

# Salesforce

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

Salesforce Certified Identity and Access Management Architect (SU23)



**NEW QUESTION 1**

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

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

**Answer:** BD

**Explanation:**

To use SAML SSO for accessing the Salesforce1 mobile app, the architect should recommend configuring the embedded web browser to use the My Domain URL and configuring the Salesforce1 app to use the My Domain URL<sup>4</sup>. Using the My Domain URL allows Salesforce to identify the identity provider and initiate the SSO process<sup>5</sup>. Using the existing SAML SSO flow along with user agent flow or web server flow is not necessary because Salesforce Mobile Applications only work with service provider initiated setups<sup>4,6</sup>. Therefore, option B and D are the correct answers.

References: Salesforce Mobile Application Single Sign-On overview, SAML SSO with Salesforce as the Service Provider, Single Sign-On

**NEW QUESTION 2**

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

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

**Answer:** D

**Explanation:**

D is correct because using a self-signed certificate leads to higher maintenance for the trusting party, which is the client or browser that connects to the server. The trusting party needs to add the self-signed certificate to their truststore, which is a repository of trusted certificates, in order to establish a secure connection with the server. Otherwise, the trusting party will see a warning message or an error when accessing the server.

A is incorrect because using a self-signed certificate leads to higher maintenance for the trusted party, not lower. The trusted party needs to maintain multiple self-signed certificates from different servers in their truststore.

B is incorrect because using a self-signed certificate does not make the trusted party act as the trusted CA (Certificate Authority). The trusted CA is the entity that issues and validates certificates for servers. The trusted party only needs to trust the CA's root certificate, which is usually pre-installed in their truststore.

C is incorrect because using a self-signed certificate leads to higher maintenance for the trusting party, not lower. The trusting party still needs to maintain a trusted CA cert in their truststore, which is the self-signed certificate itself.

References: 1: SSL Certificate Installation Instructions & Tutorials - DigiCert 2: How To Install an SSL Certificate from a Commercial ... - DigitalOcean 3: Setup SSL CSR Creation and SSL Certificate Installatio  
- DigiCert

**NEW QUESTION 3**

Which three are features of federated Single sign-on solutions? Choose 3 Answers

- A. It establishes trust between Identity Store and Service Provider.
- B. It federates credentials control to authorized applications.
- 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:** ADE

**Explanation:**

The three features of federated single sign-on (SSO) solutions are:

➤ It establishes trust between identity store and service provider. Federated SSO is a process that allows users to access multiple applications or systems with one set of credentials by using a common identity provider (IdP) that authenticates the user and issues a security token to the service provider (SP) that grants access. This process requires a trust relationship between the IdP and the SP, which is established by exchanging metadata and certificates.

➤ It improves affiliated applications adoption rates. Federated SSO improves the user experience and satisfaction by reducing the number of login prompts, passwords, and authentication failures that users have to deal with when accessing multiple applications or systems. This can increase the usage and adoption rates of the affiliated applications or systems, as users can access them more easily and conveniently.

➤ It enables quick and easy provisioning and deprovisioning of users. Federated SSO enables centralized management of user accounts and access rights by using the IdP as the source of truth for user identity and attributes. This can simplify and automate the provisioning and deprovisioning of users across multiple applications or systems, as changes made in the IdP can be reflected in the SPs without requiring manual intervention or synchronization.

The other option is not a feature of federated SSO solutions. Federated SSO does not solve all identity and access management problems, as it still faces challenges such as security risks, compatibility issues, governance policies, and user education. References: [Federated Single Sign-On], [Set Up Federated Authentication Using SAML], [Benefits of Single Sign-On], [How Single Sign-On Improves Application Adoption Rates], [User Provisioning for Federated Single Sign-On], [Just-in-Time Provisioning for SAML], [Challenges of Single Sign-On]

**NEW QUESTION 4**

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

- A. Access Tokens
- B. Mobile pins
- C. Refresh Tokens

D. Scopes

**Answer:** D

**Explanation:**

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

References: [OAuth Scopes], [Connected Apps], [OAuth Authorization Flows]

**NEW QUESTION 5**

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

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

**Answer:** CD

**Explanation:**

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

- OAuth SAML Bearer Assertion Flow, which allows the client app to use a SAML assertion issued by a trusted identity provider to request an access token from Salesforce. This flow does not require the client app to store any credentials or secrets, and leverages the existing SSO infrastructure between Salesforce and the identity provider.
- OAuth JWT Bearer Token Flow, which allows the client app to use a JSON Web Token (JWT) signed by a private key to request an access token from Salesforce. This flow does not require any user interaction or consent, and uses a certificate to verify the identity of the client app.

Verified References: [OAuth 2.0 SAML Bearer Assertion Flow for Server-to-Server Integration], [OAuth 2.0 JWT Bearer Token Flow for Server-to-Server Integration]

**NEW QUESTION 6**

A large consumer company is planning to create a community and will require login through the customers social identity. The following requirements must be met:

- \* 1. The customer should be able to login with any of their social identities, however salesforce should only have one user per customer.
- \* 2. Once the customer has been identified with a social identity, they should not be required to authorize Salesforce.
- \* 3. The customers personal details from the social sign on need to be captured when the customer logs into Salesforce using their social Identity.
- \* 3. If the customer modifies their personal details in the social site, the changes should be updated in Salesforce.

Which two options allow the Identity Architect to fulfill the requirements? Choose 2 answers

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

**Answer:** BD

**Explanation:**

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

References: Authentication Providers, Social Sign-On with Authentication Providers, Create a Custom Registration Handler

**NEW QUESTION 7**

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 Salesforce 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 8**

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 9**

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

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

**Answer:** BC

**Explanation:**

In an environment where Salesforce users are enabled to access Google Apps from within Salesforce through App Launcher and Connected App setup, Google is the service provider and Salesforce is the identity provider. A service provider is an application that provides a service to users and relies on an identity provider for authentication<sup>3</sup>. A connected app is a service provider that integrates an application with Salesforce using APIs<sup>4</sup>. An identity provider is an application that authenticates users and provides information about them to service providers<sup>3</sup>. The App Launcher is a feature that allows users to access Salesforce, connected, and on-premises apps from one location<sup>5</sup>. In this scenario, Google Apps are connected apps that provide services to Salesforce users, such as Gmail, Google Drive, and Google Calendar. Salesforce is the identity provider that authenticates users and allows them to access Google Apps with their Salesforce credentials using single sign-on (SSO)<sup>6</sup>.

References: Identity Provider Overview, Connected Apps Overview, App Launcher, Single Sign-On for Desktop and Mobile Applications using SAML and OAuth

**NEW QUESTION 10**

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

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

**Answer:** BE

**Explanation:**

Delegated authentication is a feature that allows Salesforce to delegate the authentication process to an external service of your choice<sup>1</sup>. When implementing delegated authentication, you should consider the following aspects<sup>2</sup>:

- The authentication web service can include custom attributes, such as user roles or permissions, in the response to Salesforce. These attributes can be used to update user records or trigger workflows in Salesforce<sup>2</sup>.
- Delegated authentication can be used to authenticate API clients and mobile apps that use the SOAP API or REST API login() methods. However, it does not support OAuth 2.0 flows or other authentication methods<sup>2</sup>.
- Delegated authentication does not require trusted IP ranges at the User Profile level. However, you can use them to restrict access to Salesforce from specific IP addresses or ranges<sup>2</sup>.
- Salesforce servers receive but do not validate a user's credentials. Instead, they pass the credentials to the external authentication service, which validates them and returns a response to Salesforce<sup>2</sup>.
- Just-in-time provisioning can be configured for new users who log in with delegated authentication. This feature allows Salesforce to create or update user accounts based on the information provided by the external authentication service<sup>3</sup>.

References:

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

**NEW QUESTION 10**

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

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



**Answer:** B

**Explanation:**

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

References: [Identity Provider Overview], [SAML Single Sign-On Overview], [Single Sign-On Overview], [Salesforce as an Identity Provider]

**NEW QUESTION 12**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 15**

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

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

**Answer:** BC

**Explanation:**

these are the optimal actions to troubleshoot a SAML error. According to the Salesforce documentation<sup>1</sup>, you can use the following methods to debug a SAML error:

- Use a browser that has an add-on/extension that can inspect SAML. This will allow you to see the SAML request and response messages and identify any issues with the SAML assertion or the SAML response<sup>2</sup>.
- Paste the SAML Assertion Validator in Salesforce. This is a tool that helps you validate the last SAML operation on your organization and shows you any errors or warnings with the SAML assertion or the SAML response<sup>1</sup>.

Option A is incorrect because the Callback URL is not related to SAML SSO. The Callback URL is used for OAuth SSO, which is a different protocol<sup>3</sup>. Option D is incorrect because using the browser's Development tools to view the Salesforce page's markup will not help you debug a SAML error. The page's markup does not contain any information about the SAML request or response<sup>4</sup>.

References: 1: SAML Login Errors - Salesforce 2: How to Troubleshoot a Single Sign-On Error | Salesforce Ben 3: Identity Providers and Service Providers - Salesforce 4: Single Sign-On - Salesforce

**NEW QUESTION 18**

Universal Containers (UC) is building a customer community and will allow customers to authenticate using Facebook credentials. The first time the user authenticates 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 19**

A web service is developed that allows secure access to customer order status on the Salesforce Platform. The service connects to Salesforce through a connected app with the web server flow. The following are the required actions for the authorization flow:

- \* 1. User Authenticates and Authorizes Access
  - \* 2. Request an Access Token
  - \* 3. Salesforce Grants an Access Token
  - \* 4. Request an Authorization Code
  - \* 5. Salesforce Grants Authorization Code
- What is the correct sequence for the authorization flow?

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

**Answer:** B

**Explanation:**

The web server flow is an OAuth 2.0 authorization code grant type, which follows this sequence of steps:

- The client app requests an authorization code from Salesforce by redirecting the user to the authorization endpoint.
- The user authenticates and authorizes access to the client app.
- Salesforce grants an authorization code and redirects the user back to the client app.
- The client app requests an access token from Salesforce by sending the authorization code to the token endpoint.
- Salesforce grants an access token and a refresh token to the client app. References: OAuth Authorization Flows, Authorize Apps with OAuth

**NEW QUESTION 24**

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 Provider<sup>1</sup>. Option A is incorrect because Visualforce is not a supported method for redirecting users to the Identity Provider login page<sup>2</sup>. 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 flow<sup>3</sup>. 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 authentication<sup>4</sup>.

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 28**

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 30**

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

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

**Answer:** A

**Explanation:**

The Entity ID is the SAML SSO setting in Salesforce that provides the capability to differentiate Salesforce from other service providers. The Entity ID is a unique identifier for the service provider that is sent in the SAML request and response messages<sup>1</sup>. The identity provider uses the Entity ID to determine which service provider is requesting or receiving authentication information<sup>2</sup>. You can customize the Entity ID for your Salesforce org or Experience Cloud site in the SAML

Single Sign-On Settings page3. References: 1: SAML SSO Flows 2: Federated Authentication Using SAML to Log in to Salesforce Org 3: Step 2: Create a SA Single Sign-On Setting in Salesforce

**NEW QUESTION 35**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 36**

Northern Trail Outfitters (NTO) wants to improve its engagement with existing customers to boost customer loyalty. To get a better understanding of its customers, NTO establishes a single customer view including their buying behaviors, channel preferences and purchasing history. All of this information exists but is spread across different systems and formats.

NTO has decided to use Salesforce as the platform to build a 360 degree view. The company already uses Microsoft Active Directory (AD) to manage its users and company assets.

What should an Identity Architect do to provision, deprovision and authenticate users?

- A. Salesforce Identity is not needed since NTO uses Microsoft AD.
- B. Salesforce Identity can be included but NTO will be required to build a custom integration with Microsoft AD.
- C. Salesforce Identity is included in the Salesforce licenses so it does not need to be considered separately.
- D. A Salesforce Identity can be included but NTO will require Identity Connect.

**Answer:** D

**Explanation:**

Identity Connect is a Salesforce product that integrates Microsoft Active Directory with Salesforce user records. It allows provisioning, deprovisioning, and authentication of users based on AD data. The other options are either incorrect or irrelevant for this use case. References: Get to Know Identity Connect, Identity Connect

**NEW QUESTION 40**

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 45**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 49**

What are three capabilities of Delegated Authentication? Choose 3 answers

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

**Answer:** BCE

**Explanation:**

The three capabilities of delegated authentication are:

- It can connect to SOAP services. Delegated authentication is a feature that allows Salesforce to delegate the authentication process to an external service by making a SOAP callout to a web service that verifies the user's credentials. This feature enables Salesforce to integrate with existing identity stores or authentication methods that support SOAP services.
  - It can be assigned by permission sets. Permission sets are collections of settings and permissions that give users access to various tools and functions in Salesforce. Permission sets can be used to assign delegated authentication to users by enabling the "Is Single Sign-on Enabled" permission. This permission allows users to log in with delegated authentication instead of their Salesforce username and password.
  - It can connect to REST services. REST services are web services that use HTTP methods to access or manipulate resources on a server. REST services can be used for delegated authentication by creating a custom login page that makes a REST callout to an external service that verifies the user's credentials. This approach requires custom code and configuration, but it provides more flexibility and control over the authentication process.
- The other options are not capabilities of delegated authentication. Delegated authentication cannot be assigned by custom permissions or profiles. Custom permissions are settings that can be used in Apex code or validation rules to check whether a user has access to a custom feature or functionality. Custom permissions cannot be used to enable delegated authentication for users. Profiles are collections of settings and permissions that determine what users can do in Salesforce. Profiles cannot be used to enable delegated authentication for users, as this feature is controlled by permission sets. References: [Delegated Authentication], [Permission Sets], [Enable 'Delegated Authentication'], [REST Services], [Custom Login Page for Delegated Authentication], [Custom Permissions], [Profiles]

**NEW QUESTION 53**

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.com>. 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 55**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 60**

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

- A. Users leaving laptops unattended and not logging out of Salesforce.
- B. Users accessing Salesforce from a public Wi-Fi access point.



- C. Users choosing passwords that are the same as their Facebook password.
- D. Users creating simple-to-guess password reset questions.

**Answer:** BC

**Explanation:**

Enabling Two-Factor Authentication (2FA) in Salesforce can mitigate the security risks of users accessing Salesforce from a public Wi-Fi access point or choosing passwords that are the same as their Facebook password. 2FA is an additional layer of protection beyond your password that requires users to verify their identity with another factor, such as a mobile app, a security key, or a verification code. This can prevent unauthorized access even if the user's password is compromised or guessed by a malicious actor. The other options are not directly related to 2FA, but rather to user behavior or password policies.

**NEW QUESTION 65**

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

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

**Answer:** A

**Explanation:**

According to the Salesforce documentation<sup>2</sup>, OAuth2 RPs (relying parties) are applications that use OAuth 2.0 for authentication and authorization with an external identity provider. This allows users to log in to multiple applications with a single identity provider account. The identity provider issues an access token to the relying party, which can be used to access protected resources on behalf of the user. This solution can support high volumes of logins per minute and unify multiple B2C Commerce sites and an Experience Cloud community with a single identity.

**NEW QUESTION 67**

A multinational industrial products manufacturer is planning to implement Salesforce CRM to manage their business. They have the following requirements:

- \* 1. They plan to implement Partner communities to provide access to their partner network .
- \* 2. They have operations in multiple countries and are planning to implement multiple Salesforce orgs.
- \* 3. Some of their partners do business in multiple countries and will need information from multiple Salesforce communities.
- \* 4. They would like to provide a single login for their partners.

How should an Identity Architect solution this requirement with limited custom development?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 68**

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 71**

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

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

**Answer:** B

**Explanation:**

If the third-party authentication provider supports only the OAuth protocol and not OpenID Connect, then an identity architect needs to create a custom external

authentication provider for it. A custom external authentication provider is a configuration that allows users to log in to Salesforce using an external identity provider that is not predefined by Salesforce. It requires implementing the Auth.AuthProviderPlugin interface and defining the OAuth endpoints and parameters.  
References: Custom External Authentication Providers, Create a Custom Authentication Provider

**NEW QUESTION 74**

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 logins that 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 77**

Universal Containers (UC) is rolling out its new Customer Identity and Access Management Solution built on top of its existing Salesforce instance. UC wants to allow customers to login using Facebook, Google, and other social sign-on providers.

How should this functionality be enabled for UC, assuming all social sign-on providers support OpenID Connect?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 79**

The executive sponsor for an organization has asked if Salesforce supports the ability to embed a login widget into its service providers in order to create a more seamless user experience.

What should be used and considered before recommending it as a solution on the Salesforce Platform?

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 84**

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

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

**Answer:** C

**Explanation:**

The SAML SSO flow that an architect should recommend for UC is IdP-initiated. IdP-initiated SSO is a process that allows users to start at the IdP site, such as UC's custom web page, and then be redirected to Salesforce or other SPs with a SAML assertion that contains information about the user's identity and attributes. This flow enables UC to provide a single point of entry for its users to access multiple applications with the same credentials, as they do not need to enter their username and password again for each application. This flow also simplifies the configuration and maintenance of SSO, as UC does not need to create or manage deep links or URLs for each application.

The other options are not valid SAML SSO flows for this scenario. SP-initiated with deep linking is a process that allows users to start at a specific resource on the SP site, such as a report or dashboard, and then be redirected to the IdP for authentication and back to the resource with a SAML assertion. This flow is not suitable for UC's scenario, as they want their users to start at their custom web page, not at a specific resource on Salesforce or other SPs. SP-initiated is a process that allows users to start at the SP site, such as Salesforce or other applications, and then be redirected to the IdP for authentication and back to the SP site with a SAML assertion. This flow is not suitable for UC's scenario, as they want their users to start at their custom web page, not at each application separately. User-agent is not a standard term for SAML SSO, but it could refer to user-agent flow, which is an OAuth authorization flow that allows users to obtain an access token from Salesforce by using a browser or web-view. This flow is not suitable for UC's scenario, as it does not use SAML or IdP for authentication.

References: [SAML Single Sign-On], [IdP-Initiated Login], [SP-Initiated Login], [Deep Linking], [OAuth User-Agent Flow]

**NEW QUESTION 88**

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

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

**Answer:** A

**Explanation:**

The web service that is used for delegated authentication should be secured with TLS using Salesforce trusted certificates<sup>4</sup>. This ensures that the communication between Salesforce and the external authentication method is encrypted and authenticated. The other options are not relevant for designing a delegated authentication implementation. The web service does not need to accept one to four input method parameters, as it can accept any number of parameters as long as they are wrapped in a SOAP envelope<sup>5</sup>. The web service does not need to use the Salesforce Federation ID to identify the user, as it can use any identifier that is unique and consistent across systems<sup>6</sup>. The web service does not need to implement a custom password decryption method, as it can use any encryption or hashing algorithm that is supported by both systems<sup>7</sup>. References: Delegated Authentication, Enable 'Delegated Authentication', Delegated Authentication Flow in Salesforce, FAQs fo Delegated Authentication

**NEW QUESTION 89**

A group of users try to access one of universal containers connected apps and receive the following error message: "Failed : Not approved for access". what is most likely to cause of the issue?

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

**Answer:** B

**Explanation:**

The users do not have the correct permission set assigned to them is the most likely cause of the issue. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect<sup>1</sup>. Connected apps use these protocols to authorize, authenticate, and provide single sign-on (SSO) for external apps<sup>1</sup>. To access a connected app, users must have the appropriate permissions assigned to them, either through their profile or a permission set<sup>2</sup>. If the users do not have the required permissions, they will receive an error message when they try to access the connected app. The use of high assurance sessions are required for the connected app is not a valid option, as high assurance sessions are related to multi-factor authentication (MFA), not connected apps<sup>3</sup>. The connected app setting "All users may self-authorize" is enabled is not a cause of the issue, but a possible solution. This setting allows users to access the connected app without pre-approval from an administrator<sup>4</sup>. The Salesforce administrators have revoked the OAuth authorization is not a likely cause of the issue, as OAuth authorization is granted by the users, not the administrators<sup>5</sup>. Revoking OAuth authorization would also affect all users, not just a group of them.

References: Learn About Connected Apps, Create a Connected App, [Multi-Factor Authentication (MFA) fo Salesforce], [Connected App Basics], OAuth Authorization Flows

**NEW QUESTION 93**

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 98**

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

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

**Answer:** AD

**Explanation:**

A is correct because requiring users to provide their RSA token along with their credentials is a form of two-factor authentication. An RSA token is a hardware device that generates a one-time password (OTP) that changes every few seconds. The user needs to enter both their password and the OTP to log in to Salesforce.

D is correct because requiring users to use a biometric reader as well as their password is another form of two-factor authentication. A biometric reader is a device that scans a user's fingerprint, face, iris, or other physical characteristics to verify their identity. The user needs to provide both their password and their biometric data to log in to Salesforce.

B is incorrect because requiring users to supply their email and phone number, which gets validated, is not a form of two-factor authentication. This is a form of identity verification, which is used to confirm that the user owns the email and phone number they provided. However, this does not add an extra layer of protection beyond their password when they log in to Salesforce.

C is incorrect because requiring users to enter a second password after the first authentication is not a form of two-factor authentication. This is a form of single-factor authentication, which only relies on something the user knows (their passwords). This does not increase security against unauthorized account access.

References: 4: Multi-Factor Authentication - Salesforce 5: Salesforce Multi-Factor Authentication 6: Factor Authentication - Salesforce India 7: Customer 360 | Increase Productivity - Salesforce UK 8: Secu Salesforce Login Using Two-Factor Authentication and Salesforce ...

**NEW QUESTION 102**

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

- A. The OAuth authorizations are being revoked by a nightly batch job.
- B. The refresh token expiration policy is set incorrectly in salesforce
- C. The app is requesting too many access Tokens in a 24-hour period
- D. The users forget to check the box to remember their credentials.

**Answer:** B

**Explanation:**

The most likely cause of the issue is that the refresh token expiration policy is set incorrectly in Salesforce. A refresh token is a credential that allows a connected app to obtain a new access token when the previous one expires<sup>1</sup>. The refresh token expiration policy determines how long a refresh token is valid for<sup>2</sup>. If the policy is set to a short duration, such as 24 hours, the users have to enter their credentials once a day to get a new refresh token. To prevent this, the policy should be set to a longer duration, such as "Refresh token is valid until revoked" or "Refresh token expires after 90 days of inactivity"<sup>2</sup>.

References: OAuth 2.0 Refresh Token Flow, Manage OAuth Access Policies for a Connected App

**NEW QUESTION 107**

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 110**

Universal Containers (UC) is using its production org as the identity provider for a new Experience Cloud site and the identity architect is deciding which login experience to use for the site. Which two page types are valid login page types for the site?

Choose 2 answers

- A. Experience Builder Page
- B. lightning Experience Page
- C. Login Discovery Page
- D. Embedded Login Page

**Answer:** CD



**Explanation:**

Login Discovery Page and Embedded Login Page are two valid login page types for Experience Cloud sites. Login Discovery Page allows users to choose their preferred login method, such as username/password, SSO, or social sign-on. Embedded Login Page allows users to log in from any site page without being redirected to a separate login page. References: Login Discovery Page, Embedded Login

**NEW QUESTION 111**

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.

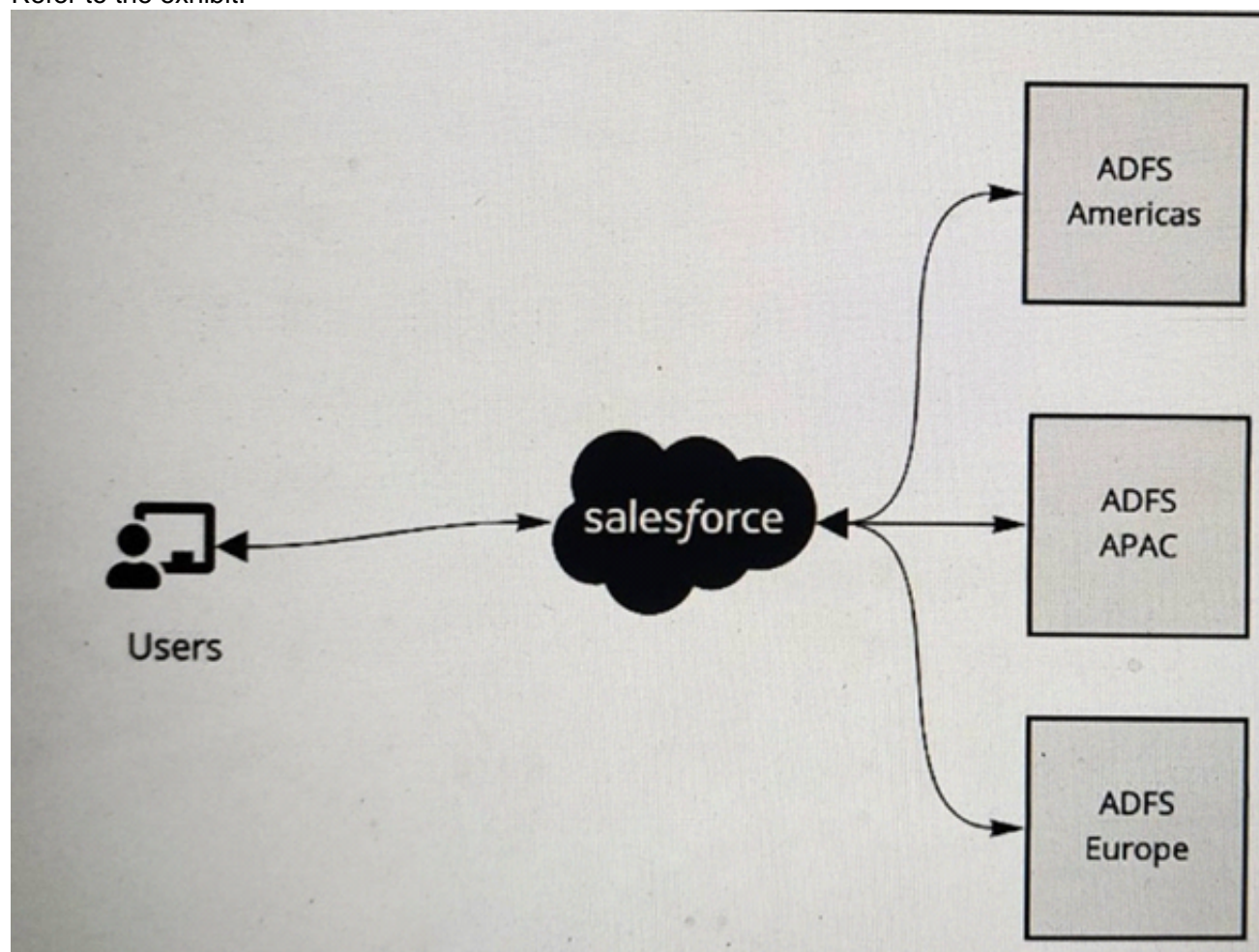
**Answer: A**

**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 URL. Therefore, option A is the correct answer. References: SAML SSO with Salesforce as the Service Provider

**NEW QUESTION 112**

Refer to the exhibit.



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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 115**

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 117**

Universal Containers (UC) has a Desktop application to collect leads for marketing campaigns. UC wants to extend this application to integrate with Salesforce to create leads. Integration between the desktop application and salesforce should be seamless. What Authorization flow should the Architect recommend?

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

**Answer:** A

**Explanation:**

The JWT Bearer Token flow is an OAuth flow in which an external app (also called client or consumer app) sends a signed JSON string to Salesforce called JWT to obtain an access token. The access token can then be used by the external app to read and write data in Salesforce<sup>1</sup>. This flow is suitable for UC's scenario because it allows seamless integration between the desktop application and Salesforce without requiring user interaction or login credentials<sup>2</sup>. The other options are not valid authorization flows for this scenario. The Web Server Authentication Flow and the User Agent Flow both require user interaction and redirection to the Salesforce OAuth authorization endpoint, which is not seamless<sup>3</sup>. The Username and Password Flow requires the external app to store the user's login credentials, which is not secure or recommended<sup>3</sup>.

References: OAuth 2.0 JWT Bearer Flow for Server-to-Server Integration, OAuth Authorization Flows, Salesforce OAuth : JWT Bearer Flow

**NEW QUESTION 119**

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

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

**Answer:** D

**Explanation:**

This is because without My Domain, Salesforce will not know in advance what Identity Provider (IdP) to use for SSO, since it does not even know yet what Organization the user is trying to log in to<sup>1</sup>. SP-initiated SSO is the scenario where the user starts with a Salesforce link (login page, deep link, Outlook Sync URL, etc.) and then gets redirected to the IdP for authentication<sup>2</sup>. Without My Domain, SP-initiated SSO requires that the user do an IdP-initiated SSO at least once first so that Salesforce can set a cookie in their browser identifying the IdP<sup>1</sup>. The other options are not correct for this question because:

- IdP-initiated SSO will work without My Domain, as long as the user starts SSO at the IdP and sends the identity information to Salesforce along with SAML protocol information that identifies the Organization and the IdP<sup>2</sup>.
- Neither SP- nor IdP-initiated SSO will not work is false, as explained above.
- Either SP- or IdP-initiated SSO will work is false, as explained above.

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

**NEW QUESTION 121**

Northern Trail Outfitters (NTO) uses Salesforce Experience Cloud sites (previously known as Customer Community) to provide a digital portal where customers can login using their Google account.

NTO would like to automatically create a case record for first time users logging into Salesforce Experience Cloud.

What should an Identity architect do to fulfill the requirement?

- A. Configure an authentication provider for Social Login using Google and a custom registration handler.
- B. Implement a Just-in-Time handler class that has logic to create cases upon first login.
- C. Create an authentication provider for Social Login using Google and leverage standard registration handler.
- D. Implement a login flow with a record create component for Case.

**Answer:** D

**Explanation:**

To automatically create a case record for first time users logging into Salesforce Experience Cloud using their Google account, the identity architect should implement a login flow with a record create component for Case. A login flow is a custom post-authentication process that can be used to add additional screens or logic after a user logs in to Salesforce. A record create component is a type of flow element that can be used to create a new record in Salesforce. By implementing a login flow with a record create component for Case, the identity architect can check if the user is logging in for the first time using their Google account and create a case record accordingly. References: Login Flows, Record Create Element

**NEW QUESTION 123**

Universal Containers (UC) is implementing Salesforce and would like to establish SAML SSO for its users to log in. UC stores its corporate user identities in a Custom Database. The UC IT Manager has heard good things about Salesforce Identity Connect as an Idp, and would like to understand what limitations they may face if they decided to use Identity Connect in their current environment. What limitation Should an Architect inform the IT Manager about?

- A. Identity Connect will not support user provisioning in UC's current environment.
- B. Identity Connect will only support Idp-initiated SAML flows in UC's current environment.
- C. Identity Connect will only support SP-initiated SAML flows in UC's current environment.
- D. Identity connect is not compatible with UC's current identity environment.

**Answer:** A

**Explanation:**

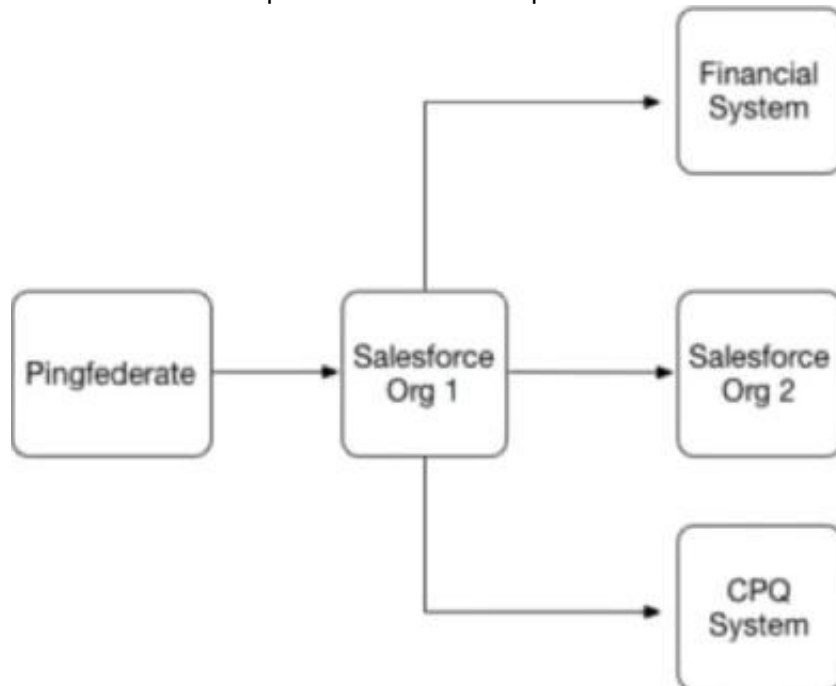
Identity Connect will not support user provisioning in UC's current environment. Identity Connect is a tool that synchronizes user data between Active Directory and Salesforce, but it does not work with other identity sources such as a Custom Database<sup>5</sup>. Therefore, if UC wants to use Identity Connect as an Idp, they will not be able to provision users from their Custom Database to Salesforce.

Options B, C, and D are incorrect because Identity Connect does not have any limitations on the type of SAML flow or the compatibility with UC's current identity environment. Identity Connect supports both Idp-initiated and SP-initiated SAML flows<sup>6</sup>, and it can act as an Idp for any external service provider that supports SAML 2.07.

References: 5: Identity Connect - Salesforce 6: SAML SSO Flows - Salesforce 7: Salesforce Connect: Integration, Benefits, and Limitations

**NEW QUESTION 125**

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 resource<sup>1</sup>. 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 System<sup>2</sup>. Therefore, the correct answer is B.

References:

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

**NEW QUESTION 130**

Universal Containers (UC) is considering a Customer 360 initiative to gain a single source of the truth for its customer data across disparate systems and services. UC wants to understand the primary benefits of Customer 360 Identity and how it contributes to a successful Customer 360 Truth project.

What are two key benefits of Customer 360 Identity as it relates to Customer 360? Choose 2 answers

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

**Answer:** BC

**Explanation:**

Customer 360 Identity is a cloud-based identity service that provides a single, trusted identity for customers across all your digital properties and applications<sup>2</sup>. Customer 360 Identity has several benefits that relate to Customer 360, such as<sup>3</sup>:

- > Customer 360 Identity enables an organization to build a single login for each of its customers, giving the organization an understanding of the user's login activity across all its digital properties and applications. This helps to create a unified customer profile and deliver personalized experiences based on user preferences and behaviors<sup>3</sup>.
- >



Customer 360 Identity supports multiple brands so you can deliver centralized identity services and correlation of user activity, even if it spans multiple corporate brands and user experiences. This helps to maintain brand consistency and loyalty while providing seamless access to your products and services3. References:

- > Customer 360 Identity
- > Customer 360 Identity Benefits

**NEW QUESTION 133**

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

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

**Answer:** CD

**Explanation:**

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

References: [Single Sign-On Implementation Guide], [Customizing User Authentication with Login Flows]

**NEW QUESTION 135**

Northern Trail Outfitters (NTO) wants to give customers the ability to submit and manage issues with their purchases. It is important for NTO to give its customers the ability to login with their Amazon credentials.

What should an identity architect recommend to meet these requirements?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 137**

A global company is using the Salesforce Platform as an Identity Provider and needs to integrate a third-party application with its Experience Cloud customer portal.

Which two features should be utilized to provide users with login and identity services for the third-party application?

Choose 2 answers

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

**Answer:** AC

**Explanation:**

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

**NEW QUESTION 141**

A client is planning to rollout multi-factor authentication (MFA) to its internal employees and wants to understand which authentication and verification methods meet the Salesforce criteria for secure authentication.

Which three functions meet the Salesforce criteria for secure mfa? Choose 3 answers

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

**Answer:** BCE

**Explanation:**



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

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

References:

- Multi-Factor Authentication
- Authentication and Verification Methods

#### NEW QUESTION 144

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

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

**Answer: D**

#### Explanation:

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

- SAML Just-In-Time Provisioning is used to create or update users in Salesforce based on SAML assertions from an identity provider3. Facebook does not support SAML as an identity provider.
- The Signed Request is a parameter that contains information about the user who is logging in to Salesforce via Facebook. It does not contain the user's profile information, such as name, email, or photo.
- A scheduled job that calls out to Facebook on a nightly basis would not reflect the changes in the Facebook profile in real time, as the requirement states. It would also require storing the user's Facebook access token and making API calls to Facebook, which could be inefficient and insecure. References: Set Up Social Sign-On, Configure a Facebook Authentication Provider, SAML Just-in-Time Provisioning, [Facebook as a SAML Identity Provider], [Facebook Login for Apps - Signed Request], [Facebook Login for Apps - Access Tokens], [Facebook Graph API - User]

#### NEW QUESTION 146

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

What should be done to fulfill the requirement? Choose 2 answers

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

**Answer: AD**

#### Explanation:

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

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

References:

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

#### NEW QUESTION 150

Northern Trail Outfitters recently acquired a company. Each company will retain its Identity Provider (IdP). Both companies rely extensively on Salesforce processes that send emails to users to take specific actions in Salesforce.

How should the combined companys' employees collaborate in a single Salesforce org, yet authenticate to the appropriate IdP?

- A. Configure unique MyDomains for each company and have generated links use the appropriate MyDomam in the URL.

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 154**

A division of a Northern Trail Outfitters (NTO) purchased Salesforce. NTO uses a third party identity provider (IdP) to validate user credentials against its corporate Lightweight Directory Access Protocol (LDAP) directory. NTO wants to help employees remember as passwords as possible. What should an identity architect recommend?

- A. Setup Salesforce as a Service Provider to the existing IdP.
- B. Setup Salesforce as an IdP to authenticate against the LDAP directory.
- C. Use Salesforce connect to synchronize LDAP passwords to Salesforce.
- D. Setup Salesforce as an Authentication Provider to the existing IdP.

**Answer:** A

**Explanation:**

To help employees remember fewer passwords, an identity architect should recommend setting up Salesforce as a service provider (SP) to the existing IdP. A SP is the system that relies on the IdP for authentication and provides access to its services based on the SAML assertions from the IdP. To set up Salesforce as a SP, you need to create a connected app for Salesforce in the IdP, enable SAML and configure the SAML settings, such as the entity ID, ACS URL, and subject type. You also need to enable SSO for your Salesforce org, upload the IdP certificate, and configure the SSO settings, such as the issuer, identity type, and service provider initiated request binding.

References:

- [SAML Single Sign-On]
- [Set Up Salesforce as a Service Provider]
- [Enable Single Sign-On for Your Org]

**NEW QUESTION 158**

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

- A. Implement JIT provisioning on the SAML IDP that will pass the profile ID in each assertion.
- B. Create an Apex scheduled job in one org that will synchronize the other orgs profile.
- C. Implement Delegated Authentication that will update the user profiles as necessary.
- D. Implement an OAuth2 flow to pass the profile credentials between systems.

**Answer:** A

**Explanation:**

To allow Salesforce profiles to be managed from a central system of record, the architect should recommend to implement JIT provisioning on the SAML IDP that will pass the profile ID in each assertion. JIT provisioning is a process that creates or updates user accounts on Salesforce based on information sent by an external identity provider (IDP) during SAML authentication. By passing the profile ID in each assertion, the IDP can control which profile is assigned to each user. Option B is not a good choice because creating an Apex scheduled job in one org that will synchronize the other orgs profile may not be scalable, reliable, or secure. Option C is not a good choice because implementing Delegated Authentication that will update the user profiles as necessary may not be feasible, as Delegated Authentication only verifies the user's credentials against an external service, but does not pass any other information to Salesforce. Option D is not a good choice because implementing an OAuth2 JWT flow to pass the profile credentials between systems may not be suitable, as OAuth2 JWT flow is used for server-to-server integration, not for user authentication.

References: Authorize Apps with OAuth, [Identity Management Concepts], [User Authentication]

**NEW QUESTION 160**

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 164

Universal containers (UC) would like to enable SSO between their existing Active Directory infrastructure and salesforce. The it team prefers to manage all users in Active Directory and would like to avoid doing any initial setup of users in salesforce directly, including the correct assignment of profiles, roles and groups. Which two optimal solutions should UC use to provision users in salesforce? Choose 2 answers

- A. Use the salesforce REST API to sync users from active directory to salesforce
- B. Use an app exchange product to sync users from Active Directory to salesforce.
- C. Use Active Directory Federation Services to sync users from active directory to salesforce.
- D. Use Identity connect to sync users from Active Directory to salesforce

**Answer:** BD

#### Explanation:

To provision users in Salesforce from Active Directory without doing any initial setup of users in Salesforce, UC can use an app exchange product or Identity Connect. An app exchange product is a third-party application that can synchronize users and groups from Active Directory to Salesforce using a web-based interface<sup>1</sup>. Identity Connect is a desktop application that can synchronize users and groups from Active Directory to Salesforce using a graphical user interface<sup>2</sup>. Both solutions can also map Active Directory attributes to Salesforce fields and assign profiles, roles, and permission sets to users<sup>12</sup>.

References: Active Directory Integration with Salesforce, Identity Connect

#### NEW QUESTION 165

An Identity architect works for a multinational, multi-brand organization. As they work with the organization to understand their Customer Identity and Access Management requirements, the identity architect learns that the brand experience is different for each of the customer's sub-brands and each of these branded experiences must be carried through the login experience depending on which sub-brand the user is logging into.

Which solution should the architect recommend to support scalability and reduce maintenance costs, if the organization has more than 150 sub-brands?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 168

Universal Containers (UC) currently uses Salesforce Sales Cloud and an external billing application. Both Salesforce and the billing application are accessed several times a day to manage customers. UC would like to configure single sign-on and leverage Salesforce as the identity provider. Additionally, UC would like the billing application to be accessible from Salesforce. A redirect is acceptable.

Which two Salesforce tools should an identity architect recommend to satisfy the requirements? Choose 2 answers

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

**Answer:** AD

#### Explanation:

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

#### NEW QUESTION 173

Universal Containers want users to be able to log in to the Salesforce mobile app with their Active Directory password. Employees are unable to use mobile VPN. Which two options should an identity architect recommend to meet the requirement? Choose 2 answers

- A. Active Directory Password Sync Plugin
- B. Configure Cloud Provider Load Balancer
- C. Salesforce Trigger & Field on Contact Object
- D. Salesforce Identity Connect

**Answer:** AD

#### Explanation:

Active Directory Password Sync Plugin allows users to log in to Salesforce with their Active Directory password without using a VPN. Salesforce Identity Connect



synchronizes users and groups between Active Directory and Salesforce and enables single sign-on. References: Active Directory Password Sync Plugin, Salesforce Identity Connect

**NEW QUESTION 176**

Northern Trail Outfitters (NTO) has a number of employees who do NOT need access Salesforce objects. Trie employees should sign in to a custom Benefits web app using their Salesforce credentials.

Which license should the identity architect recommend to fulfill this requirement?

- A. Identity Only License
- B. External Identity License
- C. Identity Verification Credits Add-on License
- D. Identity Connect License

**Answer:** A

**Explanation:**

To allow employees to sign in to a custom Benefits web app using their Salesforce credentials, the identity architect should recommend 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 181**

Universal containers (UC) has a mobile application that it wants to deploy to all of its salesforce users, including customer Community users. UC would like to minimize the administration overhead, which two items should an architect recommend? Choose 2 answers

- A. Enable the "Refresh Tokens is valid until revoked " setting in the Connected App.
- B. Enable the "Enforce Ip restrictions" settings in the connected App.
- C. Enable the "All users may self-authorize" setting in the Connected App.
- D. Enable the "High Assurance session required" setting in the Connected App.

**Answer:** AC

**Explanation:**

The two items that an architect should recommend for UC to minimize the administration overhead are:

- Enable the “Refresh Tokens is valid until revoked” setting in the Connected App. This setting 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. By enabling this setting in the Connected App, UC can reduce the number of login prompts and authentication failures for its mobile users, as they can use the refresh token to renew their access without entering their credentials again.
- Enable the “All users may self-authorize” setting in the Connected App. This setting allows users to grant access to the mobile app without administrator approval. By enabling this setting in the Connected App, UC can simplify and speed up the deployment process for its mobile app, as they do not need to manually authorize each user or group of users.

The other options are not recommended items for this scenario. Enabling the “Enforce IP restrictions” setting in the Connected App would limit the mobile app access to certain IP ranges, which could prevent some users from accessing the app from different locations or networks. Enabling the “High Assurance session required” setting in the Connected App would require users to verify their identity with a second factor before accessing the mobile app, which could increase complexity and inconvenience for users. References: [Connected Apps], [Refresh Token], [All Users May Self-Authorize], [IP Restrictions for Connected Apps], [Require a Second Factor of Authentication for Connected Apps]

**NEW QUESTION 182**

A consumer products company uses Salesforce to maintain consumer information, including orders. The company implemented a portal solution using Salesforce Experience Cloud for its consumers where the consumers can log in using their credentials. The company is considering allowing users to login with their Facebook or LinkedIn credentials.

Once enabled, what role will Salesforce play?

- A. Facebook and LinkedIn will be the SPs.
- B. Salesforce will be the service provider (SP).
- C. Salesforce will be the identity provider (IdP).
- D. Facebook and LinkedIn will act as the IdPs and SPs.

**Answer:** B

**Explanation:**

To allow users to login with their Facebook or LinkedIn credentials, Salesforce will play the role of a service provider (SP). A SP is an entity that relies on an identity provider (IdP) to authenticate and authorize users. In this scenario, Facebook and LinkedIn are the IdPs, and Salesforce is the SP. The SP receives a token from the IdP and uses it to access Salesforce resources. The other options are not correct for this scenario. References: Service Provider, Social Sign-On with Authentication Providers

**NEW QUESTION 187**

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 188

Northern Trail Outfitters want to allow its consumer to self-register on its business-to-consumer (B2C) portal that is built on Experience Cloud. The identity architect has recommended to use Person Accounts.

Which three steps need to be configured to enable self-registration using person accounts? Choose 3 answers

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

**Answer:** ACD

#### Explanation:

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

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

#### NEW QUESTION 193

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

- A. Resource deep linking
- B. App launcher
- C. SSO from Salesforce1 mobile app.
- D. Login forensics

**Answer:** AC

#### Explanation:

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

#### NEW QUESTION 198

A real estate company wants to provide its customers a digital space to design their interior decoration options. To simplify the registration to gain access to the community site (built in Experience Cloud), the CTO has requested that the IT/Development team provide the option for customers to use their existing social-media credentials to register and access.

The IT lead has approached the Salesforce Identity and Access Management (IAM) architect for technical direction on implementing the social sign-on (for Facebook, Twitter, and a new provider that supports standard OpenID Connect (OIDC)).

Which two recommendations should the Salesforce IAM architect make to the IT Lead? Choose 2 answers

- A. Use declarative registration handler process builder/flow to create, update users and contacts.
- B. Authentication provider configuration is required each social sign-on providers; and enable Authentication providers in community.
- C. For supporting OIDC it is necessary to enable Security Assertion Markup Language (SAML) with Just-in-Time provisioning (JIT) and OAuth 2.0.
- D. Apex coding skills are needed for registration handler to create and update users.

**Answer:** BD

#### Explanation:

Authentication provider configuration and Apex coding skills are two recommendations that the Salesforce IAM architect should make to the IT Lead.

Authentication providers are used to configure social sign-on providers, such as Facebook, Twitter, and any OpenID Connect compliant provider. Apex coding skills are needed for registration handlers, which are custom classes that create and update users based on social sign-on data. References: Authentication Providers, Registration Handlers

#### NEW QUESTION 202

Universal Containers is creating a mobile application that will be secured by Salesforce Identity using the OAuth 2.0 user-agent flow (this flow uses the OAuth 2.0 implicit grant type).

Which three OAuth concepts apply to this flow? Choose 3 answers

- A. Client ID
- B. Refresh Token

- C. Authorization Code
- D. Verification Code
- E. Scopes

**Answer:** AE

**Explanation:**

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

**NEW QUESTION 203**

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 204**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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](#)**