Salesforce. The apps self-authorize, and users are permitted to use the apps once they have logged into Salesforce.
How should an identity architect meet the above requirements with the privately distributed mobile app?

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

Answer: B

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

this use case. References: Mobile App Settings, Single Sign-On for Desktop and Mobile Applications using SAML and OAuth

NEW QUESTION 174
Universal Containers (UC) is planning to add Wi-Fi enabled GPS tracking devices to its shipping containers so that the GPS coordinates data can be sent from the tracking device to its Salesforce production org via a custom API. The GPS devices have no direct user input or output capabilities.
Which OAuth flow should the identity architect recommend to meet the requirement?

A. OAuth 2.0 Asset Token Flow for Securing Connected Devices
B. OAuth 2.0 Username-Password Flow for Special Scenarios
C. OAuth 2.0 Web Server Flow for Web App Integration
D. OAuth 2.0 JWT Bearer Flow for Server-to-Server Integration

Answer: A

Explanation:
OAuth 2.0 Asset Token Flow is the flow that allows connected devices to request an asset token from Salesforce. The device obtains an access token and an actor token, and uses them to create an asset token. This flow enables efficient token exchange and automatic linking of devices to Service Cloud Asset records. References: OAuth 2.0 Asset Token Flow for Securing Connected Devices, OAuth Authorization Flows

NEW QUESTION 175
Universal containers (UC) uses a home-grown employee portal for their employees to collaborate. UC decides to use salesforce ideas to allow the employees to post ideas from the employee portal. When clicking some links in the employee portal, the users should be redirected to salesforce, authenticated, and presented with relevant pages. What scope should be requested when using the Oauth token to meet this requirement?

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

Answer: A

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

NEW QUESTION 178
Universal Containers (UC) has decided to replace the homegrown customer portal with Salesforce Experience Cloud. UC will continue to use its third-party single sign-on (SSO) solution that stores all of its customer and partner credentials.
The first time a customer logs in to the Experience Cloud site through SSO, a user record needs to be created automatically.
Which solution should an identity architect recommend in order to automatically provision users in Salesforce upon login?

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

Answer: A

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

NEW QUESTION 182
Universal Containers (UC) has an Experience Cloud site (Customer Community) where customers can authenticate and place orders, view the status of orders, etc. UC allows guest checkout.
Mow can a guest register using data previously collected during order placement?

A. Enable Security Assertion Markup Language Sign-On and use a login flow to collect only order details to retrieve customer data.
B. Enable Facebook as an authentication provider and use a registration handler to collect only order details to retrieve customer data.
C. Use a Connected App Handler Apex Plugin class to collect only order details to retrieve customer data.
D. Enable self-registration and customize a self-registration page to collect only order details to retrieve customer data.

Answer: D

Explanation:
Self-registration allows guests to create their own user accounts and access the community. The
self-registration page can be customized to collect order details and use them to retrieve customer data from the org. References: Customize Self-Registration

NEW QUESTION 183
Northern Trail Outfitters (NTO) employees use a custom on-premise helpdesk application to request, approve, notify, and track access granted to various on-premises and cloud applications, including Salesforce. Salesforce is currently used to authenticate users.
How should NTO provision Salesforce users as soon as they are approved in the helpdesk application with the approved profiles and permission sets?

A. Build an integration that performs a remote call-in to the Salesforce SOAP or REST API.
B. Use a login flow to query the helpdesk to validate user status.
C. Have the helpdesk initiate an IdP-initiated Just-m-Time provisioning Security Assertion Markup Language flow.
D. Use Salesforce Connect to integrate with the helpdesk application.

Answer: A

Explanation:
Building an integration that performs a remote call-in to the Salesforce SOAP or REST API is the best way to provision Salesforce users as soon as they are approved in the helpdesk application. The API allows creating and updating user records with the approved profiles and permission sets. The other options are either not suitable or not sufficient for this use case. References: User SOAP API Developer Guide, User REST API Developer Guide

NEW QUESTION 187
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

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

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

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

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

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