Salesforce

Exam Questions Identity-and-Access-Management-Architect

Salesforce Certified Identity and Access Management Architect (SU23)

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

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

Answer: BD

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

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

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

Answer: D

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

NEW QUESTION 3
Universal Containers (UC) is planning to deploy a custom mobile app that will allow users to get e-signatures from its customers on their mobile devices. The mobile app connects to Salesforce to upload the e-signature as a file attachment and uses OAuth protocol for both authentication and authorization. What is the most recommended and secure OAuth scope setting that an Architect should recommend?

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

Answer: D

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

NEW QUESTION 4
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 risk 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 services and salesforce?

A. Include client ID and client secret in the login header callout.
B. Set up a proxy server for the login service in the DMZ.
C. Require the use of Salesforce security Tokens on password.
D. Enforce mutual Authentication between systems using SSL.

Answer: D

Explanation:
To enable a trusted connection between the login services and Salesforce, UC should enforce mutual authentication between systems using SSL. Mutual authentication is a process in which both parties in a communication verify each other's identity using certificates7. SSL (Secure Sockets Layer) is a protocol that provides secure communication over the Internet using encryption and certificates8. By using mutual authentication with SSL, UC can ensure that only authorized login services can access Salesforce and vice versa. This can prevent unauthorized access, impersonation, or phishing attacks.
References: Mutual Authentication, SSL (Secure Sockets Layer)

NEW QUESTION 5
Universal Containers (UC) is building an authenticated Customer Community for its customers. UC does not want customer credentials stored in Salesforce and is confident its customers would be willing to use their social media credentials to authenticate to the community. Which two actions should an Architect recommend UC to take?

A. Use Delegated Authentication to call the Twitter login API to authenticate users.
B. Configure an Authentication Provider for LinkedIn Social Media Accounts.
C. Create a Custom Apex Registration Handler to handle new and existing users.
D. Configure SSO Settings For Facebook to serve as a SAML Identity Provider.

Answer: BC

Explanation:
Configuring an Authentication Provider for LinkedIn Social Media Accounts allows UC to use LinkedIn as an external identity provider for its customer community. This means that customers can use their LinkedIn credentials to log in to the community without storing their credentials in Salesforce. Creating a Custom Apex Registration Handler allows UC to customize how new and existing users are handled when they log in with an external identity provider. This means that UC can control how user records are created, updated, or matched when customers use their social media credentials to authenticate to the community. These two actions can meet the requirement of UC to use social media credentials for its customer community.

NEW QUESTION 6
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 7
Universal Containers (UC) wants to integrate a third-party Reward Calculation system with Salesforce to calculate Rewards. Rewards will be calculated on a schedule basis and update back into Salesforce. The integration between Salesforce and the Reward Calculation System needs to be secure. Which are two recommended practices for using OAuth flow in this scenario. choose 2 answers

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

Answer: CD

Explanation:
OAuth is an open-standard protocol that allows a client app to access protected resources on a resource server, such as Salesforce API, by obtaining an access token from an authorization server. OAuth supports different types of flows, which are ways of obtaining an access token. For integrating a third-party Reward Calculation system with Salesforce securely, two recommended practices for using OAuth flow are:
- OAuth SAML Bearer Assertion Flow, which allows the client app to use a SAML assertion issued by a trusted identity provider to request an access token from Salesforce. This flow does not require the client app to store any credentials or secrets, and leverages the existing SSO infrastructure between Salesforce and the identity provider.
- OAuth JWT Bearer Token Flow, which allows the client app to use a JSON Web Token (JWT) signed by a private key to request an access token from Salesforce. This flow does not require any user interaction or consent, and uses a certificate to verify the identity of the client app.
Verified References: [OAuth 2.0 SAML Bearer Assertion Flow for Server-to-Server Integration], [OAuth 2.0 JWT Bearer Token Flow for Server-to-Server Integration]

NEW QUESTION 8
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 9
Universal Containers (UC) has a strict requirement to authenticate users to Salesforce using their mainframe credentials. The mainframe user store cannot be accessed from a SAML provider. UC would also like to have users in Salesforce created on the fly if they provide accurate mainframe credentials.
How can the Architect meet these requirements?

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

Answer: C

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

NEW QUESTION 10
Which two roles of the systems are involved in an environment where salesforce users are enabled to access Google Apps from within salesforce through App launcher and connected App set up? Choose 2 answers

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

Answer: BC

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

NEW QUESTION 10
Which two considerations should be made when implementing Delegated Authentication? Choose 2 answers

A. The authentication web service can include custom attributes.
B. It can be used to authenticate API clients and mobile apps.
C. It requires trusted IP ranges at the User Profile level.
D. Salesforce servers receive but do not validate a user’s credentials.
E. Just-in-time Provisioning can be configured for new users.

Answer: BE

Explanation:
Delegated authentication is a feature that allows Salesforce to delegate the authentication process to an external service of your choice1. When implementing delegated authentication, you should consider the following aspects2:

- The authentication web service can include custom attributes, such as user roles or permissions, in the response to Salesforce. These attributes can be used to update user records or trigger workflows in Salesforce2.
- Delegated authentication can be used to authenticate API clients and mobile apps that use the SOAP API or REST API login() methods. However, it does not support OAuth 2.0 flows or other authentication methods2.
- Delegated authentication does not require trusted IP ranges at the User Profile level. However, you can use them to restrict access to Salesforce from specific IP addresses or ranges2.
- Salesforce servers receive but do not validate a user's credentials. Instead, they pass the credentials to the external authentication service, which validates them and returns a response to Salesforce2.
- Just-in-time provisioning can be configured for new users who log in with delegated authentication. Thi
feature allows Salesforce to create or update user accounts based on the information provided by the external authentication service3.

References:

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

NEW QUESTION 14
Universal Containers (UC) wants to provide single sign-on (SSO) for a business-to-consumer (B2C) application using Salesforce Identity.
Which Salesforce license should UC utilize to implement this use case?

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

Answer: C

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

NEW QUESTION 19
Universal Containers (UC) employees have Salesforce access from restricted IP ranges only, to protect against unauthorized access. UC wants to roll out the Salesforce1 mobile app and make it accessible from any location. Which two options should an Architect recommend? Choose 2 answers

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

Answer: AC

Explanation:
The two options that an architect should recommend for UC to roll out the Salesforce1 mobile app and make it accessible from any location are:

- Relax the IP restriction with a second factor in the Connected App settings for Salesforce1 mobile app.

This option allows UC to enable two-factor authentication (2FA) for the Salesforce1 mobile app, which requires users to verify their identity with a second factor, such as a verification code or a mobile app, after entering their username and password. By enabling 2FA in the Connected App settings, UC can relax the IP restriction for the Salesforce1 mobile app, as users can access it from any location as long as they provide the second factor.

- Relax the IP restrictions in the Connected App settings for the Salesforce1 mobile app. This option allows UC to disable or modify the IP restriction for the Salesforce1 mobile app in the Connected App settings, which control how users can access a connected app, such as Salesforce1. By relaxing the IP restrictions, UC can allow users to access the Salesforce1 mobile app from any location without requiring 2FA.

The other options are not recommended for this scenario. Removing existing restrictions on IP ranges for all types of user access would compromise security and compliance, as it would expose Salesforce to unauthorized access from any location. Using Login Flow to bypass IP range restriction for the mobile app would require custom code and logic, which could introduce complexity and errors. References: [Connected Apps], [Two-Factor Authentication], [Require a Second Factor of Authentication for Connected Apps], [IP Restrictions for Connected Apps], [Login Flows]

NEW QUESTION 22
A service provider (SP) supports both Security Assertion Markup Language (SAML) and OpenID Connect (OIDC).
When integrating this SP with Salesforce, which use case is the determining factor when choosing OIDC or SAML?

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

Answer: B

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

NEW QUESTION 27

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 29
Universal Containers (UC) would like to enable self-registration for their Salesforce Partner Community Users. UC wants to capture some custom data elements from the partner user, and based on these data elements, wants to assign the appropriate Profile and Account values.
Which two actions should the Architect recommend to UC1 Choose 2 answers

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

Answer: CD

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

NEW QUESTION 32
A web service is developed that allows secure access to customer order status on the Salesforce Platform. The service connects to Salesforce through a connected app with the web server flow. The following are the required actions for the authorization flow:
* 1. User Authenticates and Authorizes Access
* 2. Request an Access Token
* 3. Salesforce Grants an Access Token
* 4. Request an Authorization Code
* 5. Salesforce Grants Authorization Code
What is the correct sequence for the authorization flow?

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

Answer: B

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

NEW QUESTION 35
Universal Containers (UC) uses Salesforce as a CRM and identity provider (IdP) for their Sales Team to seamlessly login to intemaJ portals. The IT team at UC is now evaluating Salesforce to act as an IdP for its remaining employees.
Which Salesforce license is required to fulfill this requirement?

A. External Identity

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

Answer: D

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

NEW QUESTION 38
Universal containers (UC) has an e-commerce website while customers can buy products, make payments, and manage their accounts. UC decides to build a customer Community on Salesforce and wants to allow the customers to access the community for their accounts without logging in again. UC decides to implement ansp-Initiated SSO using a SAML-BASED complaint IDP. In this scenario where salesforce is the service provider, which two activities must be performed in salesforce to make sp-Initiated SSO work? Choose 2 answers

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

Answer: AD

Explanation:
To enable SP-initiated SSO using a SAML-based identity provider, UC needs to configure SAML SSO settings in Salesforce and set up a custom domain using My Domain feature. This allows UC to specify the identity provider information, such as the issuer, entity ID, certificate, and SAML assertion attributes. Delegated authentication is a different mechanism that allows Salesforce to delegate the authentication process to an external web service. A connected app is not required for SP-initiated SSO, but it is used for
IDP-initiated SSO or OAuth flows. References: Certification - Identity and Access Management Architect - Trailhead, [Set Up My Domain], [Configure SAML Settings for Single Sign-On]

NEW QUESTION 41
Universal Containers (UC) uses Salesforce to allow customers to keep track of the order status. The customers can log in to Salesforce using external authentication providers, such as Facebook and Google. UC is also leveraging the App Launcher to let customers access an of platform application for generating shipping labels. The label generator application uses OAuth to provide users access. What license type should an Architect recommend for the customers?

A. Customer Community license
B. Identity license
C. Customer Community Plus license
D. External Identity license

Answer: D

Explanation:
D is correct because External Identity license is designed for customers who need to log in to Salesforce using external authentication providers, such as Facebook and Google. External Identity license also supports App Launcher, which allows customers to access other applications from Salesforce using OAuth or OpenID Connect .
A is incorrect because Customer Community license is designed for customers who need to access data and records in Salesforce, such as cases, accounts, and contacts. Customer Community license does not support App Launcher or external authentication providers.
B is incorrect because Identity license is designed for employees who need to access multiple applications from Salesforce using SSO and App Launcher. Identity license does not support external authentication providers or customer data access.
C is incorrect because Customer Community Plus license is designed for customers who need to access data and records in Salesforce, as well as collaborate with other customers and partners. Customer Community Plus license does not support App Launcher or external authentication providers.
References: : Salesforce Licensing Module - Trailhead : Free Salesforce
Identity-and-Access-Management-Architect Questions … : Salesforce Licensing Module - Trailhead : Salesforce Licensing Module - Trailhead : Salesforce Licensing Module - Trailhead

NEW QUESTION 45
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 49
Universal containers (UC) has built a custom based Two-factor Authentication (2fa) system for their existing on-premise applications. Thru are now implementing salesforce and would like to enable a Two-factor login process for it, as well. What is the recommended solution an architect should consider?

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

Answer: D

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

NEW QUESTION 53
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 58
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 61
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 63
Universal Containers has multiple Salesforce instances where users receive emails from different instances. Users should be logged into the correct Salesforce instance authenticated by their IdP when clicking on an email link to a Salesforce record.
What should be enabled in Salesforce as a prerequisite?

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

Answer: A

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

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

References:

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

NEW QUESTION 66
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 71
Northern Trail Outfitters (NTO) uses the Customer 360 Platform implemented on Salesforce Experience Cloud. The development team in charge has learned of a contactless user feature, which can reduce the overhead of managing customers and partners by creating users without contact information.
What is the potential impact to the architecture if NTO decides to implement this feature?

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

Answer: B

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

NEW QUESTION 76
An Identity and Access Management (IAM) architect is tasked with unifying multiple B2C Commerce sites and an Experience Cloud community with a single identity. The solution needs to support more than 1,000 logins per minute.
What should the IAM do to fulfill this requirement?

A. Configure both the community and the commerce sites as OAuth2 RPs (relying party) with an external identity provider.
B. Configure community as a Security Assertion Markup Language (SAML) identity provider and enable Just-in-Time Provisioning to B2C Commerce.
C. Create a default account for capturing all ecommerce contacts registered on the community because person Account is not supported for this case.
D. Confirm performance considerations with Salesforce Customer Support due to high peaks.

Answer: A

Explanation:

According to the Salesforce documentation2, OAuth2 RPs (relying parties) are applications that use OAuth 2.0 for authentication and authorization with an external identity provider. This allows users to log in to multiple applications with a single identity provider account. The identity provider issues an access token to the relying party, which can be used to access protected resources on behalf of the user. This solution can support high volumes of logins per minute and unify multiple B2C Commerce sites and an Experience Cloud community with a single identity.

NEW QUESTION 78
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 80
A multinational industrial products manufacturer is planning to implement Salesforce CRM to manage their business. They have the following requirements:
* 1. They plan to implement Partner communities to provide access to their partner network .
* 2. They have operations in multiple countries and are planning to implement multiple Salesforce orgs.
* 3. Some of their partners do business in multiple countries and will need information from multiple Salesforce communities.
* 4. They would like to provide a single login for their partners.
How should an Identity Architect solution this requirement with limited custom development?

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

Answer: A

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

NEW QUESTION 83
Universal Containers built a custom mobile app for their field reps to create orders in Salesforce. OAuth is used for authenticating mobile users. The app is built in such a way that when a user session expires after Initial login, a new access token is obtained automatically without forcing the user to log in again. While that improved the field reps' productivity, UC realized that they need a "logout" feature.
What should the logout function perform in this scenario, where user sessions are refreshed automatically?

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

Answer: A

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

- Certification Exam Guide
- Revoke OAuth Tokens

NEW QUESTION 86
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 89
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 92
Universal Containers (UC) wants its closed Won opportunities to be synced to a Data warehouse in near real time. UC has implemented Outbound Message to enable near real-time data sync. UC wants to ensure that communication between Salesforce and Target System is secure. What certificate is sent along with the Outbound Message?

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

Answer: C

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

NEW QUESTION 95
A technology enterprise is setting up an identity solution with an external vendors wellness application for its employees. The user attributes need to be returned to the wellness application in an ID token.
Which authentication mechanism should an identity architect recommend to meet the requirements?

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

Answer: A

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

NEW QUESTION 98
Universal Containers (UC) is rolling out its new Customer Identity and Access Management Solution built on top of its existing Salesforce instance. UC wants to allow customers to login using Facebook, Google, and other social sign-on providers.
How should this functionality be enabled for UC, assuming ail social sign-on providers support OpenID Connect?

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

Answer: A

Explanation:
To allow customers to login using Facebook, Google, and other social sign-on providers, the identity architect should configure an authentication provider and a registration handler for each social sign-on provider. Authentication providers are configurations that enable users to authenticate with an external identity provider and access Salesforce resources. OpenID Connect is a protocol that allows users to sign in with an external identity provider, such as Facebook or Google, and

access Salesforce resources. To enable this, the identity architect needs to configure an OpenID Connect Authentication Provider in Salesforce and link it to a connected app. A registration handler is a class that implements the Auth.RegistrationHandler interface and defines how to create or update users in Salesforce based on the information from the external identity provider. The registration handler can also be used to link the user's social identity with their Salesforce identity and prevent duplicate accounts. References: OpenID Connect Authentication Providers, Social Sign-On with OpenID Connect, Create a Custom Registration Handler

NEW QUESTION 101
The executive sponsor for an organization has asked if Salesforce supports the ability to embed a login widget into its service providers in order to create a more seamless user experience.
What should be used and considered before recommending it as a solution on the Salesforce Platform?

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

Answer: D

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

NEW QUESTION 104
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 107
Universal Containers (UC) is looking to build a Canvas app and wants to use the corresponding Connected App to control where the app is visible. Which two options are correct in regards to where the app can be made visible under the Connected App setting for the Canvas app? Choose 2 answers

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

Answer: CD

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

NEW QUESTION 109
Universal Containers (UC) is building a custom Innovation platform on their Salesforce instance. The Innovation platform will be written completely in Apex and

Visualforce and will use custom objects to store the Data. UC would like all users to be able to access the system without having to log in with Salesforce credentials. UC will utilize a third-party idp using SAML SSO. What is the optimal Salesforce licence type for all of the UC employees?

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

Answer: D

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

NEW QUESTION 112
What item should an Architect consider when designing a Delegated Authentication implementation?

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

Answer: A

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

NEW QUESTION 116
Northern Trail Outfitters (NTO) is planning to implement a community for its customers using Salesforce Experience Cloud. Customers are not able to self-register. NTO would like to have customers set their own passwords when provided access to the community.
Which two recommendations should an identity architect make to fulfill this requirement? Choose 2 answers

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

Answer: CD

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

NEW QUESTION 118
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 119
Universal Containers (UC) has built a custom token-based Two-factor authentication (2FA) system for their existing on-premise applications. They are now

implementing Salesforce and would like to enable a
Two-factor login process for it, as well. What is the recommended solution as Architect should consider?

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

Answer: D

Explanation:
The recommended solution for UC to enable a two-factor login process for Salesforce and their existing
on-premise applications is to replace the custom 2FA system with Salesforce 2FA for on-premise applications and Salesforce. Salesforce 2FA is a feature that requires users to verify their identity with a second factor, such as a verification code or a mobile app, after entering their username and password. Salesforce 2FA can be enabled for both Salesforce and on-premise applications by using one of the following methods:

- Use Salesforce Authenticator, a mobile app that generates verification codes or sends push notifications to users' devices.
- Use a third-party authenticator app, such as Google Authenticator or Microsoft Authenticator, that generates verification codes based on a shared secret key.
- Use a verification code sent by email or SMS to users' registered email address or phone number.
- Use a U2F security key, such as YubiKey, that plugs into users' devices and provides a physical token. By replacing the custom 2FA system with Salesforce 2FA, UC can benefit from the following advantages:
- Improved security and compliance by using a standard and proven 2FA solution that protects against
phishing, credential theft, and brute force attacks.
- Reduced complexity and cost by eliminating the need to maintain a custom 2FA system and integrating it with Salesforce.
- Enhanced user experience and convenience by providing multiple options for verifying identity and allowing users to remember trusted devices or browsers.

The other options are not recommended solutions for this scenario. Using the custom 2FA system for
on-premise applications and native 2FA for Salesforce would create inconsistency and confusion for users who have to use different methods of verification for different applications. Replacing the custom 2FA system with an AppExchange app that supports on-premise applications and Salesforce would require UC to find an app that meets their specific needs and pay for its license and maintenance. Using custom login flows to connect to the existing custom 2FA system for use in Salesforce would require UC to write custom code and logic to invoke the custom 2FA system from Salesforce, which could introduce security and performance issues. References: [Two-Factor Authentication], [Salesforce Authenticator], [Third-Party Authenticator Apps], [Verification Code via Email or SMS], [U2F Security Keys], [Custom Login Flows]

NEW QUESTION 122
A security architect is rolling out a new multi-factor authentication (MFA) mandate, where all employees must go through a secure authentication process before accessing Salesforce. There are multiple Identity Providers (IdP) in place and the architect is considering how the "Authentication Method Reference" field (AMR) in the Login History can help.
Which two considerations should the architect keep in mind? Choose 2 answers

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

Answer: AB

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

NEW QUESTION 124
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 125
Universal containers (UC) has a mobile application that calls the salesforce REST API. In order to prevent users from having to enter their credentials everytime they use the app, UC has enabled the use of refresh Tokens as part of the salesforce connected App and updated their mobile app to take advantage of the refresh token. Even after enabling the refresh token, Users are still complaining that they have to enter their credentials once a day. What is the most likely cause of the issue?

A. The Oauth authorizations are being revoked by a nightly batch job.

B. The refresh token expiration policy is set incorrectly in salesforce
C. The app is requesting too many access Tokens in a 24-hour period
D. The users forget to check the box to remember their credentials.

Answer: B

Explanation:
The most likely cause of the issue is that the refresh token expiration policy is set incorrectly in Salesforce. A refresh token is a credential that allows a connected app to obtain a new access token when the previous one expires1. The refresh token expiration policy determines how long a refresh token is valid for2. If the policy is set to a short duration, such as 24 hours, the users have to enter their credentials once a day to get a new refresh token. To prevent this, the policy should be set to a longer duration, such as “Refresh token is valid until revoked” or "Refresh token expires after 90 days of inactivity"2.
References: OAuth 2.0 Refresh Token Flow, Manage OAuth Access Policies for a Connected App

NEW QUESTION 128
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 130
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 134
In an SP-Initiated SAML SSO setup where the user tries to access a resource on the Service Provider, What HTTP param should be used when submitting a SAML Request to the Idp to ensure the user is returned to the intended resourse after authentication?

A. RedirectURL
B. RelayState
C. DisplayState
D. StartURL

Answer: B

Explanation:
The HTTP parameter that should be used when submitting a SAML request to the IdP to ensure the user is returned to the intended resource after authentication is RelayState. RelayState is an optional parameter that can be used to preserve some state information across the SSO process. For example, RelayState can be used to specify the URL of the resource that the user originally requested on the SP before being redirected to the IdP for authentication. After the IdP validates the user’s identity and sends back a SAML response, it also sends back the RelayState parameter with the same value as it received from the SP. The SP then uses the RelayState value to redirect the user to the intended resource after validating the SAML response. The other options are not valid HTTP parameters for this purpose. RedirectURL, DisplayState, and StartURL are not standard SAML parameters and they are not supported by Salesforce as SP or IdP. References: [SAML SSO Flows], [RelayState Parameter]

NEW QUESTION 138
Universal Containers would like its customers to register and log in to a portal built on Salesforce Experience Cloud. Customers should be able to use their Facebook or Linkedln credentials for ease of use.
Which three steps should an identity architect take to implement social sign-on? Choose 3 answers

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

Answer: BCE

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

- Create authentication providers for both Facebook and LinkedIn. Authentication providers are configurations that enable users to authenticate with an external identity provider and access Salesforce resources. Salesforce provides predefined authentication providers for some common identity providers, such as Facebook and LinkedIn, which can be easily configured with minimal customization.
- Check “Facebook” and “LinkedIn” under Login Page Setup. Login Page Setup is a setting that allows administrators to customize the login page for Experience Cloud sites. By checking “Facebook” and “LinkedIn”, the identity architect can enable social sign-on buttons for these identity providers on the login page.
- Update the default registration handlers to create and update users. Registration handlers are classes that implement the Auth.RegistrationHandler interface and define how to create or update users in Salesforce based on the information from the external identity provider. The identity architect can update the default registration handlers to link the user’s social identity with their Salesforce identity and prevent duplicate accounts. References: Authentication Providers, Social Sign-On with Authentication Providers, Login Page Setup, Create a Custom Registration Handler

NEW QUESTION 142
Universal Containers (UC) has an existing Salesforce org configured for SP-Initiated SAML SSO with their Idp. A second Salesforce org is being introduced into the environment and the IT team would like to ensure they can use the same Idp for new org. What action should the IT team take while implementing the second org?

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

Answer: B

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

NEW QUESTION 144
Containers (UC) uses a legacy Employee portal for their employees to collaborate. Employees access the portal from their company’s internal website via SSO. It is set up to work with SiteMinder and Active Directory. The Employee portal has features to support posing ideas. UC decides to use Salesforce Ideas for voting and better tracking purposes. To avoid provisioning users on Salesforce, UC decides to integrate Employee portal ideas with Salesforce idea through the API. What is the role of Salesforce in the context of SSO, based on this scenario?

A. Service Provider, because Salesforce is the application for managing ideas.
B. Connected App, because Salesforce is connected with Employee portal via API.
C. Identity Provider, because the API calls are authenticated by Salesforce.
D. An independent system, because Salesforce is not part of the SSO setup.

Answer: D

Explanation:
D is correct because Salesforce is an independent system that is not part of the SSO setup between the Employee portal and Active Directory. Salesforce does not act as an IdP or an SP for the SSO, nor does it use a connected app to integrate with the Employee portal. Salesforce only exposes its API to allow the Employee portal to access its ideas feature.
A is incorrect because Salesforce is not a service provider for the SSO. The SSO is between the Employee portal and Active Directory, not between the Employee portal and Salesforce.
B is incorrect because Salesforce is not a connected app for the SSO. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect1. The Employee portal does not use any of these protocols to integrate with Salesforce, but only uses its API.
C is incorrect because Salesforce is not an identity provider for the SSO. The IdP is the system that authenticates users and issues tokens or assertions to allow access to other systems. In this scenario, the IdP is Active Directory, not Salesforce.
References: 1: Oauth Authorization flows in Salesforce - Apex Hours

NEW QUESTION 146
Northern Trail Outfitters (NTO) has a requirement to ensure all user logins include a single multi-factor authentication (MFA) prompt. Currently, users are allowed the choice to login with a username and password or via single sign-on against NTO's corporate Identity Provider, which includes built-in MFA.
Which configuration will meet this requirement?

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

Answer: C

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

NEW QUESTION 151
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 156
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 157
Universal containers (UC) would like to enable SAML-BASED SSO for a salesforce partner community. UC has an existing ldap identity store and a third-party portal. They would like to use the existing portal as the primary site these users' access, but also want to allow seamless access to the partner community. What SSO flow should an architect recommend?

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

Answer: B

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

NEW QUESTION 159
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

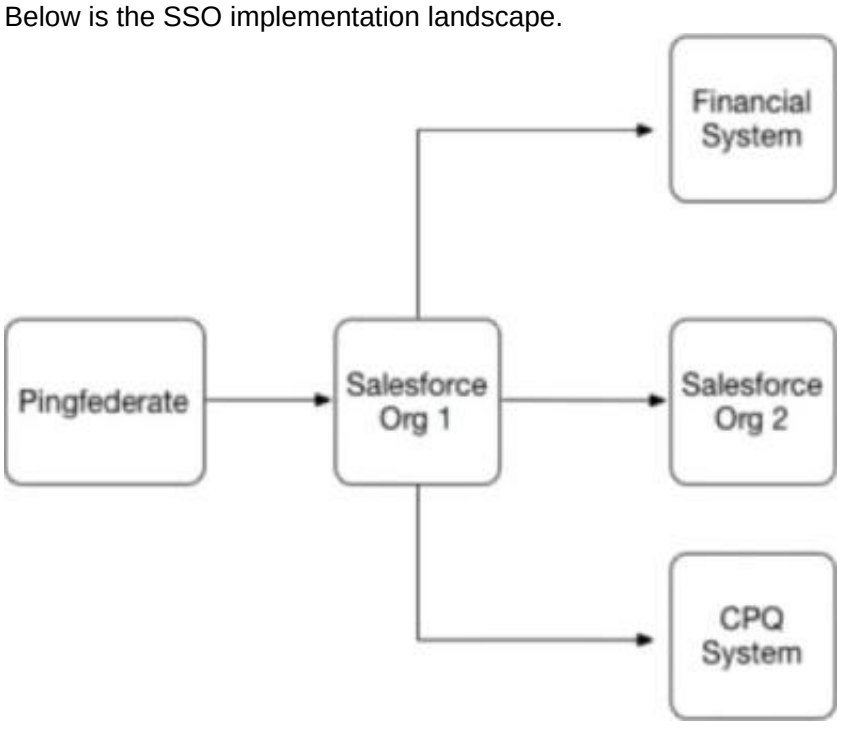
NEW QUESTION 161
Universal containers(UC) has decided to build a new, highly sensitive application on Force.com platform. The security team at UC has decided that they want users to provide a fingerprint in addition to username/Password to authenticate to this application. How can an architect support 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 163
Universal Containers (UC) has implemented SAML-based Single Sign-On to provide seamless access to its Salesforce Orgs, financial system, and CPQ system. Below is the SSO implementation landscape.



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

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

Answer: B

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

NEW QUESTION 166

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

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

Answer: BC

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

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

References:

- Customer 360 Identity
- Customer 360 Identity Benefits

NEW QUESTION 168
Universal Containers (UC) is using a custom application that will act as the Identity Provider and will generate SAML assertions used to log in to Salesforce. UC is considering including custom parameters in the SAML assertion. These attributes contain sensitive data and are needed to authenticate the users. The assertions are submitted to salesforce via a browser form post. The majority of the users will only be able to access Salesforce via UC's corporate network, but a subset of admins and executives would be allowed access from outside the corporate network on their mobile devices. Which two methods should an Architect consider to ensure that the sensitive data cannot be tampered with, nor accessible to anyone while in transit?

A. Use the Identity Provider's certificate to digitally sign and Salesforce's Certificate to encrypt the payload.
B. Use Salesforce's Certificate to digitally sign the SAML Assertion and a Mobile Device Management client on the users' mobile devices.
C. Use the Identity provider's certificate to digitally Sign and the Identity provider's certificate to encrypt the payload.
D. Use a custom login flow to retrieve sensitive data using an Apex callout without including the attributes in the assertion.

Answer: CD

Explanation:
Using the identity provider’s certificate to digitally sign and encrypt the payload, and using a custom login flow to retrieve sensitive data using an Apex callout without including the attributes in the assertion are two methods that can ensure that the sensitive data cannot be tampered with, nor accessible to anyone while in transit. Option A is not a good choice because using Salesforce’s certificate to encrypt the payload may not work, as Salesforce does not support encrypted SAML assertions. Option B is not a good choice because using Salesforce’s certificate to digitally sign the SAML assertion may not be necessary, as Salesforce does not validate digital signatures on SAML assertions. Also, using a mobile device management client on the users’ mobile devices may not be relevant, as it does not affect how the sensitive data is transmitted between the identity provider and Salesforce.
References: [Single Sign-On Implementation Guide], [Customizing User Authentication with Login Flows]

NEW QUESTION 169
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 173
A client is planning to rollout multi-factor authentication (MFA) to its internal employees and wants to understand which authentication and verification methods meet the Salesforce criteria for secure authentication.
Which three functions meet the Salesforce criteria for secure mfa? Choose 3 answers

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

Answer: BCE

Explanation:
Multi-factor authentication (MFA) is a security feature that requires users to verify their identity with two or more factors when they log in to Salesforce4. Salesforce supports several types of authentication and verification methods that meet the criteria for secure MFA, such as5:

- Username and password + security key: A security key is a physical device that plugs into a USB port or connects wirelessly to your computer or mobile device. It generates a unique code that you use to verify your identity when you log in to Salesforce5.
- Third-party single sign-on with Mobile Authenticator app: Single sign-on (SSO) is an authentication method that allows users to access multiple applications with one login and one set of credentials. A mobile authenticator app is an app that generates temporary codes or sends push notifications that you use to verify your identity when you log in to Salesforce via SSO5.
- Lightning Login: Lightning Login is an authentication method that allows users to log in to Salesforce without entering a password. Instead, users scan a QR code with their mobile device or click an email
link that they receive when they try to log in. Then they use their fingerprint, face ID, or PIN to verify their identity on their mobile device5.

References:

- Multi-Factor Authentication
- Authentication and Verification Methods

NEW QUESTION 177
Universal Containers wants to implement Single Sign-on for a Salesforce org using an external Identity Provider and corporate identity store.
What type of authentication flow is required to support deep linking'

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

Answer: B

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

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

References:

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

NEW QUESTION 181
Universal Containers (UC) uses Salesforce for its customer service agents. UC has a proprietary system for order tracking which supports Security Assertion Markup Language (SAML) based single sign-on. The VP of customer service wants to ensure only active Salesforce users should be able to access the order tracking system which is only visible within Salesforce.
What should be done to fulfill the requirement? Choose 2 answers

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

Answer: AD

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

- Setup Salesforce as an identity provider (IdP) for order tracking. An IdP is the system that performs authentication and passes the user's identity and authorization level to the SP, which trusts the IdP and authorizes the user to access the requested resource. To set up Salesforce as an IdP, you need to enable the Identity Provider feature, download the IdP certificate, and configure the SAML settings.
- Setup order tracking as a Canvas app in Salesforce to POST IdP initiated SAML assertion. A Canvas app is an application that can be embedded within a Salesforce page and interact with Salesforce data and APIs. To set up order tracking as a Canvas app, you need to create a connected app for order tracking in Salesforce, enable SAML and configure the SAML settings, such as the entity ID, ACS URL, and subject type. You also need to enable IdP initiated SAML assertion POST binding for the connected app, which allows Salesforce to initiate the SSO process by sending a SAML assertion to order tracking.

References:

- [SAML Single Sign-On]
- [Set Up Your Domain as an Identity Provider]
- [Canvas Apps]
- [Create a Connected App for Your Canvas App]
- [IdP Initiated SAML Assertion POST Binding]

NEW QUESTION 185

Northern Trail Outfitters recently acquired a company. Each company will retain its Identity Provider (IdP). Both companies rely extensively on Salesforce processes that send emails to users to take specific actions in Salesforce.
How should the combined companys' employees collaborate in a single Salesforce org, yet authenticate to the appropriate IdP?

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

Answer: D

Explanation:
To allow employees to collaborate in a single Salesforce org, yet authenticate to the appropriate IdP, the identity architect should enable each IdP as a login option in the MyDomain Authentication Service settings. Users will then click on the appropriate IdP button. MyDomain is a feature that allows administrators to customize the Salesforce login URL with a unique domain name. Authentication Service is a setting that allows administrators to enable different authentication options for users, such as social sign-on or single
sign-on with an external IdP. By enabling each IdP as a login option in the MyDomain Authentication Service settings, the identity architect can provide a user-friendly and secure way for employees to log in to Salesforce using their preferred IdP. References: MyDomain, Authentication Service

NEW QUESTION 189
Universal Containers (UC) would like its community users to be able to register and log in with Linkedin or Facebook Credentials. UC wants users to clearly see Facebook &Linkedin Icons when they register and login. What are the two recommended actions UC can take to achieve this Functionality? Choose 2 answers

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

Answer: AB

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

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

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

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

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

NEW QUESTION 194
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

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

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

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

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

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