



## **Salesforce**

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

Salesforce Certified Identity and Access Management Architect (SU23)

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

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.

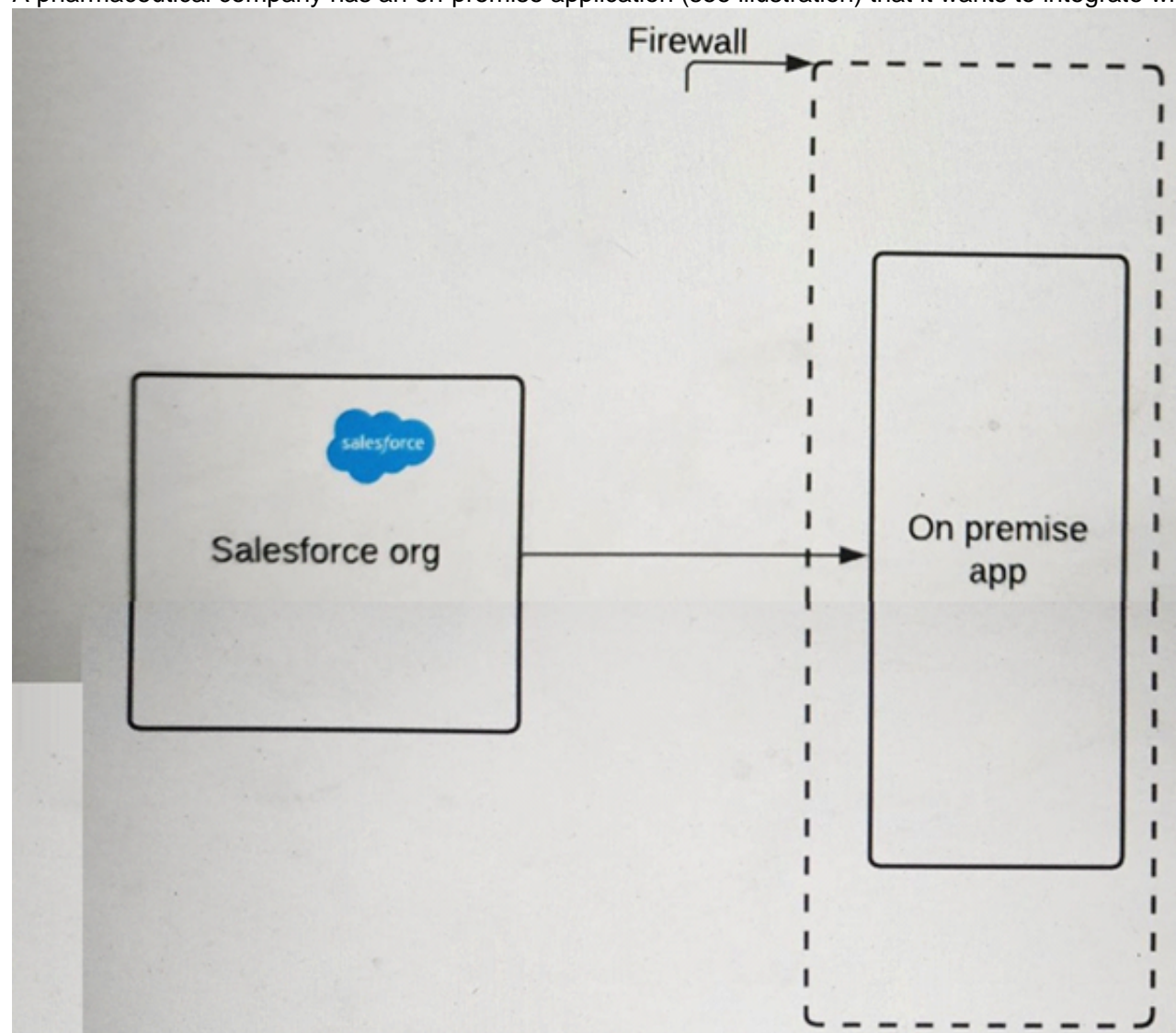
B is incorrect because using a self-signed certificate does not make the trusted party act as the trusted CA (Certificate Authority). The trusted CA is the entity that issues and validates certificates for servers. The trusted party only needs to trust the CA's root certificate, which is usually pre-installed 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 2

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



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

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

**Answer: C**

#### Explanation:

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

### NEW QUESTION 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 is considering using Delegated Authentication as the sole means of Authenticating of Salesforce users. A Salesforce Architect has been brought in to assist with the implementation. What two risks Should the Architect point out? Choose 2 answers

- A. Delegated Authentication is enabled or disabled for the entire Salesforce org.
- B. UC will be required to develop and support a custom SOAP web service.
- C. Salesforce users will be locked out of Salesforce if the web service goes down.
- D. The web service must reside on a public cloud service, such as Heroku.

**Answer:** BC

#### Explanation:

The two risks that the architect should point out for using delegated authentication as the sole means of authenticating Salesforce users are:

➤ UC will be required to develop and support a custom SOAP web service. 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 requires UC to develop and support a custom SOAP web service that can accept and validate the user's username and password, and return a boolean value to indicate whether the authentication is successful or not. This could increase complexity and cost for UC, as they need to write custom code and maintain the web service.

➤ Salesforce users will be locked out of Salesforce if the web service goes down. Delegated authentication relies on the availability and performance of the external web service that handles the authentication requests from Salesforce. If the web service goes down or becomes slow, Salesforce users will not be able to log in or access Salesforce, as they will receive an error message or a timeout response. This could cause disruption and frustration for UC's business operations and user satisfaction.

The other options are not valid risks for using delegated authentication. Delegated authentication can be enabled or disabled for individual users or groups of users by using permission sets or profiles, not for the entire Salesforce org. The web service does not need to reside on a public cloud service, such as Heroku, as it can be hosted on any platform that supports SOAP services and can communicate with Salesforce. References: [Delegated Authentication], [Enable 'Delegated Authentication'], [Troubleshoot Delegated Authentication]

### NEW QUESTION 5

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 6



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 7**

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 8**

Universal Containers wants to implement single Sign-on for a Salesforce org using an external identity provider and corporate identity store. What type of Authentication flow is required to support deep linking?

- A. Web server OAuth SSO flow.
- B. Identity-provider-initiated SSO
- C. Service-provider-initiated SSO
- D. Start URL on identity provider

**Answer:** C

**Explanation:**

Service-provider-initiated SSO is required to support deep linking, which is the ability to direct users to a specific page within Salesforce from a different app. With service-provider-initiated SSO, the user requests a resource from Salesforce (the service provider), which then redirects the user to the identity provider for authentication. After the user is authenticated, the identity provider sends a SAML response back to Salesforce, which then grants access to the requested resource. Web server OAuth SSO flow is used for OAuth 2.1 authentication, not SAML. Identity-provider-initiated SSO is when the user logs in to the identity provider first and then selects a service provider to access. Start URL on identity provider is not a type of authentication flow, but a parameter that can be used to specify the landing page after SSO. References: Certification - Identity and Access Management Architect - Trailhead, Deep Linking, Single Sign On Deep Linking - Salesforce Developer Community

**NEW QUESTION 9**

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 10**

A third-party app provider would like to have users provisioned via a service endpoint before users access their app from Salesforce.

What should an identity architect recommend to configure the requirement with limited changes to the third-party app?

- A. Use a connected app with user provisioning flow.
- B. Create Canvas app in Salesforce for third-party app to provision users.
- C. Redirect users to the third-party app for registration.

D. Use Salesforce identity with Security Assertion Markup Language (SAML) for provisioning users.

**Answer:** A

**Explanation:**

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

**NEW QUESTION 10**

An identity architect has built a native mobile application and plans to integrate it with a Salesforce Identity solution. The following are the requirements for the solution:

- \* 1. Users should not have to login every time they use the app.
- \* 2. The app should be able to make calls to the Salesforce REST API.
- \* 3. End users should NOT see the OAuth approval page.

How should the identity architect configure the Salesforce connected app to meet the requirements?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 12**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 16**

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

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

**Answer:** CD

**Explanation:**

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

References:

➤ [Customize Self-Registration](#)

**NEW QUESTION 17**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 19**

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 24**

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

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

**Answer:** AD

**Explanation:**

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

**NEW QUESTION 25**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 26**

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

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



**Answer:** CD

**Explanation:**

The two options that an architect should recommend to UC are to build a custom web service that is supported by delegated authentication and to implement the OpenID protocol and configure an authentication provider. Delegated authentication is a feature that allows Salesforce to delegate user authentication to an external service instead of using Salesforce credentials<sup>3</sup>. A custom web service can be built to use the credentials stored in the custom identity store and validate them against Salesforce using SOAP or REST API<sup>3</sup>. OpenID is an open standard protocol that allows users to authenticate with various web services using an existing account<sup>4</sup>. An authentication provider can be configured in Salesforce to use OpenID and connect with the custom identity store<sup>5</sup>.

References: Delegated Authentication, OpenID, Authentication Providers

**NEW QUESTION 29**

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

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

**Answer:** AD

**Explanation:**

The appropriate license type choices for sales and marketing users, given that Salesforce is using delegated authentication, are:

➤ Salesforce license for sales users. This license type allows internal users, such as employees, to access standard and custom Salesforce objects and features, such as opportunities and reports. This license type also supports delegated authentication, which is a feature that allows Salesforce to delegate the authentication process to an external service by making a SOAP callout to a web service that verifies the user's credentials. This license type is suitable for sales users who use Salesforce for opportunity management and need to log in with delegated authentication.

➤ Platform license for marketing users. This license type allows internal users to access custom Salesforce objects and features, such as custom apps and tabs. This license type also supports delegated authentication and single sign-on (SSO), which are features that allow users to log in with an external identity provider (IdP) or service provider (SP). This license type is suitable for marketing users who use a third-party application called Nest for lead nurturing and need to log in with SSO using Salesforce as the IdP or SP.

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

**NEW QUESTION 34**

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 38**

Universal containers (UC) uses a legacy Employee portal for their employees to collaborate and post their ideas. UC decides to use salesforce ideas for voting and better tracking purposes. To avoid provisioning users on Salesforce, UC decides to push ideas posted on the Employee portal to salesforce through API. UC decides to use an API user using OAuth Username - password flow for the connection. How can the connection to salesforce be restricted only to the employee portal server?

- A. Add the Employee portals IP address to the Trusted IP range for the connected App
- B. Use a digital certificate signed by the employee portal Server.
- C. Add the employee portals IP address to the login IP range on the user profile.
- D. Use a dedicated profile for the user the Employee portal uses.

**Answer:** A

**Explanation:**

Adding the employee portal's IP address to the trusted IP range for the connected app is the best way to restrict the connection to Salesforce only to the employee portal server. This will ensure that only requests from the specified IP range will be accepted by Salesforce for that connected app. Option B is not a good choice because using a digital certificate signed by the employee portal server may not be supported by Salesforce for OAuth username-password flow. Option C is not a good choice because adding the employee portal's IP address to the login IP range on the user profile may not be sufficient, as it will still allow other users with the same profile to log in from that IP range. Option D is not a good choice because using a dedicated profile for the user that the employee portal uses may not be



effective, as it will still allow other users with that profile to log in from any IP address. References: [Connected Apps], [OAuth 2.0 Username-Password Flow]

#### NEW QUESTION 41

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 42

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 45

A university is planning to set up an identity solution for its alumni. A third-party identity provider will be used for single sign-on Salesforce will be the system of records. Users are getting error messages when logging in. Which Salesforce feature should be used to debug the issue?

- A. Apex Exception Email
- B. View Setup Audit Trail
- C. Debug Logs
- D. Login History

**Answer:** D

#### NEW QUESTION 47

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 51

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 52**

Universal Containers uses an Employee portal for their employees to collaborate. Employees access the portal from their company's internal website via SSO. It is set up to work with Active Directory. What is the role of Active Directory in this scenario?

- A. Identity store
- B. Authentication store
- C. Identity provider
- D. Service provider

**Answer:** C

**Explanation:**

The role of Active Directory in this scenario is an identity provider. An identity provider is an application that authenticates users and provides information about them to service providers<sup>6</sup>. A service provider is an application that provides a service to users and relies on an identity provider for authentication<sup>6</sup>. In this scenario, the employee portal is a service provider that provides collaboration features to employees and relies on Active Directory for authentication. Active Directory is an identity provider that authenticates employees using their corporate credentials and sends information about them to the employee portal<sup>7</sup>.

References: Identity Provider Overview, Configure SSO to Salesforce Using Microsoft AD FS as the Identity Provider

**NEW QUESTION 55**

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 60**

Northern Trail Outfitters (NTO) is setting up Salesforce to authenticate users with an external identity provider. The NTO Salesforce Administrator is having trouble getting things setup.

What should an identity architect use to show which part of the login assertion is failing?

- A. SAML Metadata file importer
- B. Identity Provider Metadata download
- C. Connected App Manager
- D. Security Assertion Markup Language Validator

**Answer:** D

**Explanation:**

Security Assertion Markup Language (SAML) Validator is a tool that allows administrators to test and troubleshoot SAML single sign-on configurations. It can show which part of the login assertion is failing and provide error messages and suggestions. SAML Metadata file importer and Identity Provider Metadata download are features that allow administrators to import or download metadata files for SAML configurations. Connected App Manager is a tool that allows administrators to manage connected apps in Salesforce. References: SAML Validator, SAML Single Sign-On Settings, Connected App Manager

**NEW QUESTION 61**

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 66

A public sector agency is setting up an identity solution for its citizens using a Community built on Experience Cloud and requires the new user registration functionality to capture first name, last name, and phone number. The phone number will be used for identity verification. Which feature should an identity architect recommend to meet the requirements?

- A. Integrate with social websites (Facebook, LinkedIn)
- B. Twitter)
- C. Use an external Identity Provider
- D. Create a custom Lightning Web Component
- E. Use Login Discovery

**Answer: D**

#### Explanation:

Login Discovery allows the administrator to configure a custom login page that collects additional information from users, such as phone number, and use it for identity verification. Login Discovery can also be used to route users to different identity providers based on their input. References: Login Discovery, Customize Your Experience Cloud Site Login Process

#### NEW QUESTION 67

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 70

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 74

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 77

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

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 79

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

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

**Answer:** B

#### Explanation:

Using SAML Federated Authentication, treating SAML sessions as high assurance, and raising the session level required for exporting reports is the solution that should be recommended. This solution ensures that users can only export reports when they log in using AD credentials, which provide a high level of identity verification. Users who log in using Salesforce credentials, which provide a standard level of security, can still view reports but not export them. To implement this solution, you need to configure SAML Federated Authentication with AD as the identity provider<sup>4</sup>, set the session security level for SAML assertions to high assurance<sup>5</sup>, and require high-assurance session security for exporting reports<sup>1</sup>. This solution also avoids the complexity and overhead of creating and managing custom permission sets or login flows.

#### NEW QUESTION 81

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

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

**Answer:** C

#### Explanation:

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

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

#### NEW QUESTION 84

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 85**

Northern Trail Outfitters (NTO) is planning to implement a community for its customers using Salesforce Experience Cloud. Customers are not able to self-register. NTO would like to have customers set their own passwords when provided access to the community.

Which two recommendations should an identity architect make to fulfill this requirement? Choose 2 answers

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

**Answer:** CD

**Explanation:**

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

**NEW QUESTION 89**

Universal containers (UC) have a custom, internal-only, mobile billing application for users who are commonly out of the office. The app is configured as a connected App in salesforce. Due to the nature of this app, UC would like to take the appropriate measures to properly secure access to the app. Which two are recommendations to make the UC? Choose 2 answers

- A. Disallow the use of single Sign-on for any users of the mobile app.
- B. Require high assurance sessions in order to use the connected App
- C. Use Google Authenticator as an additional part of the logical processes.
- D. Set login IP ranges to the internal network for all of the app users profiles.

**Answer:** BC

**Explanation:**

High assurance sessions are sessions that require a stronger level of identity verification, such as two-factor authentication or SAML assertions<sup>1</sup>. Google Authenticator is an app that generates verification codes on your mobile device that you can use as a second factor of authentication<sup>2</sup>. These measures can help prevent unauthorized access to the connected app by ensuring that the user is who they claim to be and that they have access to their mobile device. Disallowing the use of single sign-on (SSO) for the mobile app is not a recommendation because SSO can provide a seamless and secure user experience across multiple applications<sup>3</sup>. Setting login IP ranges to the internal network for the app users profiles is not a recommendation because it can limit the mobility and flexibility of the users who are commonly out of the office. References: 1: Session Security Levels 2: Google Authenticator 3: Connected Apps : [Restri Access by IP Address]

**NEW QUESTION 93**

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

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

**Answer:** B

**Explanation:**

The users do not have the correct permission set assigned to them is the most likely cause of the issue. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID 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 98**

Which two statements are capable of Identity Connect? Choose 2 answers

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

**Answer:** BD

**Explanation:**

The two statements that are capabilities of Identity Connect are:

- It supports both identity-provider-initiated and service-provider-initiated SSO. Identity Connect is a desktop application that integrates Salesforce with Microsoft Active Directory (AD) and enables single sign-on (SSO) between the two systems. Identity Connect supports both identity-provider-initiated SSO, which is when the user starts at the AD site and then is redirected to Salesforce with a SAML assertion, and service-provider-initiated SSO, which is when the user starts at the Salesforce site and then is redirected to AD for authentication.
- It enables automated user synchronization and deactivation. Identity Connect allows administrators to synchronize user accounts and attributes between AD and Salesforce, either manually or on a scheduled basis. Identity Connect also allows administrators to deactivate user accounts in Salesforce when they are disabled or deleted in AD, which helps maintain security and compliance.

The other options are not capabilities of Identity Connect. Identity Connect does not support synchronization of Salesforce permission set license assignments, as these are not related to AD attributes. Identity Connect does not support multiple orgs connecting to multiple AD servers, as it can only connect one Salesforce org to one AD domain at a time. References: [Identity Connect], [Identity Connect Features], [Identity Connect User Synchronization], [Identity Connect Single Sign-On]

**NEW QUESTION 100**

Universal Containers (UC) has implemented a multi-org architecture in their company. Many users have licences across multiple orgs, and they are complaining about remembering which org and credentials are tied to which business process. Which two recommendations should the Architect make to address the Complaints? Choose 2 answers

- A. Activate My Domain to Brand each org to the specific business use case.
- B. Implement SP-Initiated Single Sign-on flows to allow deep linking.
- C. Implement IdP-Initiated Single Sign-on flows to allow deep linking.
- D. Implement Delegated Authentication from each org to the LDAP provider.

**Answer:** AB

**Explanation:**

Activating My Domain allows each org to have a unique domain name that can be branded to the specific business use case<sup>2</sup>. This can help users identify which org they are logging into and avoid confusion. Implementing SP-Initiated Single Sign-on flows enables users to start from a service provider (such as Salesforce) and be redirected to an identity provider (such as Active Directory) for authentication<sup>3</sup>. This can also allow deep linking, which means users can access specific resources within the service provider after logging in<sup>4</sup>. These two recommendations can address the complaints of the users who have licenses across multiple orgs.

**NEW QUESTION 102**

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

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

**Answer:** D

**Explanation:**

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

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

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

**NEW QUESTION 103**

A security architect is rolling out a new multi-factor authentication (MFA) mandate, where all employees must go through a secure authentication process before accessing Salesforce. There are multiple Identity Providers (IdP) in place and the architect is considering how the "Authentication Method Reference" field (AMR) in the Login History can help.

Which two considerations should the architect keep in mind? Choose 2 answers

- A. AMR field shows the authentication methods used at IdP.
- B. Both OIDC and Security Assertion Markup Language (SAML) are supported but AMR must be implemented at IdP.

- C. High-assurance sessions must be configured under Session Security Level Policies.
- D. Dependency on what is supported by OpenID Connect (OIDC) implementation at IdP.

**Answer:** AB

**Explanation:**

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

**NEW QUESTION 106**

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 111**

Universal Containers is implementing Salesforce Identity to broker authentication from its enterprise single sign-on (SSO) solution through Salesforce to third party applications using SAML.

What role does Salesforce Identity play in its relationship with the enterprise SSO system?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 114**

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<sup>3</sup>. Therefore, option A is the correct answer. References: SAML



## SSO with Salesforce as the Service Provider

### NEW QUESTION 116

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

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

**Answer: B**

#### Explanation:

The Entity ID is a unique identifier for a service provider or an identity provider in SAML SSO. It is used to differentiate between different service providers or identity providers that may share the same issuer or login URL. In Salesforce, the Entity ID is automatically generated based on the organization ID and can be viewed in the Single Sign-On Settings page<sup>1</sup>. If you have a custom domain set up, you can use [https:// \[customDomain\].my.salesforce.com](https://[customDomain].my.salesforce.com) as the Entity ID<sup>2</sup>. If you want to use the same IdP for two Salesforce orgs, you need to use different Entity IDs for each org, otherwise the IdP will not be able to distinguish them and may send incorrect assertions. You can also use different certificates, issuers, or login URLs for each org, but using different Entity IDs is the simplest and recommended way<sup>3</sup>.

### NEW QUESTION 121

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

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

**Answer: D**

#### Explanation:

D is correct because Salesforce is an independent system that is not part of the SSO setup between the Employee portal and Active Directory. Salesforce does not act as an IdP or an SP for the SSO, nor does it use a connected app to integrate with the Employee portal. Salesforce only exposes its API to allow the Employee portal to access its ideas feature.

A is incorrect because Salesforce is not a service provider for the SSO. The SSO is between the Employee portal and Active Directory, not between the Employee portal and Salesforce.

B is incorrect because Salesforce is not a connected app for the SSO. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect<sup>1</sup>. The Employee portal does not use any of these protocols to integrate with Salesforce, but only uses its API.

C is incorrect because Salesforce is not an identity provider for the SSO. The IdP is the system that authenticates users and issues tokens or assertions to allow access to other systems. In this scenario, the IdP is Active Directory, not Salesforce.

References: 1: OAuth Authorization flows in Salesforce - Apex Hours

### NEW QUESTION 126

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 set
- 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 130

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 131

Universal Containers (UC) has a mobile application for its employees that uses data from Salesforce as well as uses Salesforce for Authentication purposes. UC wants its mobile users to only enter their credentials the first time they run the app. The application has been live for a little over 6 months, and all of the users who were part of the initial launch are complaining that they have to re-authenticate. UC has also recently changed the URI Scheme associated with the mobile app. What should the Architect at UC first investigate? Universal Containers (UC) has a mobile application for its employees that uses data from Salesforce as well as uses Salesforce for Authentication purposes. UC wants its mobile users to only enter their credentials the first time they run the app. The application has been live for a little over 6 months, and all of the users who were part of the initial launch are complaining that they have to re-authenticate. UC has also recently changed the URI Scheme associated with the mobile app. What should the Architect at UC first investigate?

- A. Check the Refresh Token policy defined in the Salesforce Connected App.
- B. Validate that the users are checking the box to remember their passwords.
- C. Verify that the Callback URL is correctly pointing to the new URI Scheme.
- D. Confirm that the access Token's Time-To-Live policy has been set appropriately.

**Answer:** A

#### Explanation:

The first thing that the architect at UC should investigate is the refresh token policy defined in the Salesforce connected app. A refresh token is a credential that allows an application to obtain new access tokens without requiring the user to re-authenticate. The refresh token policy determines how long a refresh token is valid and under what conditions it can be revoked. If the refresh token policy is set to expire after a certain period of time or after a change in IP address or device ID, then the users may have to re-authenticate after using the app for a while or from a different location or device. Option B is not a good choice because validating that the users are checking the box to remember their passwords may not be relevant, as the app uses SSO with a third-party identity provider and does not rely on Salesforce credentials. Option C is not a good choice because verifying that the callback URL is correctly pointing to the new URI scheme may not be necessary, as the callback URL is used for redirecting the user back to the app after authentication, but it does not affect how long the user can stay authenticated. Option D is not a good choice because confirming that the access token's time-to-live policy has been set appropriately may not be effective, as the access token's time-to-live policy determines how long an access token is valid before it needs to be refreshed by a refresh token, but it does not affect how long a refresh token is valid or when it can be revoked. References: [Connected Apps Developer Guide], [Digging Deeper into OAuth 2.0 on Force.com]

#### NEW QUESTION 134

Universal Containers allows employees to use a mobile device to access Salesforce for daily operations using a hybrid mobile app. This app uses Mobile software development kits (SDK), leverages refresh token to regenerate access token when required and is distributed as a private app.

The chief security officer is rolling out an org wide compliance policy to enforce re-verification of devices if an employee has not logged in from that device in the last week.

Which connected app setting should be leveraged to comply with this policy change?

- A. Scope - Deny refresh\_token scope for this connected app.
- B. Refresh Token Policy - Expire the refresh token if it has not been used for 7 days.
- C. Session Policy - Set timeout value of the connected app to 7 days.
- D. Permitted User - Ask admins to maintain a list of users who are permitted based on last login date.

**Answer:** B

#### Explanation:

Refresh Token Policy - Expire the refresh token if it has not been used for 7 days is the connected app setting that should be leveraged to comply with the policy change. This setting ensures that users have to re-verify their devices if they have not logged in from that device in the last week. The other settings are either not relevant or not effective for this scenario. References: Connected App Basics, OAuth 2.0 Refresh Token Flow

#### NEW QUESTION 138

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 143

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 2.0<sup>7</sup>.

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

**NEW QUESTION 145**

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

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

**Answer:** AD

**Explanation:**

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

- Option A is correct because configuring SAML SSO settings involves specifying the identity provider details, such as the entity ID, login URL, logout URL, and certificate<sup>2</sup>.
- Option D is correct because setting up My Domain enables you to use a custom domain name for your Salesforce org and allows you to use SAML as an authentication method<sup>3</sup>.
- Option B is incorrect because creating a connected app is not necessary for SP-initiated SSO using a SAML-compliant IdP. A connected app is used for OAuth-based authentication or OpenID Connect-based authentication<sup>4</sup>.
- Option C is incorrect because configuring delegated authentication is not related to SP-initiated SSO using a SAML-compliant IdP. Delegated authentication is a feature that allows Salesforce to delegate user authentication to an external service, such as LDAP or Active Directory<sup>5</sup>.

References: SAML-based single sign-on: Configuration and Limitations, Configure SAML single sign-on with an identity provider, My Domain, Create a Connected App, Configure Salesforce for Delegated Authentication

**NEW QUESTION 147**

Universal containers(UC) has decided to build a new, highly sensitive application on Force.com platform. The security team at UC has decided that they want users to provide a fingerprint in addition to username/Password to authenticate to this application. How can an architect support fingerprint as a form of identification for salesforce Authentication?

- A. Use salesforce Two-factor Authentication with callouts to a third-party fingerprint scanning application.
- B. Use Delegated Authentication with callouts to a third-party fingerprint scanning application.
- C. Use an AppExchange product that does fingerprint scanning with native salesforce identity confirmation.
- D. Use custom login flows with callouts to a third-party fingerprint scanning application.

**Answer:** D

**Explanation:**

D is correct because using custom login flows with callouts to a third-party fingerprint scanning application allows UC to support fingerprints as a form of identification for Salesforce authentication. Custom login flows allow UC to implement custom logic and UI elements for authentication, such as calling an external web service that performs fingerprint scanning and verification. A is incorrect because using Salesforce two-factor authentication with callouts to a third-party fingerprint scanning application does not support fingerprints as a form of identification for Salesforce authentication. Salesforce two-factor authentication requires users to enter a verification code or use an app like Salesforce Authenticator, not a fingerprint. B is incorrect because using delegated authentication with callouts to a third-party fingerprint scanning application does not support fingerprints as a form of identification for Salesforce authentication. Delegated authentication requires users to enter their username and password, not a fingerprint. C is incorrect because using an AppExchange product that does fingerprint scanning with native Salesforce identity confirmation does not support fingerprints as a form of identification for Salesforce authentication. AppExchange products are third-party applications that integrate with Salesforce, not native Salesforce features. Verified References: [Custom Login Flows], [Two-Factor Authentication], [Delegated Authentication], [AppExchange]

**NEW QUESTION 149**

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 151**

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 156**

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

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

**Answer:** ABC

**Explanation:**

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

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

**NEW QUESTION 161**

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 164**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 165**

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 flow to pass the profile credentials between systems may not be suitable, as OAuth2 flow is used for server-to-server integration, not for user authentication.

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

**NEW QUESTION 169**

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

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

**Answer:** A

**Explanation:**

The CA-Signed Certificate from the Certificate and Key Management menu is the certificate that is sent along with the outbound message. An outbound message is a SOAP message that is sent from Salesforce to an external endpoint when a workflow rule or approval process is triggered. To ensure that the communication between Salesforce and the target system is secure, the outbound message can be signed with a certificate that is generated or uploaded in the Certificate and Key Management menu. The certificate must be CA-Signed, which means that it is issued by a trusted certificate authority (CA) that verifies the identity of the sender. The other options are not valid certificates for this purpose. The default client certificate from the Develop--> API Menu is a self-signed certificate that is used for testing purposes only and does not provide adequate security. The default client certificate or a certificate from Certificate and Key Management menu is too vague and does not specify whether the certificate is CA-Signed or self-signed. The self-signed certificates from the Certificate & Key Management menu are certificates that are generated by Salesforce without any verification by a CA, and they are not recommended for production use.

References: [Outbound Messages], [Sign Outbound Messages with a Certificate], [CA-Signed Certificates], [Default Client Certificate], [Self-Signed Certificates]



#### NEW QUESTION 171

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

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

**Answer:** ACE

#### Explanation:

AD groups can control public group assignment, role assignment, and permission set assignment through Identity Connect. Identity Connect is a tool that integrates Microsoft Active Directory (AD) user accounts with Salesforce user records<sup>1</sup>. It allows Salesforce admins to leverage the existing user data and group memberships in AD to automate user provisioning and deprovisioning in Salesforce. Identity Connect can map AD groups to Salesforce public groups, roles, and permission sets, and assign them to users based on their group membership<sup>2</sup>. This way, AD groups can control the access level and visibility of users in Salesforce. AD groups cannot control granting report folder access or custom permission assignment through Identity Connect. These are not supported features of Identity Connect. Report folder access is controlled by the folder sharing settings in Salesforce. Custom permission assignment is controlled by the custom permission settings in Salesforce. References: Get to Know Identity Connect, Map Your Data, [Folder Sharing], [Custom Permissions]

#### NEW QUESTION 174

A technology enterprise is planning to implement single sign-on login for users. When users log in to the Salesforce User object custom field, data should be populated for new and existing users.

Which two steps should an identity architect recommend? Choose 2 answers

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

**Answer:** AB

#### Explanation:

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

#### NEW QUESTION 178

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 182

Universal Containers (UC) plans to use a SAML-based third-party IdP serving both of the Salesforce Partner Community and the corporate portal. UC partners will log in 65\* to the corporate portal to access protected resources, including links to Salesforce resources. What would be the recommended way to configure the IdP so that seamless access can be achieved in this scenario?

- A. Set up the corporate portal as a Connected App in Salesforce and use the Web server OAuth flow.
- B. Configure SP-initiated SSO that passes the SAML token upon Salesforce resource access request.
- C. Set up the corporate portal as a Connected App in Salesforce and use the User Agent OAuth flow.
- D. Configure IdP-initiated SSO that passes the SAML token upon Salesforce resource access request.

**Answer:** D

#### Explanation:

The recommended way to configure the IdP for seamless access is to use IdP-initiated SSO that passes the SAML token upon Salesforce resource access request. This means that the user logs in to the corporate portal first, and then clicks a link to access a Salesforce resource. The IdP sends a SAML response to Salesforce with the user's identity and other attributes. Salesforce verifies the SAML response and logs in the user to the appropriate Salesforce org and community<sup>12</sup>. This way, the user does not have to log in again to Salesforce or enter any credentials<sup>3</sup>. References: 1: SAML SSO with Salesforce as the Service Provider 2: Set Up Single Sign-On for Your Internal Users Unit | Salesforce - Trailhead 3: What is IdP-Initiated Single Sign-On? – OneLogin

#### NEW QUESTION 184

Universal Containers is creating a mobile application that will be secured by Salesforce Identity using the OAuth 2.0 user-agent flow. Application users will authenticate using username and password. They should not be forced to approve API access in the mobile app or reauthenticate for 3 months.

Which two connected app options need to be configured to fulfill this use case?

Choose 2 answers

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

**Answer: BD**

#### Explanation:

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

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

#### NEW QUESTION 186

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

- A. Use SAML Federated Authentication and block access to reports when accessed through a Standard Assurance session.
- B. Use SAML Federated Authentication and Custom SAML JIT Provisioning to dynamically add or remove a permission set that grants the Export Reports Permission.
- C. Use SAML federated Authentication, treat SAML Sessions as High Assurance, and raise the session level required for exporting reports.
- D. Use SAML federated Authentication with a Login Flow to dynamically add or remove a Permission Set that grants the Export Reports Permission.

**Answer: C**

#### Explanation:

The best solution to prevent exporting reports except when logged in using AD credentials while maintaining the ability to view reports when logged in with Salesforce credentials is to use SAML federated authentication, treat SAML sessions as high assurance, and raise the session level required for exporting reports. SAML federated authentication is a process that allows users to log in to Salesforce with an external identity provider (IdP), such as AD, that authenticates the user and issues a security token to Salesforce. By treating SAML sessions as high assurance, Salesforce assigns a higher level of trust and security to the sessions that are established by SAML federated authentication. By raising the session level required for exporting reports, Salesforce requires users to have a high assurance session before they can export reports. This solution ensures that only users who log in with AD credentials can export reports, while users who log in with Salesforce credentials can still view reports but not export them.

The other options are not valid solutions for this scenario. Using SAML federated authentication and blocking access to reports when accessed through a standard assurance session would prevent users who log in with Salesforce credentials from viewing reports at all, which is not the desired outcome. Using SAML federated authentication and custom SAML JIT provisioning to dynamically add or remove a permission set that grants the export reports permission would require UC to write custom code and logic to implement the JIT provisioning and manage the permission set, which could increase complexity and cost. Using SAML federated authentication with a login flow to dynamically add or remove a permission set that grants the export reports permission would also require UC to write custom code and logic to implement the login flow and manage the permission set, which could introduce errors and performance issues. References: [SAML Single Sign-On], [Session Security Levels], [Set Session Security Levels for Your Org], [Just-in-Time Provisioning for SAML], [Login Flows]

#### NEW QUESTION 191

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 196

.....

## Relate Links

**100% Pass Your Identity-and-Access-Management-Architect Exam with ExamBible Prep Materials**

<https://www.exambible.com/Identity-and-Access-Management-Architect-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>