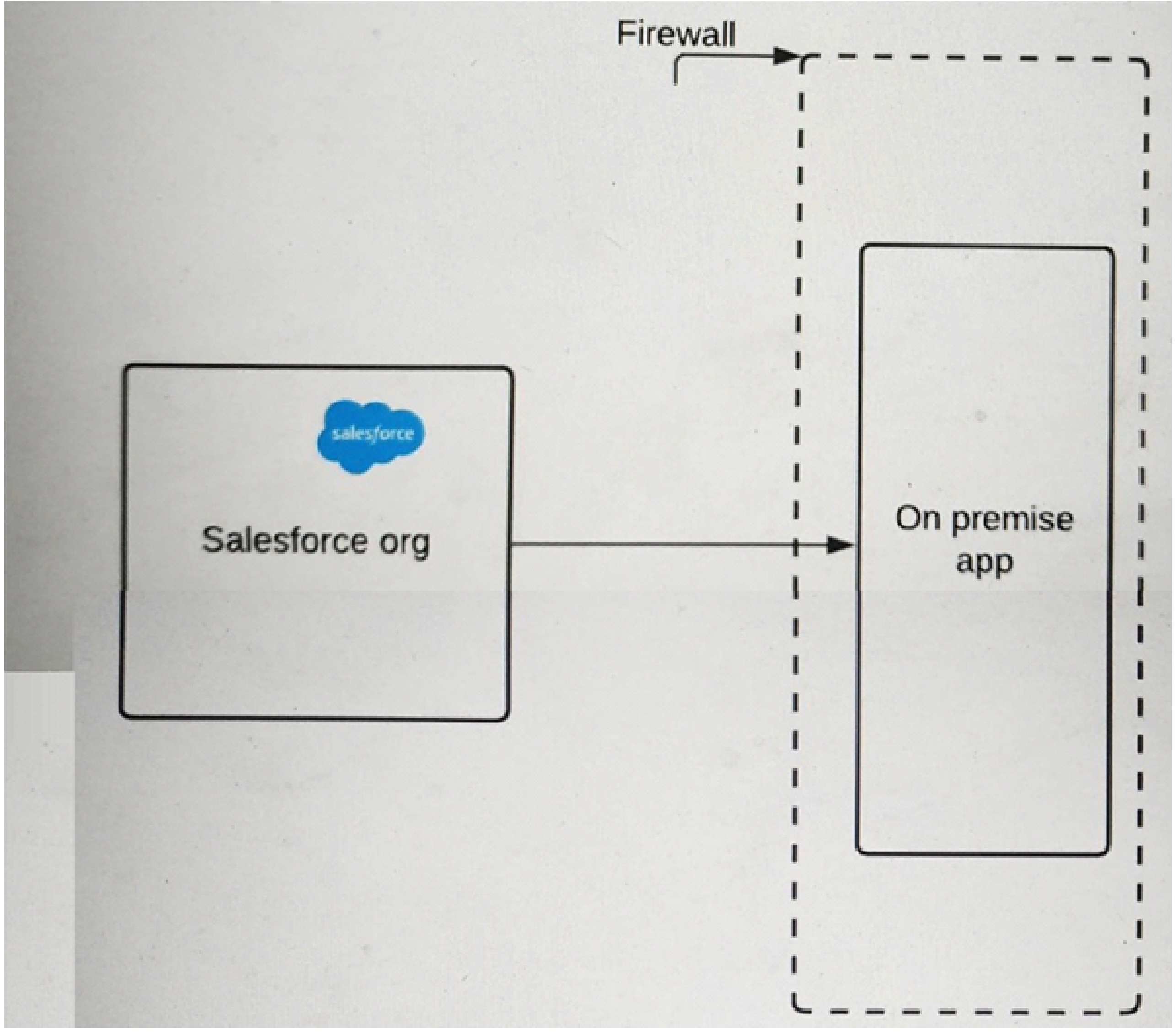
# Salesforce

## Exam Questions Identity-and-Access-Management-Architect

Salesforce Certified Identity and Access Management Architect (SU23)

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



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

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

**Answer:** C

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

**NEW QUESTION 2**
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 3**
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 4**
A global company's Salesforce Identity Architect is reviewing its Salesforce production org login history and is seeing some intermittent Security Assertion Markup Language (SAML SSO) 'Replay Detected and Assertion Invalid' login errors.
Which two issues would cause these errors?
Choose 2 answers

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

**Answer:** CD

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

**NEW QUESTION 5**
Universal Containers (UC) has a strict requirement to authenticate users to Salesforce using their mainframe credentials. The mainframe user store cannot be accessed from a SAML provider. UC would also like to have users in Salesforce created on the fly if they provide accurate mainframe credentials.
How can the Architect meet these requirements?

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

**Answer:** C

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

**NEW QUESTION 6**
Universal containers (UC) uses an internal company portal for their employees to collaborate. UC decides to use salesforce ideas and provide the ability for employees to post ideas from the company portal. They use SAML-BASED SSO to get into the company portal and would like to leverage it to access salesforce. Most of the users don't exist in salesforce and they would like the user records created in salesforce communities the first time they try to access salesforce. What recommendation should an architect make to meet this requirement?

A. Use on-the-fly provisioning
B. Use just-in-time provisioning
C. Use salesforce APIs to create users on the fly
D. Use Identity connect to sync users

**Answer:** B

**Explanation:**
Just-in-time provisioning is a feature that allows Salesforce to create user accounts automatically when users log in for the first time via an external identity provider. This way, UC can avoid creating user records manually or synchronizing them with another system. On-the-fly provisioning is not a valid term in Salesforce. Salesforce APIs can be used to create users programmatically, but they are not related to SSO. Identity Connect is a tool that can sync users between Salesforce and Active Directory, but it is not required for SSO.
References: Certification - Identity and Access Management Architect - Trailhead, [Just-in-Time Provisioning for SAML and OpenID Connect]

**NEW QUESTION 7**
Universal Containers (UC) is building a customer community and will allow customers to authenticate using Facebook credentials. The First time the user authenticating using Facebook, UC would like a customer account created automatically in their accounting system. The accounting system has a web service accessible to Salesforce for the creation of accounts. How can the Architect meet these requirements?

A. Create a custom application on Heroku that manages the sign-on process from Facebook.
B. Use JIT Provisioning to automatically create the account in the accounting system.

C. Add an Apex callout in the registration handler of the authorization provider.
D. Use OAuth JWT flow to pass the data from Salesforce to the Accounting System.

**Answer:** C

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

**NEW QUESTION 8**
Which two capabilities does My Domain enable in the context of a SAML SSO configuration? Choose 2 answers

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

**Answer:** BC

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

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

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

**NEW QUESTION 9**
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 10**
How should an Architect automatically redirect users to the login page of the external Identity provider when using an SP-Initiated SAML flow with Salesforce as a Service Provider?

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

**Answer:** D

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

Configuration Settings

**NEW QUESTION 10**
Universal containers (UC) is setting up their customer Community self-registration process. They are uncomfortable with the idea of assigning new users to a default account record. What will happen when customers self-register in the community?

A. The self-registration process will produce an error to the user.
B. The self-registration page will ask user to select an account.
C. The self-registration process will create a person Account record.
D. The self-registration page will create a new account record.

**Answer:** C

**Explanation:**
When customers self-register in the community, the self-registration process will create a person account record. A person account is a special type of account that combines both account and contact information in one record. This allows customers to have their own individual accounts without being associated with a default account. Option A is not a good choice because the self-registration process will not produce an error to the user, unless there is some configuration or validation issue. Option B is not a good choice because the self-registration page will not ask user to select an account, unless it is customized to do so. Option D is not a good choice because the self-registration page will not create a new account record, unless it is customized to do so.
References: [How to Provision Salesforce Communities Users], [Salesforce Licensing]

**NEW QUESTION 14**
Which two are valid choices for digital certificates when setting up two-way SSL between Salesforce and an external system. Choose 2 answers

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

**Answer:** CD

**Explanation:**
Two-way SSL is a method of mutual authentication between two parties using digital certificates. A digital certificate is an electronic document that contains information about the identity of the certificate owner and a public key that can be used to verify their signature. A digital certificate can be either self-signed or CA-signed. A self-signed certificate is created and signed by its owner, while a CA-signed certificate is created by its owner but signed by a trusted Certificate Authority (CA). For setting up two-way SSL between Salesforce and an external system, two valid choices for digital certificates are:
> Use a self-signed certificate for Salesforce and a self-signed certificate for the external system. This option is simple and cost-effective, but requires both parties to trust each other’s self-signed certificates explicitly.
> Use a self-signed certificate for Salesforce and a trusted CA-signed certificate for the external system.
This option is more secure and reliable, but requires Salesforce to trust the CA that signed the external system’s certificate implicitly.
References: Know more about all the SSL certificates that are supported by Salesforce, two way ssl. How to

**NEW QUESTION 18**
Northern Trail Outfitters (NTO) believes a specific user account may have been compromised. NTO inactivated the user account and needs U perform a forensic analysis and identify signals that could Indicate a breach has occurred.
What should NTO's first step be in gathering signals that could indicate account compromise?

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

**Answer:** D

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

**NEW QUESTION 22**
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 26**
Northern Trail Outfitters would like to use a portal built on Salesforce Experience Cloud for customer self-service. Guests of the portal be able to self-register, but be unable to automatically be assigned to a contact record until verified. External Identity licenses have been purchased for the project.
After registered guests complete an onboarding process, a flow will create the appropriate account and contact records for the user.
Which three steps should an identity architect follow to implement the outlined requirements? Choose 3 answers

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

**Answer:** ABE

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

**NEW QUESTION 29**
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 33**
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 35**
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 39**

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

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

**Answer:** AB

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

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

**NEW QUESTION 43**

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

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

**Answer:** B

**Explanation:**
The OAuth 2.0 Device Flow is a type of authorization flow that allows users to register an IoT device with limited display input or capabilities, such as a smart TV, a printer, or a smart speaker1. The device flow works as follows1:

- The device displays or reads out a verification code and a verification URL to the user.
- The user visits the verification URL on another device, such as a smartphone or a laptop, and enters the verification code.
- The user logs in to Salesforce and approves the device.
- The device polls Salesforce for an access token using the verification code.
- Salesforce returns an access token to the device, which can then access Salesforce APIs.

References:

- OAuth 2.0 Device Flow

**NEW QUESTION 44**

A company with 15,000 employees is using Salesforce and would like to take the necessary steps to highlight or curb fraudulent activity.
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 Forensics
B. Login Report
C. Login Inspector
D. Login History

**Answer:** A

**Explanation:**
To track login data and highlight or curb fraudulent activity, the identity architect should use Login Forensics. Login Forensics is a tool that analyzes login history data and provides insights into user login patterns, such as average number of logins, login outliers, login anomalies, and login risk scores. Login Forensics can help identify suspicious or malicious login attempts and take preventive actions. References: Login Forensics, Login Forensics Implementation Guide

**NEW QUESTION 49**

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 54**
Northern Trail Outfitters (NTO) is planning to build a new customer service portal and wants to use passwordless login, allowing customers to login with a one-time passcode sent to them via email or SMS.
How should the quantity of required Identity Verification Credits be estimated?

A. Each community comes with 10,000 Identity Verification Credits per month and only customers with more than 10,000 logins a month should estimate additional SMS verifications needed.
B. Identity Verification Credits are consumed with each SMS (text message) sent and should be estimated based on the number of login verification challenges for SMS verification users.
C. Identity Verification Credits are consumed with each verification sent and should be estimated based on the number of loginsthat will incur a verification challenge.
D. Identity Verification Credits are a direct add-on license based on the number of existing member-based or login-based Community licenses.

**Answer:** B

**Explanation:**
Identity Verification Credits are units that are consumed when Salesforce sends verification messages to users via email or SMS. To use passwordless login, customers need to receive a one-time passcode via email or SMS that they can use to log in to the customer service portal. Therefore, Identity Verification Credits are consumed with each SMS (text message) sent and should be estimated based on the number of login verification challenges for SMS verification users. Email verification does not consume Identity Verification Credits. References: Identity Verification Credits, Passwordless Login

**NEW QUESTION 55**
The security team at Universal containers(UC) has identified exporting reports as a high-risk action and would like to require users to be logged into salesforce with their active directory (AD) credentials when doing so. For all other uses of Salesforce, Users should be allowed to use AD credentials or salesforce credentials.
What solution should be recommended to prevent exporting reports except when logged in using AD credentials while maintaining the ability to view reports when logged in with salesforce credentials?

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

**Answer:** B

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

**NEW QUESTION 58**
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 60**
Which two statements are capable of Identity Connect? Choose 2 answers

A. Synchronization of Salesforce Permission Set Licence Assignments.
B. Supports both Identity-Provider-Initiated and Service-Provider-Initiated SSO.
C. Support multiple orgs connecting to multiple Active Directory servers.
D. Automated user synchronization and de-activation.

**Answer:** BD

**Explanation:**
The two statements that are capabilities of Identity Connect are:

> It supports both identity-provider-initiated and service-provider-initiated SSO. Identity Connect is a desktop application that integrates Salesforce with Microsoft Active Directory (AD) and enables single sign-on (SSO) between the two systems. Identity Connect supports both identity-provider-initiated SSO, which is when the user starts at the AD site and then is redirected to Salesforce with a SAML assertion, and service-provider-initiated SSO, which is when the user starts at the Salesforce site and then is redirected to AD for authentication.

> It enables automated user synchronization and deactivation. Identity Connect allows administrators to synchronize user accounts and attributes between AD and Salesforce, either manually or on a scheduled basis. Identity Connect also allows administrators to deactivate user accounts in Salesforce when they are disabled or deleted in AD, which helps maintain security and compliance.
The other options are not capabilities of Identity Connect. Identity Connect does not support synchronization of Salesforce permission set license assignments, as these are not related to AD attributes. Identity Connect does not support multiple orgs connecting to multiple AD servers, as it can only connect one Salesforce org to one AD domain at a time. References: [Identity Connect], [Identity Connect Features], [Identity Connect User Synchronization], [Identity Connect Single Sign-On]

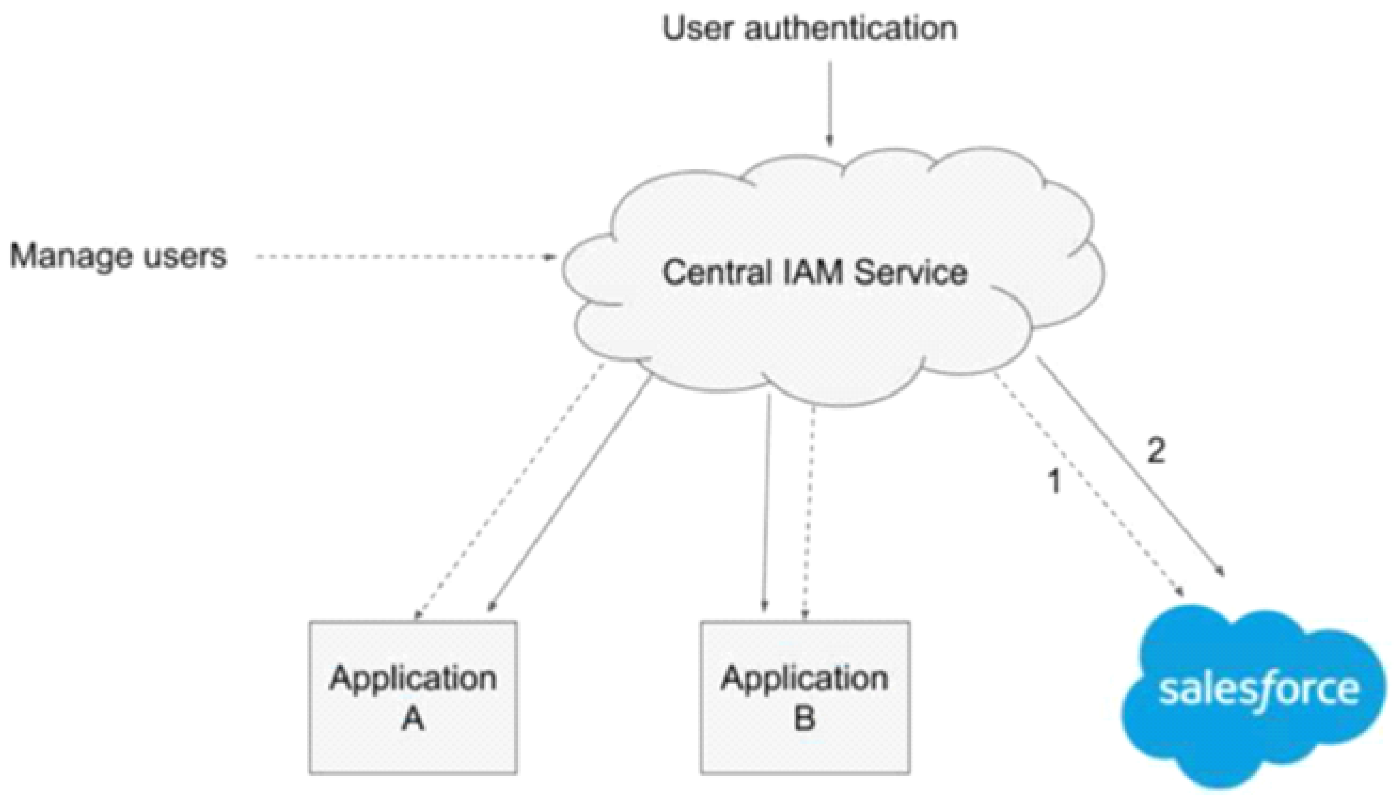
**NEW QUESTION 65**
An identity architect is setting up an integration between Salesforce and a third-party system. The third-party system needs to authenticate to Salesforce and then make API calls against the REST API.
One of the requirements is that the solution needs to ensure the third party service providers connected app in Salesforce mini need for end user interaction and maximizes security.
Which OAuth flow should be used to fulfill the requirement?

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

**Answer:** A

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

**NEW QUESTION 69**
An organization has a central cloud-based Identity and Access Management (IAM) Service for authentication and user management, which must be utilized by all applications as follows:



1 - Change of a user status in the central IAM Service triggers provisioning or deprovisioning in the integrated cloud applications.
2 - Security Assertion Markup Language single sign-on (SSO) is used to facilitate access for users authenticated at identity provider (Central IAM Service).
Which approach should an IAM architect implement on Salesforce Sales Cloud to meet the requirements?

A. A Configure Salesforce as a SAML Service Provider, and enable SCIM (System for Cross-Domain Identity Management) for provisioning and deprovisioning of users.
B. Configure Salesforce as a SAML service provider, and enable Just-in Time (JIT) provisioning and deprovisioning of users.
C. Configure central IAM Service as an authentication provider and extend registration handler to manage provisioning and deprovisioning of users.
D. Deploy Identity Connect component and set up automated provisioning and deprovisioning of users, as well as SAML-based SSO.

**Answer:** A

**Explanation:**

To meet the requirements of using a central cloud-based IAM service for authentication and user management, the IAM architect should implement Salesforce Sales Cloud as a SAML service provider and enable SCIM for provisioning and deprovisioning of users. SAML is a protocol that allows users to authenticate and authorize with an external identity provider and access Salesforce resources. By configuring Salesforce as a SAML service provider, the IAM architect can use the central IAM service as an identity provider and enable single sign-on for users. SCIM is a standard that defines how to manage user identities across different systems. By enabling SCIM in Salesforce, the IAM architect can synchronize user data between the central IAM service and Salesforce and automate user provisioning and deprovisioning based on the changes made in the central IAM service. References: SAML Single Sign-On Settings, SCIM User Provisioning for Connected Apps

**NEW QUESTION 72**
Universal Containers (UC) is looking to purchase a third-party application as an Identity Provider. UC is looking to develop a business case for the purchase in general and has enlisted an Architect for advice. Which two capabilities of an Identity Provider should the Architect detail to help strengthen the business case?
Choose 2 answers

A. The Identity Provider can authenticate multiple applications.
B. The Identity Provider can authenticate multiple social media accounts.
C. The Identity provider can store credentials for multiple applications.
D. The Identity Provider can centralize enterprise password policy.

**Answer:** AD

**Explanation:**
The two capabilities of an identity provider that the architect should detail to help strengthen the business case are that the identity provider can authenticate multiple applications and that the identity provider can centralize enterprise password policy. These capabilities can provide benefits such as reducing login friction, improving user experience, enhancing security, and simplifying administration. Option B is not a good choice because the identity provider can authenticate multiple social media accounts may not be relevant for UC’s business case, as it does not specify how UC will use social media for its identity management. Option C is not a good choice because the identity provider can store credentials for multiple applications may not be desirable or secure for UC’s business case, as it may imply that the identity provider is using password vaulting or federation rather than single sign-on (SSO) or identity federation. References: Identity Management Concepts, [Single Sign-On Implementation Guide]

**NEW QUESTION 74**
Universal Containers (UC) has five Salesforce orgs (UC1, UC2, UC3, UC4, UC5). of Every user that is in UC2, UC3, UC4, and UC5 is also in UC1, however not all users 65* have access to every org. Universal Containers would like to simplify the authentication process such that all Salesforce users need to remember one set of credentials. UC would like to achieve this with the least impact to cost and maintenance. What approach should an Architect recommend to UC?

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

**Answer:** C

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

➢ Purchasing a third-party Identity Provider for all five Salesforce orgs would incur additional cost and maintenance, and would not leverage the existing user base in UC1.

➢ Not setting up JIT user provisioning for other orgs would require manually creating or updating user accounts in each org, which would be time-consuming and error-prone. References: Salesforce as an Identity Provider, Identity Providers and Service Providers, Just-in-Time Provisioning for SAML

**NEW QUESTION 79**
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 81**
Universal containers (UC) has multiple salesforce orgs and would like to use a single identity provider to access all of their orgs. How should UC'S architect enable this behavior?

A. Ensure that users have the same email value in their user records in all of UC's salesforce orgs.
B. Ensure the same username is allowed in multiple orgs by contacting salesforce support.
C. Ensure that users have the same Federation ID value in their user records in all of UC's salesforce orgs.
D. Ensure that users have the same alias value in their user records in all of UC's salesforce orgs.

**Answer:** C

**Explanation:**
The best option for UC's architect to enable the behavior of using a single identity provider to access all of their Salesforce orgs is to ensure that users have the same Federation ID value in their user records in all of UC's Salesforce orgs. The Federation ID is a field on the user object that stores a unique identifier for each user that is consistent across multiple systems. The Federation ID is used by Salesforce to match the user with the SAML assertion that is sent by the identity provider during the single sign-on (SSO) process. By ensuring that users have the same Federation ID value in all of their Salesforce orgs, UC can enable users to log in with the same identity provider and credentials across multiple orgs. The other options are not valid ways to enable this behavior. Ensuring that users have the same email value in their user records in all of UC's Salesforce orgs does not guarantee that they can log in with SSO, as email is not used as a unique identifier by Salesforce. Ensuring the same username is allowed in multiple orgs by contacting Salesforce support is not possible, as username must be unique across all Salesforce orgs. Ensuring that users have the same alias value in their user records in all of UC's Salesforce orgs does not affect the SSO process, as alias is not used as a unique identifier by Salesforce. References: [Federation ID], [SAML SSO with Salesforce as the Service Provider], [Username], [Alias]

**NEW QUESTION 86**
Universal Containers (UC) has an existing web application that it would like to access from Salesforce without requiring users to re-authenticate. The web application is owned UC and the UC team that is responsible for it is willing to add new javascript code and/or libraries to the application. What implementation should an Architect recommend to UC?

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

**Answer:** A

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

**NEW QUESTION 91**
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 93**
How should an Architect force user to authenticate with Two-factor Authentication (2FA) for Salesforce only when not connected to an internal company network?

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

**Answer:** A

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

**NEW QUESTION 95**
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 99**
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 102**
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 105**
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]

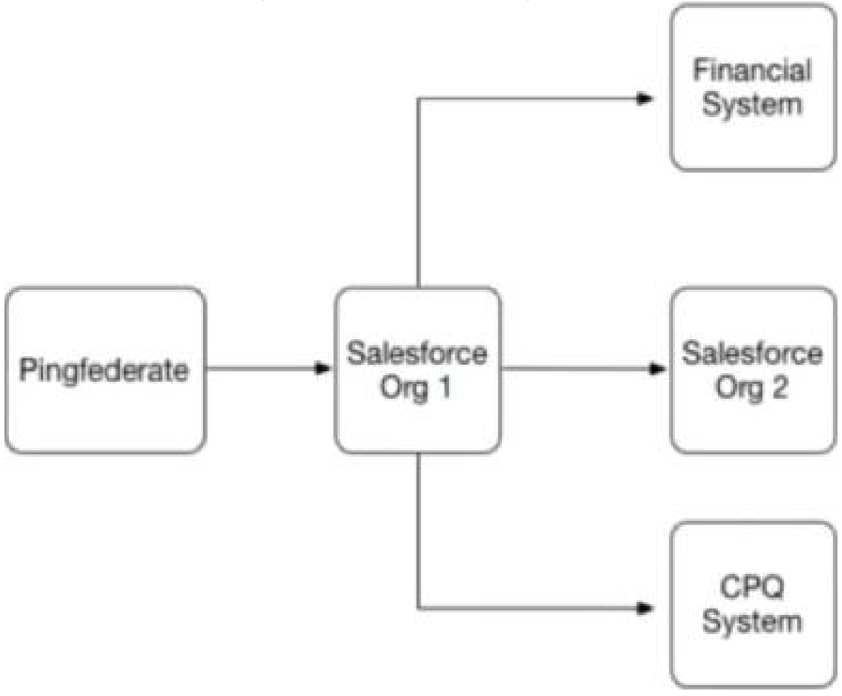
**NEW QUESTION 106**
Northern Trail Outfitters manages application functional permissions centrally as Active Directory groups. The CRM_Superllser and CRM_Reportmg_SuperUser groups should respectively give the user the SuperUser and Reportmg_SuperUser permission set in Salesforce. Salesforce is the service provider to a Security Assertion Markup Language (SAML) identity provider.
Mow should an identity architect ensure the Active Directory groups are reflected correctly when a user accesses Salesforce?

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

**Answer:** B

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

**NEW QUESTION 109**
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 110**
Universal Containers (UC) wants to build a custom mobile app for their field reps to create orders in salesforce. After the first time the users log in, they must be able to access salesforce upon opening the mobile app without being prompted to log in again. What Oauth flows should be considered to support this requirement?

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

**Answer:** AC

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

**NEW QUESTION 114**
Universal containers wants to set up SSO for a selected group of users to access external applications from salesforce through App launcher. Which three steps must be completed in salesforce to accomplish the goal?

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

**Answer:** ABC

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

- Associate user profiles with the connected apps. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect3. To access a connected app, users must have the appropriate permissions assigned to them, either through their profile or a permission set4. UC can associate user profiles with the connected apps to control which users can access which apps.
- Complete My Domain and identity provider setup. My Domain is a feature that lets UC create a custom domain name for their Salesforce org. It is required for setting up SSO with external identity providers. An identity provider is a trusted system that authenticates users for other service providers. UC must set up an identity provider that supports SSO protocols such as SAML or OpenID Connect and configure it to communicate with Salesforce.
- Create connected apps for the external applications. UC must create connected apps for each external application that they want to access from Salesforce through App Launcher. A connected app defines the attributes of the external application, such as its name, logo, description, and callback URL4. It also specifies the SSO protocol and settings that are used to authenticate users and grant access tokens4.
- References: Learn About Connected Apps, Create a Connected App, [Set Up My Domain], Single Sign-On, [Identity Providers and Service Providers]

**NEW QUESTION 118**
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 120**
How should an identity architect automate provisioning and deprovisioning of users into Salesforce from an external system?

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

**Answer:** C

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

**NEW QUESTION 121**
Universal Containers (UC) has Active Directory (AD) as their enterprise identity store and would like to use it for Salesforce user authentication. UC expects to synchronize user data between Salesforce and AD and Assign the appropriate Profile and Permission Sets based on AD group membership. What would be the optimal way to implement SSO?

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

D. Use Salesforce Identity Connect as the Identity Provider.

**Answer:** D

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

**NEW QUESTION 126**
An architect has successfully configured SAML-BASED SSO for universal containers. SSO has been working for 3 months when Universal containers manually adds a batch of new users to salesforce. The new users receive an error from salesforce when trying to use SSO. Existing users are still able to successfully use SSO to access salesforce. What is the probable cause of this behaviour?

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

**Answer:** B

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

**NEW QUESTION 130**
An identity architect wants to secure Salesforce APIs using Security Assertion Markup Language (SAML). For security purposes, administrators will need to authorize the applications that will be consuming the APIs.
Which Salesforce OAuth authorization flow should be used?

A. OAuth 2-0 SAML Bearer Assertion Flow
B. OAuth 2.0 JWT Bearer Flow
C. SAML Assertion Flow
D. OAuth 2.0 User-Agent Flow

**Answer:** C

**Explanation:**
OAuth 2.0 SAML Bearer Assertion Flow is a protocol that allows a client app to obtain an access token from Salesforce by using a SAML assertion instead of an authorization code. The SAML assertion contains information about the client app and the user who wants to access Salesforce APIs. To use this flow, the client app needs to have a connected app configured in Salesforce with the Use Digital Signature option enabled and the “api” OAuth scope assigned. The administrators can authorize the applications that will be consuming the APIs by setting the Permitted Users policy of the connected app to Admin approved users are pre-authorized and assigning profiles or permission sets to the connected app. References: OAuth 2.0 SAML Bearer Assertion Flow, Connected Apps, OAuth Scopes

**NEW QUESTION 132**
An identity architect has been asked to recommend a solution that allows administrators to configure personalized alert messages to users before they land on the Experience Cloud site (formerly known as Community) homepage.
What is recommended to fulfill this requirement with the least amount of customization?

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

**Answer:** B

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

**NEW QUESTION 135**
Universal containers (UC) wants to implement a partner community. As part of their implementation, UC would like to modify both the Forgot password and change password experience with custom branding for their partner community users. Which 2 actions should an architect recommend to UC? Choose 2 answers

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

**Answer:** BC

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

**NEW QUESTION 140**
Universal Containers (UC) uses Global Shipping (GS) as one of their shipping vendors. Regional leads of GS need access to UC's Salesforce instance for reporting damage of goods using Cases. The regional leads also need access to dashboards to keep track of regional shipping KPIs. UC internally uses a third-party cloud analytics tool for capacity planning and UC decided to provide access to this tool to a subset of GS employees. In addition to regional leads, the GS capacity planning team would benefit from access to this tool. To access the analytics tool, UC IT has set up Salesforce as the Identity provider for Internal users and would like to follow the same approach for the GS users as well. What are the most appropriate license types for GS Tregional Leads and the GS Capacity Planners? Choose 2 Answers

A. Customer Community Plus license for GS Regional Leads and External Identity for GS Capacity Planners.
B. Customer Community Plus license for GS Regional Leads and Customer Community license for GS Capacity Planners.
C. Identity License for GS Regional Leads and External Identity license for GS capacity Planners.
D. Customer Community license for GS Regional Leads and Identity license for GS Capacity Planners.

**Answer:** AD

**Explanation:**
The most appropriate license types for GS regional leads and the GS capacity planners are:
➢ Customer Community Plus license for GS regional leads. This license type allows external users, such as customers or partners, to access standard Salesforce objects, such as cases and dashboards, and custom objects in a community. This license type also supports role hierarchy, sharing rules, and reports. This license type is suitable for GS regional leads who need to report damage of goods using cases and access dashboards to track regional shipping KPIs.
➢ External Identity license for GS capacity planners. This license type allows external users to access a limited set of standard Salesforce objects, such as contacts and documents, and custom objects in a community. This license type also supports identity features, such as single sign-on (SSO) and social sign-on. This license type is suitable for GS capacity planners who need to access the third-party cloud analytics tool using Salesforce as the identity provider.
The other options are not appropriate license types for this scenario. Customer Community license for GS capacity planners would not allow them to access the third-party cloud analytics tool using SSO, as this license type does not support identity features. Identity license for GS regional leads would not allow them to access cases and dashboards in the community, as this license type does not support standard Salesforce objects. References: [Customer Community Plus Licenses], [External Identity Licenses], [Customer Community Licenses], [Identity Licenses]

**NEW QUESTION 143**
Northern Trail Outfitters wants to implement a partner community. Active community users will need to review and accept the community rules, and update key contact information for each community member before their annual partner event.
Which approach will meet this requirement?

A. Create tasks for users who need to update their data or accept the new community rules.
B. Create a custom landing page and email campaign asking all community members to login and verify their data.
C. Create a login flow that conditionally prompts users who have not accepted the new community rules and who have missing or outdated information.
D. Add a banner to the community Home page asking users to update their profile and accept the new community rules.

**Answer:** C

**Explanation:**
To meet the requirement of having active community users review and accept the community rules and update key contact information before their annual partner event, the identity architect should create a login flow that conditionally prompts users who have not accepted the new community rules and who have missing or outdated information. A login flow is a custom post-authentication process that can be used to add additional screens or logic after a user logs in to Salesforce. By creating a login flow, the identity architect can check the user’s status and information and display the appropriate screens for them to review and accept the community rules and update their contact information. References: Login Flows, Create a Login Flow

**NEW QUESTION 144**
Universal Container's (UC) identity architect needs to recommend a license type for their new Experience Cloud site that will be used by external partners (delivery providers) for reviewing and updating their accounts, downloading files provided by UC and obtaining scheduled pickup dates from their calendar.
UC is using their Salesforce production org as the identity provider for these users and the expected number of individual users is 2.5 million with 13.5 million unique logins per month.
Which of the following license types should be used to meet the requirement?

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

**Answer:** C

**Explanation:**
Partner Community Login License is the best option for UC’s use case, as it allows external partners to access Experience Cloud sites and Salesforce data with a

pay-per-login model. The other license types are either too expensive or not suitable for partner users. References: Experience Cloud User Licenses, Salesforce Experience Cloud Pricing

**NEW QUESTION 149**
The CIO of universal containers(UC) wants to start taking advantage of the refresh token capability for the UC applications that utilize Oauth 2.0. UC has listed an architect to analyze all of the applications that use Oauth flows to. See where refresh Tokens can be applied. Which two OAuth flows should the architect consider in their evaluation? Choose 2 answers

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

**Answer:** AC

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

**NEW QUESTION 154**
Universal Containers (UC) implemented SSO to a third-party system for their Salesforce users to access the App Launcher. UC enabled “User Provisioning” on the Connected App so that changes to user accounts can be synched between Salesforce and the third-party system. However, UC quickly notices that changes to user roles in Salesforce are not getting synched to the third-party system. What is the most likely reason for this behavior?

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

**Answer:** B

**Explanation:**
User Provisioning for Connected Apps supports role sync, but the required operation(s) must be mapped in User Provisioning Settings. According to the Salesforce documentation1, “To provision roles, map the Role operation to a field in the connected app. The field must contain the role’s unique name.”
Therefore, option B is the correct answer.
References: Salesforce Documentation

**NEW QUESTION 157**
An Enterprise is using a Lightweight Directory Access Protocol (LDAP ) server as the only point for user authentication with a username/password. Salesforce delegated authentication is configured to integrate Salesforce under single sign-on (SSO).
Mow can end users change their password?

A. Users once logged In, can go to the Change Password screen in Salesforce.
B. Users can click on the "Forgot your Password" link on the Salesforce.com login page.
C. Users can request the Salesforce Admin to reset their password.
D. Users can change it on the enterprise LDAP authentication portal.

**Answer:** C

**Explanation:**
Users can request the Salesforce Admin to reset their password if they are using delegated authentication with LDAP. The other options are not applicable for this scenario, as the password is managed by the LDAP server, not by Salesforce. References: Delegated Authentication, FAQs for Delegated Authentication

**NEW QUESTION 162**
Users logging into Salesforce are frequently prompted to verify their identity.
The identity architect is required to provide recommendations so that frequency of prompt verification can be reduced.
What should the identity architect recommend to meet the requirement?

A. Implement 2FA authentication for the Salesforce org.
B. Set trusted IP ranges for the organization.
C. Implement a single sign-on for Salesforce using an external identity provider.
D. Implement multi-factor authentication for the Salesforce org.

**Answer:** B

**Explanation:**
To reduce the frequency of prompt verification for users logging into Salesforce, the identity architect should recommend setting trusted IP ranges for the organization. Trusted IP ranges are IP addresses that are considered safe for logging in without any additional verification. Users who log in from trusted IP ranges do not need to activate their computer or use a verification code. Trusted IP ranges can improve user convenience and security. References: Trusted IP Ranges, Set Trusted IP Ranges for Your Organization

**NEW QUESTION 163**
Northern Trail Outfitters (NTO) has an existing custom business-to-consumer (B2C) website that does NOT support single sign-on standards, such as Security Assertion Markup Language (SAMi) or OAuth. NTO wants to use Salesforce Identity to register and authenticate new customers on the website.
Which two Salesforce features should an identity architect use in order to provide username/password
authentication for the website? Choose 2 answers

A. Identity Connect
B. Delegated Authentication
C. Connected Apps
D. Embedded Login

**Answer:** BD

**Explanation:**
To register and authenticate new customers on the website using Salesforce Identity, the identity architect should use Delegated Authentication and Embedded Login. Delegated Authentication is a feature that allows Salesforce to delegate the authentication process to an external service, such as a custom website, instead of validating the username and password internally. Embedded Login is a feature that allows Salesforce to embed a login widget into any web page, such as a custom website, to enable users to log in with their Salesforce credentials. The other options are not relevant for this scenario. References: Delegated Authentication, Embedded Login

**NEW QUESTION 167**
A financial enterprise is planning to set up a user authentication mechanism to login to the Salesforce system. Due to regulatory requirements, the CIO of the company wants user administration, including passwords and authentication requests, to be managed by an external system that is only accessible via a SOAP webservice.
Which authentication mechanism should an identity architect recommend to meet the requirements?

A. OAuth Web-Server Flow
B. Identity Connect
C. Delegated Authentication
D. Just-in-Time Provisioning

**Answer:** C

**Explanation:**
Delegated Authentication is an authentication mechanism that allows Salesforce to delegate the authentication process to an external system via a SOAP webservice. The external system can manage the user administration, passwords, and authentication requests. The other options are either not suitable or not supported for this use case. References: Delegated Authentication, FAQs for Delegated Authentication

**NEW QUESTION 172**
Northern Trail Outfitters (NTO) leverages Microsoft Active Directory (AD) for management of employee usernames, passwords, permissions, and asset access. NTO also owns a third-party single sign-on (SSO) solution. The third-party party SSO solution is used for all corporate applications, including Salesforce.
NTO has asked an architect to explore Salesforce Identity Connect for automatic provisioning and deprovisioning of users in Salesforce.
What role does identity Connect play in the outlined requirements?

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

**Answer:** D

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

**NEW QUESTION 176**
Universal Containers (UC) has implemented SSO according to the diagram below. uses SAML while Salesforce Org 1 uses OAuth 2.0. Users usually start their day by first attempting to log into Salesforce Org 2 and then later in the day, they will log into either the Financial System or CPQ system depending upon their job position. Which two systems are acting as Identity Providers?

A. Financial System
B. Pingfederate
C. Salesforce Org 2
D. Salesforce Org 1

**Answer:** BD

**Explanation:**
These are the systems that are acting as identity providers (IdPs) in the SSO scenario. An IdP is a trusted provider that enables a customer to use single sign-on (SSO) to access other websites5. In this case, Pingfederate and Salesforce Org 1 are the IdPs that authenticate the users and issue SAML assertions or OAuth tokens to the service providers (SPs). The SPs are the websites that host apps and rely on the IdPs for authentication5. In this case, Salesforce Org 2, Financial System, and CPQ System are the SPs that receive the SAML assertions or OAuth tokens from the IdPs and grant access to the users.
Option A is incorrect because Financial System is not an IdP, but an SP. It does not authenticate the users, but receives SAML assertions from Pingfederate.
Option C is incorrect because Salesforce Org 2 is not an IdP, but an SP. It does not authenticate the users, but receives OAuth tokens from Salesforce Org 1.
References: 5: Identity Providers and Service Providers - Salesforce 6: Salesforce as Service Provider an Identity Provider for SSO

**NEW QUESTION 178**
customer service representatives at Universal containers (UC) are complaining that whenever they click on links to case records and are asked to login with SAML SSO, they are being redirected to the salesforce home tab and not the specific case record. What item should an architect advise the identity team at UC to investigate first?

A. My domain is configured and active within salesforce.
B. The salesforce SSO settings are using http post
C. The identity provider is correctly preserving the Relay state

D. The users have the correct Federation ID within salesforce.

**Answer:** C

**Explanation:**
The identity provider must correctly preserve the Relay state in order to redirect the user to the specific case record after login with SAML SSO. According to the Salesforce documentation3, “The RelayState parameter is used by SAML to indicate where the user should be redirected after they’ve been authenticated by the identity provider.” Therefore, option C is the correct answer. References: Salesforce Documentation

**NEW QUESTION 181**
Which two things should be done to ensure end users can only use single sign-on (SSO) to login in to Salesforce?
Choose 2 answers

A. Enable My Domain and select "Prevent login from https://login.salesforce.com".
B. Request Salesforce Support to enable delegated authentication.
C. Once SSO is enabled, users are only able to login using Salesforce credentials.
D. Assign user "is Single Sign-on Enabled" permission via profile or permission set.

**Answer:** AD

**Explanation:**
To ensure end users can only use single sign-on (SSO) to log in to Salesforce, two things should be done:

- Enable My Domain and select “Prevent login from https://login.salesforce.com”. My Domain is a feature that allows administrators to customize the Salesforce login URL with a unique domain name. By preventing login from the standard login URL, administrators can enforce SSO and restrict users from logging in with their Salesforce credentials.
- Assign user “is Single Sign-on Enabled” permission via profile or permission set. This permission allows users to log in to Salesforce using SSO. Users who do not have this permission will not be able to access Salesforce even if they have valid Salesforce credentials. References: My Domain, User Permissions for Single Sign-On

**NEW QUESTION 182**
Universal containers (UC) employees have salesforce access from restricted ip ranges only, to protect against unauthorized access. UC wants to rollout the salesforce1 mobile app and make it accessible from any location.
Which two options should an architect recommend? Choose 2 answers

A. Relax the ip restriction in the connect app settings for the salesforce1 mobile app
B. Use login flow to bypass ip range restriction for the mobile app.
C. Relax the ip restriction with a second factor in the connect app settings for salesforce1 mobile app
D. Remove existing restrictions on ip ranges for all types of user access.

**Answer:** AC

**Explanation:**
Relaxing the IP restriction in the connected app settings for the Salesforce1 mobile app and relaxing the IP restriction with a second factor in the connected app settings for Salesforce1 mobile app are two options that an architect should recommend. These options allow UC employees to access the Salesforce1 mobile app from any location, while still maintaining some level of security. Relaxing the IP restriction means that users can log in to the connected app from outside the trusted IP ranges defined in their profiles1. Adding a second factor means that users need to provide an additional verification method, such as a verification code or a security key, to access the app2. Using a login flow to bypass IP range restriction for the mobile app is not a recommended option because it can create a complex and inconsistent user experience3. Removing existing restrictions on IP ranges for all types of user access is not a recommended option because it can expose UC’s data and applications to unauthorized access4. References: 1: Restrict Access to Trusted IP Ranges for a Connected App 2: Require Multi-Factor Authentication for Connected Apps 3: [Custom Login Flows] 4: [Restrict Login Access by IP Address]

**NEW QUESTION 186**
Which three are capabilities of SAML-based Federated authentication? Choose 3 answers

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

**Answer:** ACE

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

**NEW QUESTION 191**
Northern Trail Outfitters mar ages functional group permissions in a custom security application supported by a relational database and a REST service layer. Group permissions are mapped as permission sets in Salesforce.
Which action should an identity architect use to ensure functional group permissions are reflected as permission set assignments?

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

**Answer:** B

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

**NEW QUESTION 193**
An administrator created a connected app for a custom wet) application in Salesforce which needs to be visible as a tile in App Launcher The tile for the custom web application is missing in the app launcher for all users in Salesforce. The administrator requested assistance from an identity architect to resolve the issue.
Which two reasons are the source of the issue? Choose 2 answers

A. StartURL for the connected app is not set in Connected App settings.
B. OAuth scope does not include "openid*.
C. Session Policy is set as 'High Assurance Session required' for this connected app.
D. The connected app is not set in the App menu as 'Visible in App Launcher".

**Answer:** AD

**Explanation:**
The StartURL for the connected app is required to specify the landing page for the app. The connected app
must also be set as visible in the App Launcher to appear as a tile for users. References: Connected App Basics, Manage Connected Apps

**NEW QUESTION 196**
A farming enterprise offers smart farming technology to its farmer customers, which includes a variety of sensors for livestock tracking, pest monitoring, climate monitoring etc. They plan to store all the data in Salesforce. They would also like to ensure timely maintenance of the Installed sensors. They have engaged a salesforce Architect to propose an appropriate way to generate sensor Information In Salesforce.
Which OAuth flow should the architect recommend?

A. OAuth 2.0 Asset Token Flow
B. OAuth 2.0 Device Authentication Row
C. OAuth 2.0 JWT Bearer Token Flow
D. OAuth 2.0 SAML Bearer Assertion Flow

**Answer:** A

**Explanation:**
To generate sensor information in Salesforce, the architect should recommend OAuth 2.0 Asset Token Flow. OAuth 2.0 Asset Token Flow is a protocol that allows devices, such as sensors, to obtain an access token from Salesforce by using a certificate instead of an authorization code. The access token can be used to access Salesforce APIs and send data to Salesforce. OAuth 2.0 Asset Token Flow is designed for devices that do not have a user interface or a web browser.
References: OAuth 2.0 Asset Token Flow, Authorize Apps with OAuth

**NEW QUESTION 198**
which three are features of federated Single Sign-on solutions? Choose 3 answers

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

**Answer:** ABD

**Explanation:**
> It federates credentials control to authorized applications. This means that users can access multiple applications across different domains or organizations using one set of credentials, without having to share their passwords with each application1. The applications rely on a trusted identity provider (IdP) to authenticate the users and grant them access.
> It establishes trust between Identity store and service provider. This means that the IdP and the service provider (SP) have a mutual agreement to exchange identity information using standard protocols, such as SAML, OpenID Connect, or OAuth2. The IdP and the SP also share metadata and certificates to ensure secure communication and verification.
> It improves affiliated applications adoption rates. This means that users are more likely to use applications that are connected to their existing identity provider, as they do not have to create or remember multiple passwords3. This also reduces the friction and frustration of logging in to different applications, and enhances the user experience.
The other options are not features of federated single sign-on solutions because:
> It solves all identity and access management problems. This is false, as federated single sign-on solutions only address the authentication aspect of identity and access management, not the authorization, provisioning, governance, or auditing aspects. Federated single sign-on solutions also have some challenges, such as complexity, interoperability, and security risks.
> It enables quick and easy provisioning and deactivating of users. This is not necessarily true, as

federated single sign-on solutions do not automatically create or delete user accounts in the service provider applications. Users still need to be provisioned and deprovisioned manually or through other mechanisms, such as just-in-time provisioning or SCIM.
References: Federated Identity Management vs. Single Sign-On: What's the Difference?, What is single sign-on?, Single Sign-On (SSO) Solution, [Identity Management vs. Access Management: What's the Difference?], [Federated Identity Management Challenges], [Just-in-Time Provisioning for SAML], [SCIM User Provisioning]

**NEW QUESTION 200**
An Identity and Access Management (IAM) Architect is recommending Identity Connect to integrate Microsoft Active Directory (AD) with Salesforce for user provisioning, deprovisioning and single sign-on (SSO).
Which feature of Identity Connect is applicable for this scenario?

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

**Answer:** A

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

**NEW QUESTION 201**
Northern Trail Outfitters (NTO) employees use a custom on-premise helpdesk application to request, approve, notify, and track access granted to various on-premises and cloud applications, including Salesforce. Salesforce is currently used to authenticate users.
How should NTO provision Salesforce users as soon as they are approved in the helpdesk application with the approved profiles and permission sets?

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

**Answer:** A

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

**NEW QUESTION 204**
Universal containers (UC) is building a mobile application that will make calls to the salesforce REST API. Additionally, UC would like to provide the optimal experience for its mobile users. Which two OAuth scopes should UC configure in the connected App? Choose 2 answers

A. Refresh token
B. API
C. full
D. Web

**Answer:** AB

**Explanation:**
The two OAuth scopes that UC should configure in the connected app are:

- Refresh token. This scope allows the mobile app to obtain a refresh token from Salesforce when it obtains an access token. A refresh token can be used to obtain a new access token when the previous one expires or becomes invalid. This scope enables UC to provide an optimal experience for its mobile users by reducing the number of login prompts and authentication failures.
- API. This scope allows the mobile app to make REST API calls to Salesforce using the access token.

The REST API allows the mobile app to access or manipulate data and metadata in Salesforce using HTTP methods. This scope enables UC to build a custom mobile app that can connect to Salesforce and perform various operations on Salesforce resources.

- References: [OAuth Scopes], [Connected Apps], [Refresh Token], [REST API]

**NEW QUESTION 208**
Which three different attributes can be used to identify the user in a SAML 65> assertion when Salesforce is acting as a Service Provider? Choose 3 answers

A. Federation ID
B. Salesforce User ID
C. User Full Name
D. User Email Address
E. Salesforce Username

**Answer:** ADE

**Explanation:**
The three different attributes that can be used to identify the user in a SAML assertion when Salesforce is acting as a Service Provider are Federation ID, User Email Address, and Salesforce Username. According to the Salesforce documentation, "Salesforce supports three attributes for identifying users in a SAML assertion: Federation ID, User Email Address, and Salesforce Username." Therefore, option A, D, and E are the correct answers.

References: [SAML Assertion Attributes]

**NEW QUESTION 210**

Universal containers (UC) has implemented ansp-Initiated SAML flow between an external IDP and salesforce. A user at UC is attempting to login to salesforce1 for the first time and is being prompted for salesforce credentials instead of being shown the IDP login page. What is the likely cause of the issue?

A. The "Redirect to Identity Provider" option has been selected in the my domain configuration.
B. The user has not configured the salesforce1 mobile app to use my domain for login
C. The "Redirect to identity provider" option has not been selected the SAML configuration.
D. The user has not been granted the "Enable single Sign-on" permission

**Answer:** B

**Explanation:**

B is correct because the user has not configured the Salesforce1 mobile app to use My Domain for login, which is the likely cause of the issue. The My Domain URL is used to redirect the user to the identity provider’s login page and initiate the SP-Initiated SAML flow. If the user does not configure the Salesforce1 mobile app to use My Domain for login, they will be prompted for Salesforce credentials instead of being shown the IDP login page. A is incorrect because the “Redirect to Identity Provider” option has been selected in the My Domain configuration, which is not the cause of the issue. The “Redirect to Identity Provider” option determines whether users are redirected to the identity provider’s login page automatically or after clicking a button. C is incorrect because the “Redirect to Identity Provider” option has not been selected in the SAML configuration, which is not the cause of the issue. The “Redirect to Identity Provider” option determines whether users are redirected to the identity provider’s login page automatically or after clicking a button. D is incorrect because the user has been granted the “Enable Single Sign-On” permission, which is not the cause of the issue. The “Enable Single Sign-On” permission allows users to use SSO with connected apps or external systems. Verified References: [My Domain URL], [SP-Initiated SAML Flow], [Redirect to Identity Provider Option], [Enable Single Sign-On Permission]

**NEW QUESTION 215**

......

# Thank You for Trying Our Product

## We offer two products:

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

2nd - Questons and Answers in PDF Format

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

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

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

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

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

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