



## **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

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

- A. Id
- B. Web
- C. Api
- D. Custom\_permissions

**Answer: D**

#### Explanation:

The most recommended and secure OAuth scope setting for UC's custom mobile app is custom\_permissions. Custom\_permissions are settings that can be used in Apex code or validation rules to check whether a user has access to a custom feature or functionality. Custom\_permissions can also be used as OAuth scopes to limit the access of an external application, such as UC's mobile app, to certain custom features or functionalities in Salesforce. By configuring custom\_permissions as OAuth scopes in the connected app settings, UC can restrict the mobile app access to only the e-signature feature and protect against unauthorized or excessive access.

The other options are not recommended or secure OAuth scope settings for UC's custom mobile app. Id is an OAuth scope that allows the mobile app to access basic information about the user and their org, such as name, email, profile picture, and instance URL. This scope does not provide any access to Salesforce data or features, such as uploading e-signatures. Web is an OAuth scope that allows the mobile app to access Salesforce data and features through a browser or web-view. This scope provides full access to Salesforce data and features, which could expose sensitive information or allow unwanted actions. Api is an OAuth scope that allows the mobile app to make REST or SOAP API calls to Salesforce using the access token. This scope also provides full access to Salesforce data and features, which could compromise security and compliance. References: [OAuth Scopes], [Connected Apps], [Custom Permissions]

### NEW QUESTION 2

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 3

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

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

**Answer: D**

#### Explanation:

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

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

### NEW QUESTION 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**

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

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

**Answer:** CD

**Explanation:**

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

➤ OAuth SAML Bearer Assertion Flow, which allows the client app to use a SAML assertion issued by a trusted identity provider to request an access token from Salesforce. This flow does not require the client app to store any credentials or secrets, and leverages the existing SSO infrastructure between Salesforce and the identity provider.

➤ OAuth JWT Bearer Token Flow, which allows the client app to use a JSON Web Token (JWT) signed by a private key to request an access token from Salesforce. This flow does not require any user interaction or consent, and uses a certificate to verify the identity of the client app.

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

**NEW QUESTION 6**

A 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**

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

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

**Answer:** AC

**Explanation:**

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

two flows can meet the requirement of UC to use OAuth and digital certificates to connect to Salesforce from the recruiting system.

#### NEW QUESTION 8

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

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

**Answer:** BE

#### Explanation:

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

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

References:

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

#### NEW QUESTION 9

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

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

**Answer:** BC

#### Explanation:

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

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

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

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

#### NEW QUESTION 10

Northern Trail Outfitters (NTO) wants its customers to use phone numbers to log in to their new digital portal, which was designed and built using Salesforce Experience Cloud. In order to access the portal, the user will need to do the following:

- \* 1. Enter a phone number and/or email address
- \* 2. Enter a verification code that is to be sent via email or text.

What is the recommended approach to fulfill this requirement?

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

**Answer:** A

#### Explanation:

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



#### NEW QUESTION 10

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

Which two actions should an identity architect recommend to meet these requirements? Choose 2 answers

- A. Create a custom external authentication provider for Facebook.
- B. Configure a predefined authentication provider for Facebook.
- C. Create a custom external authentication provider for Twitter.
- D. Configure a predefined authentication provider for Twitter.

**Answer:** BD

#### Explanation:

To give customers the ability to login with their Facebook and Twitter credentials, the identity architect should configure a predefined authentication provider for Facebook and a predefined authentication provider for Twitter. Authentication providers are configurations that enable users to authenticate with an external identity provider and access Salesforce resources. Salesforce provides predefined authentication providers for some common identity providers, such as Facebook and Twitter, which can be easily configured with minimal customization. Creating a custom external authentication provider is not necessary for this scenario. References: Authentication Providers, Social Sign-On with Authentication Providers

#### NEW QUESTION 14

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

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

**Answer:** A

#### Explanation:

The Entity ID is the SAML SSO setting in Salesforce that provides the capability to differentiate Salesforce from other service providers. The Entity ID is a unique identifier for the service provider that is sent in the SAML request and response messages<sup>1</sup>. The identity provider uses the Entity ID to determine which service provider is requesting or receiving authentication information<sup>2</sup>. You can customize the Entity ID for your Salesforce org or Experience Cloud site in the SAML Single Sign-On Settings page<sup>3</sup>. References: 1: SAML SSO Flows 2: Federated Authentication Using SAML to Log in to Salesforce Org 3: Step 2: Create a SA Single Sign-On Setting in Salesforce

#### NEW QUESTION 18

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

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

**Answer:** D

#### Explanation:

D is correct because External Identity license is designed for customers who need to log in to Salesforce using external authentication providers, such as Facebook and Google. External Identity license also supports App Launcher, which allows customers to access other applications from Salesforce using OAuth or OpenID Connect .

A is incorrect because Customer Community license is designed for customers who need to access data and records in Salesforce, such as cases, accounts, and contacts. Customer Community license does not support App Launcher or external authentication providers.

B is incorrect because Identity license is designed for employees who need to access multiple applications from Salesforce using SSO and App Launcher. Identity license does not support external authentication providers or customer data access.

C is incorrect because Customer Community Plus license is designed for customers who need to access data and records in Salesforce, as well as collaborate with other customers and partners. Customer Community Plus license does not support App Launcher or external authentication providers.

References: : Salesforce Licensing Module - Trailhead : Free Salesforce

Identity-and-Access-Management-Architect Questions ... : Salesforce Licensing Module - Trailhead : Salesforce Licensing Module - Trailhead : Salesforce Licensing Module - Trailhead

#### NEW QUESTION 22

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

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

**Answer:** AD

#### Explanation:

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

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

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

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

#### NEW QUESTION 25

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 29

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 31

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 35

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

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

**Answer: B**

#### Explanation:

The OAuth 2.0 Device Flow is a type of authorization flow that allows users to register an IoT device with limited display input or capabilities, such as a smart TV, a printer, or a smart speaker<sup>1</sup>. The device flow works as follows<sup>1</sup>:

- The device displays or reads out a verification code and a verification URL to the user.
- The user visits the verification URL on another device, such as a smartphone or a laptop, and enters the verification code.

- The user logs in to Salesforce and approves the device.
- The device polls Salesforce for an access token using the verification code.
- Salesforce returns an access token to the device, which can then access Salesforce APIs.

References:

- OAuth 2.0 Device Flow

#### NEW QUESTION 37

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

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

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 42

Containers (UC) has implemented SAML-based single Sign-on for their Salesforce application and is planning to provide access to Salesforce on mobile devices using the Salesforce1 mobile app. UC wants to ensure that Single Sign-on is used for accessing the Salesforce1 mobile App. Which two recommendations should the Architect make? Choose 2 Answers

- A. Configure the Embedded Web Browser to use My Domain URL.
- B. Configure the Salesforce1 App to use the MY Domain URL.
- C. Use the existing SAML-SSO flow along with User Agent Flow.
- D. Use the existing SAML SSO flow along with Web Server Flow.

**Answer:** BC

#### Explanation:

To ensure that SSO is used for accessing the Salesforce1 mobile app, UC should configure the Salesforce1 app to use the My Domain URL instead of the default login.salesforce.com URL. My Domain is a feature that allows UC to create a custom domain name for their Salesforce org that supports SSO with their identity provider. UC should also use the existing SAML-SSO flow along with User Agent Flow, which is an OAuth 2.1 flow that allows users to authenticate with their identity provider through an embedded browser within the mobile app. Verified References: [Configure SSO with Salesforce as a SAML Service Provider], [User-Agent Flow]

#### NEW QUESTION 47

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 52

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



#### NEW QUESTION 55

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 56

Northern Trail Outfitters (NTO) is planning to build a new customer service portal and wants to use passwordless login, allowing customers to login with a one-time passcode sent to them via email or SMS.

How should the quantity of required Identity Verification Credits be estimated?

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 57

Universal Containers (UC) is building a custom Innovation platform on their Salesforce instance. The Innovation platform will be written completely in Apex and Visualforce and will use custom objects to store the Data. UC would like all users to be able to access the system without having to log in with Salesforce credentials. UC will utilize a third-party idp using SAML SSO. What is the optimal Salesforce licence type for all of the UC employees?

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 58

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

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

**Answer: C**

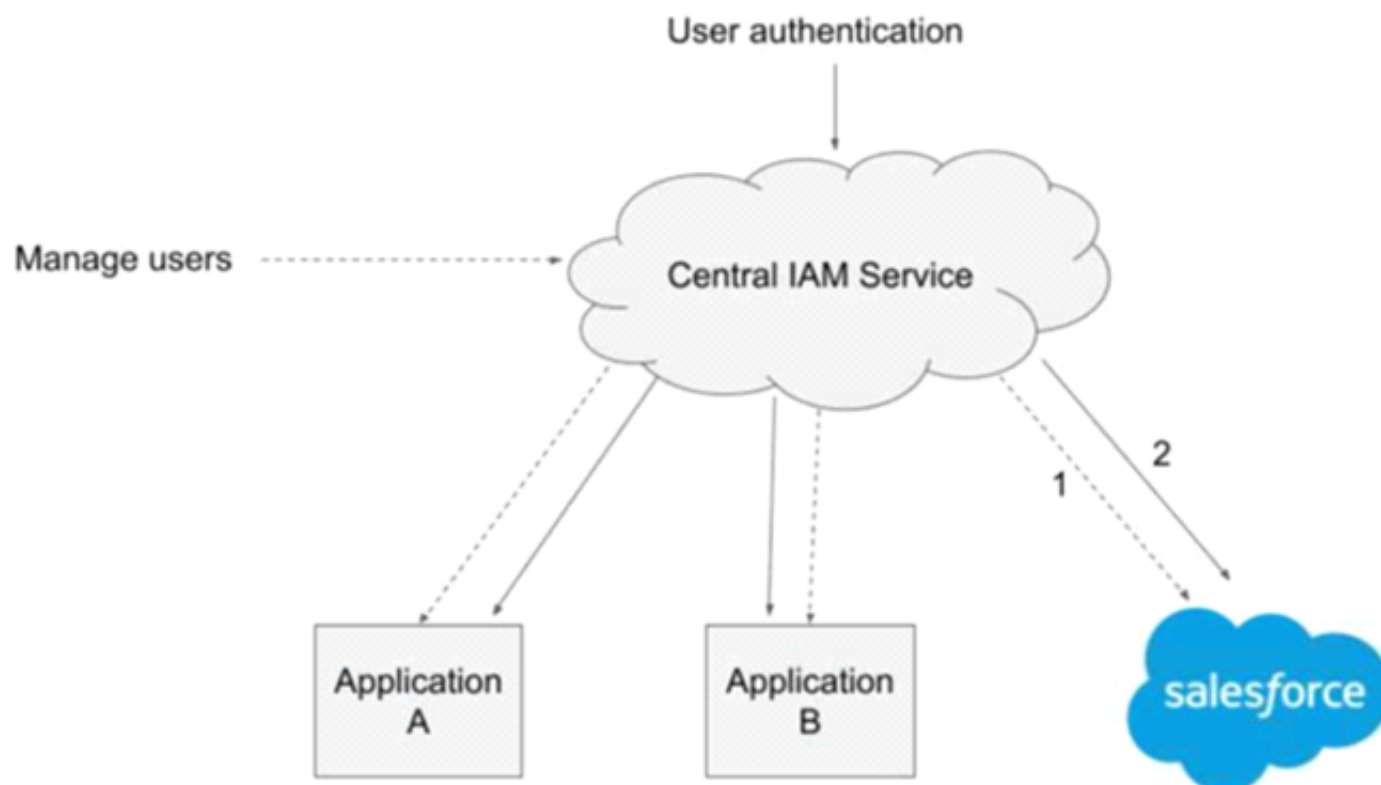
#### Explanation:

The Entity Id is the SAML SSO setting in Salesforce that provides the capability to differentiate Salesforce from other service providers. The Entity Id is a unique identifier for the service provider that is sent to the identity provider as part of the SSO request<sup>4</sup>. The identity provider uses the Entity Id to determine which service provider configuration to use and which SAML assertion to send back<sup>5</sup>. The other options are not valid SAML SSO settings for this purpose. The Identity Provider Login URL is the URL of the identity provider's SSO service that Salesforce redirects the user to for authentication<sup>4</sup>. The Issuer is the unique identifier for the identity provider that is sent by the identity provider as part of the SAML response<sup>4</sup>. The SAML Identity Location is the location of the user's identity in the SAML assertion, either in the Subject element or in an Attribute element<sup>4</sup>.

References: Configure SSO with Salesforce as a SAML Service Provider, Set Up Single Sign-On for Your Internal Users

#### NEW QUESTION 60

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



1 - Change of a user status in the central IAM Service triggers provisioning or deprovisioning in the integrated cloud applications.

2 - Security Assertion Markup Language single sign-on (SSO) is used to facilitate access for users authenticated at identity provider (Central IAM Service).

Which approach should an IAM architect implement on Salesforce Sales Cloud to meet the requirements?

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 61

Universal containers (UC) built a customer Community for customers to buy products, review orders, and manage their accounts. UC has provided three different options for customers to log in to the customer Community: salesforce, Google, and Facebook. Which two role combinations are represented by the systems in the scenario? Choose 2 answers

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

**Answer: BD**

#### Explanation:

The two role combinations that are represented by the systems in the scenario are Salesforce as the service provider and Google as the identity provider, and Salesforce as the service provider and Facebook as the identity provider. This means that Salesforce hosts the customer community app and relies on Google or Facebook to authenticate the users who log in with those options<sup>4</sup>. Therefore, option B and D are the correct answers.

References: Salesforce as Service Provider and Identity Provider for SSO

#### NEW QUESTION 62

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 64**

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 66**

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 68**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 69**

Universal Containers would like its customers to register and log in to a portal built on Salesforce Experience Cloud. Customers should be able to use their Facebook or LinkedIn credentials for ease of use.

Which three steps should an identity architect take to implement social sign-on? Choose 3 answers



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

**Answer:** BCE

**Explanation:**

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

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

**NEW QUESTION 72**

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

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

**Answer:** D

**Explanation:**

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

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

B is incorrect because Salesforce is not a connected app for the SSO. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect1. The Employee portal does not use any of these protocols to integrate with Salesforce, but only uses its API.

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

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

**NEW QUESTION 77**

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 78**

Universal containers (UC) wants to implement Delegated Authentication for a certain subset of Salesforce users. Which three items should UC take into consideration while building the Web service to handle the Delegated Authentication request? Choose 3 answers

- A. The web service needs to include Source IP as a method parameter.
- B. UC should whitelist all salesforce ip ranges on their corporate firewall.
- C. The web service can be written using either the soap or rest protocol.
- D. Delegated Authentication is enabled for the system administrator profile.
- E. The return type of the Web service method should be a Boolean value

**Answer:** ABE



**Explanation:**

Delegated authentication is a feature that allows Salesforce to delegate the authentication process to an external web service. The web service needs to include the source IP address of the user as a method parameter, so that Salesforce can pass it along with the username and password. UC should whitelist all Salesforce IP ranges on their corporate firewall, so that the web service can accept requests from Salesforce. The return type of the web service method should be a Boolean value, indicating whether the authentication was successful or not. The web service can be written using either SOAP or REST protocol, but this is not a consideration for UC while building the web service. Delegated authentication is not enabled for the system administrator profile, but it can be enabled for other profiles or permission sets. References: Certification - Identity and Access Management Architect - Trailhead, [Delegated Authentication Single Sign-On], [Implementing Single Sign-On Across Multiple Organizations]

**NEW QUESTION 83**

Universal Containers (UC) has an existing e-commerce platform and is implementing a new customer community. They do not want to force customers to register on both applications due to concern over the customers experience. It is expected that 25% of the e-commerce customers will utilize the customer community . The e-commerce platform is capable of generating SAML responses and has an existing REST-ful API capable of managing users. How should UC create the identities of its e-commerce users with the customer community?

- A. Use SAML JIT in the Customer Community to create users when a user tries to login to the community from the e-commerce site.
- B. Use the e-commerce REST API to create users when a user self-register on the customer community and use SAML to allow SSO.
- C. Use a nightly batch ETL job to sync users between the Customer Community and the e-commerce platform and use SAML to allow SSO.
- D. Use the standard Salesforce API to create users in the Community When a User is Created in the e-Commerce platform and use SAML to allow SSO.

**Answer:** A

**Explanation:**

The best option for UC to create the identities of its e-commerce users with the customer community is to use SAML JIT in the customer community to create users when a user tries to login to the community from the e-commerce site. SAML JIT (Just-in-Time) is a feature that allows Salesforce to create or update user accounts based on the information provided in a SAML assertion from an identity provider (IdP). This feature enables UC to avoid duplicating user registration on both applications and provide a seamless single sign-on (SSO) experience for its customers. The other options are not optimal for this scenario. Using the e-commerce REST API to create users when a user self-registers on the customer community would require the user to register twice, once on the e-commerce site and once on the customer community, which would degrade the customer experience. Using a nightly batch ETL job to sync users between the customer community and the e-commerce platform would introduce a delay in user creation and synchronization, which could cause errors or inconsistencies. Using the standard Salesforce API to create users in the community when a user is created in the e-commerce platform would require UC to write custom code and maintain API integration, which could increase complexity and cost. References: [Just-in-Time Provisioning for SAML], [Single Sign-On], [SAML SSO Flows]

**NEW QUESTION 86**

Northern Trail Outfitters manages application functional permissions centrally as Active Directory groups. The CRM\_SuperUser and CRM\_Reportmg\_SuperUser groups should respectively give the user the SuperUser and Reportmg\_SuperUser permission set in Salesforce. Salesforce is the service provider to a Security Assertion Markup Language (SAML) identity provider. How should an identity architect ensure the Active Directory groups are reflected correctly when a user accesses Salesforce?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 88**

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

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

**Answer:** BC

**Explanation:**

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

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

References:

- Customer 360 Identity
- Customer 360 Identity Benefits

### NEW QUESTION 93

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

What should an identity architect recommend to meet these requirements?

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

**Answer:** C

#### Explanation:

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

### NEW QUESTION 94

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

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

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

**Answer:** BCE

#### Explanation:

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

➤ Username and password + security key: A security key is a physical device that plugs into a USB port or connects wirelessly to your computer or mobile device. It generates a unique code that you use to verify your identity when you log in to Salesforce5.

➤ Third-party single sign-on with Mobile Authenticator app: Single sign-on (SSO) is an authentication method that allows users to access multiple applications with one login and one set of credentials. A mobile authenticator app is an app that generates temporary codes or sends push notifications that you use to verify your identity when you log in to Salesforce via SSO5.

➤ Lightning Login: Lightning Login is an authentication method that allows users to log in to Salesforce without entering a password. Instead, users scan a QR code with their mobile device or click an email link that they receive when they try to log in. Then they use their fingerprint, face ID, or PIN to verify their identity on their mobile device5.

References:

- Multi-Factor Authentication
- Authentication and Verification Methods

### NEW QUESTION 99

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 100

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

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

#### NEW QUESTION 105

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

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

**Answer: D**

#### Explanation:

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

References: Salesforce Identity Connect Implementation Guide, Single Sign-On Implementation Guide

#### NEW QUESTION 106

Containers (UC) has an existing Customer Community. UC wants to expand the self-registration capabilities such that customers receive a different community experience based on the data they provide during the registration process. What is the recommended approach an Architect Should recommend to UC?

- A. Create an After Insert Apex trigger on the user object to assign specific custom permissions.
- B. Create separate login flows corresponding to the different community user personas.
- C. Modify the Community pages to utilize specific fields on the User and Contact records.
- D. Modify the existing Communities registration controller to assign different profiles.

**Answer: C**

#### Explanation:

The recommended approach for UC to expand the self-registration capabilities such that customers receive a different community experience based on the data they provide during the registration process is to modify the community pages to utilize specific fields on the user and contact records. This approach allows UC to customize the community pages based on the user's profile, preferences, interests, or other attributes that are stored in the user or contact fields. For example, UC can use conditional visibility rules or audience criteria to display different components or content based on the user's field values. This approach does not require any code or complex configuration, and it provides a flexible and personalized community experience for different customer segments. The other options are not recommended for this scenario. Creating an after-insert Apex trigger on the user object to assign specific custom permissions would require UC to write code and manage custom permissions, which could increase maintenance and testing efforts. Creating separate login flows corresponding to the different community user personas would require UC to create multiple login pages and logic, which could increase complexity and confusion. Modifying the existing communities' registration controller to assign different profiles would require UC to write code and manage multiple profiles, which could increase security and governance risks. References: [Customize Your Community Pages], [Set Component Visibility], [Create Custom Login Flows], [Customize Self-Registration]

#### NEW QUESTION 110

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

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

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

**Answer: A**

#### Explanation:

To allow employees to sign in to a custom Benefits web app using their Salesforce credentials, the identity architect should recommend the Identity Only License. The Identity Only License is a license type that enables users to access external applications that are integrated with Salesforce using single sign-on (SSO) or delegated authentication, but not access Salesforce objects or data. The other license types are not relevant for this scenario. References: Identity Only License, User Licenses

#### NEW QUESTION 114

An identity architect wants to secure Salesforce APIs using Security Assertion Markup Language (SAML). For security purposes, administrators will need to authorize the applications that will be consuming the APIs.

Which Salesforce OAuth authorization flow should be used?

- A. OAuth 2-0 SAML Bearer Assertion Flow



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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 115**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 119**

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

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

**Answer:** BC

**Explanation:**

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

**NEW QUESTION 121**

Universal Containers (UC) has a classified information system that its call center team uses only when they are working on a case with a record type "Classified". They are only allowed to access the system when they own an open "Classified" case, and their access to the system is removed at all other times. They would like to implement SAML SSO with Salesforce as the IdP, and automatically allow or deny the staff's access to the classified information system based on whether they currently own an open "Classified" case record when they try to access the system using SSO. What is the recommended solution for automatically allowing or denying access to the classified information system based on the open "classified" case record criteria?

- A. Use Salesforce reports to identify users that currently own open "Classified" cases and should be granted access to the Classified information system.
- B. Use Apex trigger on case to dynamically assign permission Sets that Grant access when a user is assigned with an open "Classified" case, and remove it when the case is closed.
- C. Use Custom SAML JIT Provisioning to dynamically query the user's open "Classified" cases when attempting to access the classified information system.
- D. Use a Common Connected App Handler using Apex to dynamically allow access to the system based on whether the staff owns any open "Classified" Cases.

**Answer:** C

**Explanation:**

Custom SAML JIT Provisioning allows Salesforce to dynamically create or update user records in the classified information system based on the SAML assertion sent by Salesforce as the IdP. This way, the staff can access the system only when they have an open "Classified" case, and their access is revoked when they don't. Option A is incorrect because Salesforce reports are not a reliable way to grant or revoke access to the system, as they are not updated in real time and may not reflect the current status of the cases. Option B is incorrect because Apex triggers can only assign or remove permission sets within Salesforce, not in an external system. Option D is incorrect because a Common Connected App Handler using Apex is used to customize the behavior of a connected app, not to control access to an external system based on user attributes. References: Custom SAML JIT Provisioning, Create a Custom Connected App Handler

**NEW QUESTION 122**

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

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



D. Add a banner to the community Home page asking users to update their profile and accept the new community rules.

**Answer:** C

**Explanation:**

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

**NEW QUESTION 126**

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

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

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

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

**Answer:** BD

**Explanation:**

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

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

**NEW QUESTION 127**

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

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

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

**Answer:** AE

**Explanation:**

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

**NEW QUESTION 129**

Universal Container's (UC) identity architect needs to recommend a license type for their new Experience Cloud site that will be used by external partners (delivery providers) for reviewing and updating their accounts, downloading files provided by UC and obtaining scheduled pickup dates from their calendar.

UC is using their Salesforce production org as the identity provider for these users and the expected number of individual users is 2.5 million with 13.5 million unique logins per month.

Which of the following license types should be used to meet the requirement?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 131**

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

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

**Answer:** AC

**Explanation:**

The two OAuth flows that support refresh tokens are Web server and User-Agent. According to the Salesforce documentation<sup>2</sup>, “The web server authentication flow and user-agent flow both provide a refresh token that can be used to get a new access token.” Therefore, option A and C are the correct answers.

References: Salesforce Documentation

**NEW QUESTION 134**

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

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

**Answer:** BD

**Explanation:**

These are the systems that are acting as identity providers (IdPs) in the SSO scenario. An IdP is a trusted provider that enables a customer to use single sign-on (SSO) to access other websites<sup>5</sup>. In this case, Pingfederate and Salesforce Org 1 are the IdPs that authenticate the users and issue SAML assertions or OAuth tokens to the service providers (SPs). The SPs are the websites that host apps and rely on the IdPs for authentication<sup>5</sup>. In this case, Salesforce Org 2, Financial System, and CPQ System are the SPs that receive the SAML assertions or OAuth tokens from the IdPs and grant access to the users.

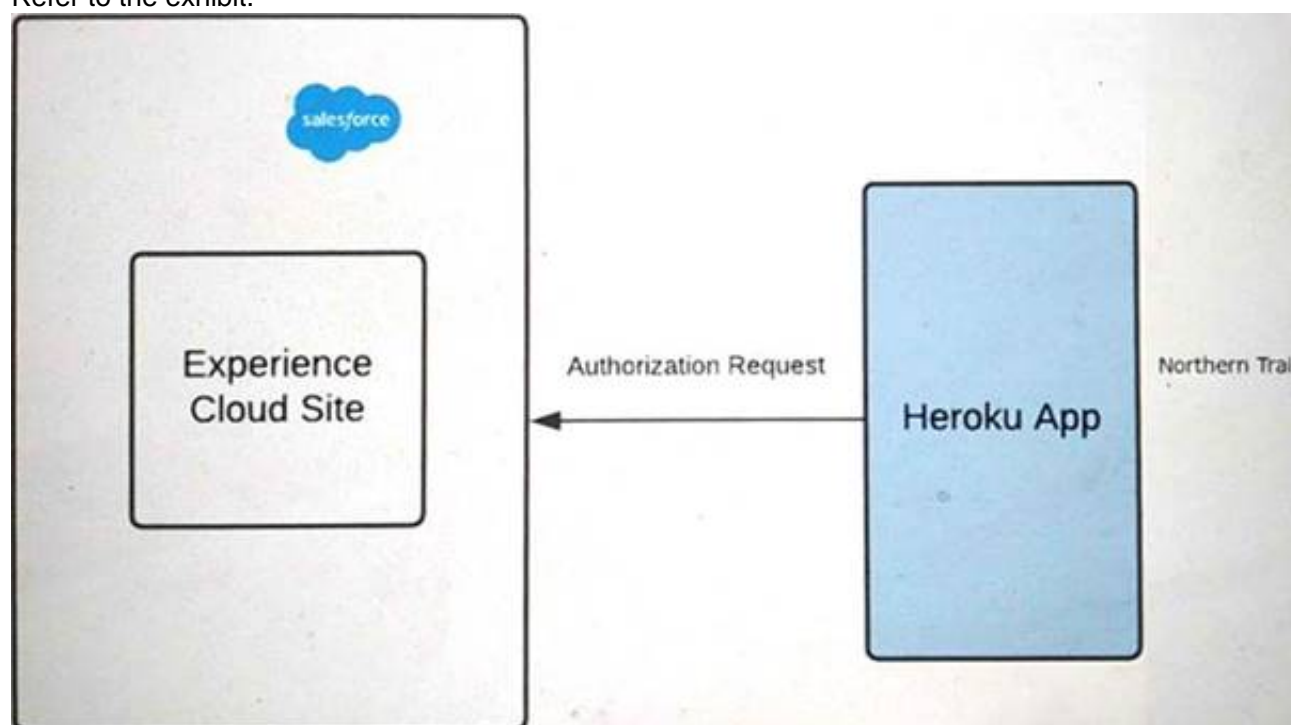
Option A is incorrect because Financial System is not an IdP, but an SP. It does not authenticate the users, but receives SAML assertions from Pingfederate.

Option C is incorrect because Salesforce Org 2 is not an IdP, but an SP. It does not authenticate the users, but receives OAuth tokens from Salesforce Org 1.

References: 5: Identity Providers and Service Providers - Salesforce 6: Salesforce as Service Provider an Identity Provider for SSO

**NEW QUESTION 135**

Refer to the exhibit.



Outfitters (NTO) is using Experience Cloud as an Identity for its application on Heroku. The application on Heroku should be able to handle two brands, Northern Trail Shoes and Northern Trail Shirts.

A user should select either of the two brands in Heroku before logging into the community. The app then performs Authorization using OAuth2.0 with the Salesforce Experience Cloud site.

NTO wants to make sure it renders login page images dynamically based on the user's brand preference selected in Heroku before Authorization.

what should an identity architect do to fulfill the above requirements?

- A. For each brand create different communities and redirect users to the appropriate community using a custom Login controller written in Apex.
- B. Create multiple login screens using Experience Builder and use Login Flows at runtime to route to different login screens.
- C. Authorize third-party service by sending authorization requests to the community-url/services/oauth2/authorize/cookie\_value.
- D. Authorize third-party service by sending authorization requests to thecommunity-url/services/oauth2/authonze/expid\_value.

**Answer:** D

**Explanation:**

OAuth 2.0 is an open standard for authorization that allows a third-party application to obtain limited access to a protected resource on behalf of a user. To authorize a third-party service using OAuth 2.0 with the Salesforce Experience Cloud site, the identity architect should do the following steps:

➤ Create a connected app for the third-party service in Salesforce. A connected app is an application that integrates with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect. To create a connected app, you need to provide the basic information, such as the app name, logo URL, contact email, and API name. You also need to enable OAuth and configure the OAuth settings, such as the callback URL, the scopes, and the policies.

➤ Authorize the third-party service by sending authorization requests to the community-url/services/oauth2/authorize/expid\_value. This is a special endpoint that allows you to specify an experience ID (expid) as a query parameter in the authorization request. The experience ID is a unique identifier for each experience (community or site) in Salesforce. By using this endpoint, you can dynamically render the login page images based on the user's brand preference selected in the third-party service before authorization.

References:

- OAuth 2.0
- OAuth 2.0 Web Server Authentication Flow

- Connected Apps
- Create a Connected App
- Experience ID
- Authorize Apps with OAuth

#### NEW QUESTION 140

Universal Containers (UC) is building a custom employee hut) application on Amazon Web Services (AWS) and would like to store their users' credentials there. Users will also need access to Salesforce for internal operations. UC has tasked an identity architect with evaluating Afferent solutions for authentication and authorization between AWS and Salesforce.

How should an identity architect configure AWS to authenticate and authorize Salesforce users?

- A. Configure the custom employee app as a connected app.
- B. Configure AWS as an OpenID Connect Provider.
- C. Create a custom external authentication provider.
- D. Develop a custom Auth server in AWS.

**Answer: B**

#### Explanation:

To authenticate and authorize Salesforce users with AWS, the identity architect should configure AWS as an OpenID Connect Provider. OpenID Connect is a protocol that allows users to sign in with an external identity provider, such as AWS, 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. The other options are not relevant for this scenario.

References: OpenID Connect Authentication Providers, Social Sign-On with OpenID Connect

#### NEW QUESTION 141

Which two things should be done to ensure end users can only use single sign-on (SSO) to login in to Salesforce?

Choose 2 answers

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

**Answer: AD**

#### Explanation:

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

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

#### NEW QUESTION 143

Universal containers (UC) employees have salesforce access from restricted ip ranges only, to protect against unauthorized access. UC wants to rollout the salesforce1 mobile app and make it accessible from any location.

Which two options should an architect recommend? Choose 2 answers

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

**Answer: AC**

#### Explanation:

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

#### NEW QUESTION 146

Northern Trail Outfitters (NTO) uses a Security Assertion Markup Language (SAML)-based Identity Provider (IdP) to authenticate employees to all systems. The IdP authenticates users against a Lightweight Directory Access Protocol (LDAP) directory and has access to user information. NTO wants to minimize Salesforce license usage since only a small percentage of users need Salesforce.

What is recommended to ensure new employees have immediate access to Salesforce using their current IdP?

- A. Install Salesforce Identity Connect to automatically provision new users in Salesforce the first time they attempt to login.
- B. Build an integration that queries LDAP periodically and creates new active users in Salesforce.
- C. Configure Just-in-Time provisioning using SAML attributes to create new Salesforce users as necessary when a new user attempts to login to Salesforce.
- D. Build an integration that queries LDAP and creates new inactive users in Salesforce and use a login flow to activate the user at first login.



**Answer:** C

**Explanation:**

Just-in-Time (JIT) provisioning is a feature that allows Salesforce to create or update user records on the fly when users log in through an external identity provider, such as a SAML-based IdP. This eliminates the need for manual or batch user provisioning in Salesforce and minimizes license usage. To use JIT provisioning, the identity architect needs to configure the SAML settings in Salesforce and include the user attributes in the SAML assertion sent by the IdP. References: Just-in-Time Provisioning for SAML and OpenID Connect, Identity 101: Design Patterns for Access Management

**NEW QUESTION 150**

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

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

**Answer:** AD

**Explanation:**

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

**NEW QUESTION 151**

What information does the 'Relaystate' parameter contain in sp-Initiated Single Sign-on?

- A. Reference to a URL redirect parameter at the identity provider.
- B. Reference to a URL redirect parameter at the service provider.
- C. Reference to the login address URL of the service provider.
- D. Reference to the login address URL of the identity Provider.

**Answer:** B

**Explanation:**

The 'Relaystate' parameter is an HTTP parameter that can be included as part of the SAML request and SAML response. In an SP-initiated sign-in flow, the SP can set the RelayState parameter in the SAML request with additional information about the request, such as the URL of the resource that the user is trying to access.

The IDP should just relay it back in the SAML response without any modification or inspection. Therefore, the 'Relaystate' parameter contains a reference to a URL redirect parameter at the service provider.

References: 1: single sign on - What is exactly RelayState parameter used in SSO (Ex. SAML)? - Stack

Overflow 2: java - How to send current URL as relay state while sending authentication request to IDP - Stack Overflow 3: Understanding SAML | Okta Developer

**NEW QUESTION 154**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 158**

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

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

**Answer:** A

**Explanation:**

To generate sensor information in Salesforce, the architect should recommend OAuth 2.0 Asset Token Flow. OAuth 2.0 Asset Token Flow is a protocol that allows devices, such as sensors, to obtain an access token from Salesforce by using a certificate instead of an authorization code. The access token can be used to



access Salesforce APIs and send data to Salesforce. OAuth 2.0 Asset Token Flow is designed for devices that do not have a user interface or a web browser.  
References: OAuth 2.0 Asset Token Flow, Authorize Apps with OAuth

#### NEW QUESTION 161

Universal Containers (UC) wants to build a few applications that leverage the Salesforce REST API. UC has asked its Architect to describe how the API calls will be authenticated to a specific user. Which two mechanisms can the Architect provide? Choose 2 Answers

- A. Authentication Token
- B. Session ID
- C. Refresh Token
- D. Access Token

**Answer:** CD

#### Explanation:

These are the mechanisms that the Salesforce REST API uses for authentication. According to the Salesforce documentation<sup>1</sup>, the REST API requires an access token obtained by authentication. The access token is a session credential that represents the authorization of a specific application to access specific parts of a user's data<sup>2</sup>. The access token is valid for a limited time and can be refreshed using a refresh token. A refresh token is a credential that represents the authorization of an application to refresh an expired access token<sup>2</sup>.

Option A is incorrect because an authentication token is not used by the Salesforce REST API. An authentication token is an email security feature that appends a unique string of characters to your password when you log in from an unrecognized device or IP address<sup>3</sup>. Option B is incorrect because a session ID is not used by the Salesforce REST API. A session ID is a unique identifier for a user's session that can be used for SOAP API calls<sup>4</sup>.

References: 1: Step Two: Set Up Authentication | REST API Developer Guide | Salesforce Developers 2: Salesforce REST APIs with Heroku - Trailhead 3: Authentication Token - Salesforce 4: Session ID - Salesforce

#### NEW QUESTION 166

Northern Trail Outfitters (NTO) is planning to roll out a partner portal for its distributors using Experience Cloud. NTO would like to use an external identity provider (IdP) and for partners to register for access to the portal. Each partner should be allowed to register only once to avoid duplicate accounts with Salesforce. What should a identity architect recommend to create partners?

- A. On successful creation of Partners using Self Registration page in Experience Cloud, create identity in Ping.
- B. Create a custom page in Experience Cloud to self register partner with Experience Cloud and Ping identity store.
- C. Create a custom web page in the Portal and create users in the IdP and Experience Cloud using published APIs.
- D. Allow partners to register through the IdP and create partner users in Salesforce through an API.

**Answer:** B

#### Explanation:

To create partners using an external identity provider (IdP) and avoid duplicate accounts with Salesforce, the identity architect should recommend creating a custom page in Experience Cloud to self register partner with Experience Cloud and Ping identity store. Ping is an IdP that supports OpenID Connect protocol, which allows users to sign in with an external identity provider and access Salesforce resources. By creating a custom page in Experience Cloud, the identity architect can use a custom registration handler to link the partner's Ping identity with their Salesforce identity and prevent duplicate accounts. The custom page can also provide a seamless user experience for the partners. References: OpenID Connect Authentication Providers, Social Sign-On with OpenID Connect, Create a Custom Registration Handler

#### NEW QUESTION 170

.....

## 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/>