



Salesforce

Exam Questions Identity-and-Access-Management-Architect

Salesforce Certified Identity and Access Management Architect (SU23)

NEW QUESTION 1

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 2

A Salesforce customer is implementing Sales Cloud and a custom pricing application for its call center agents. An Enterprise single sign-on solution is used to authenticate and sign-in users to all applications. The customer has the following requirements:

* 1. The development team has decided to use a Canvas app to expose the pricing application to agents.

* 2. Agents should be able to access the Canvas app without needing to log in to the pricing application.

Which two options should the identity architect consider to provide support for the Canvas app to initiate login for users?

Choose 2 answers

- A. Select "Enable as a Canvas Personal App" in the connected app settings.
- B. Enable OAuth settings in the connected app with required OAuth scopes for the pricing application.
- C. Configure the Canvas app as a connected app and set Admin-approved users as pre-authorized.
- D. Enable SAML in the connected app and Security Assertion Markup Language (SAML) Initiation Method as Service Provider Initiated.

Answer: CD

Explanation:

To allow agents to access the Canvas app without needing to log in to the pricing application, the identity architect should consider two options:

➤ Configure the Canvas app as a connected app and set Admin-approved users as pre-authorized. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols. A Canvas app is a type of connected app that allows an external application to be embedded within Salesforce. By setting Admin-approved users as pre-authorized, the identity architect can control which users can access the Canvas app by assigning profiles or permission sets to the connected app.

➤ Enable SAML in the connected app and Security Assertion Markup Language (SAML) Initiation Method as Service Provider Initiated. SAML is a protocol that allows users to authenticate and authorize with an external identity provider and access Salesforce resources. By enabling SAML in the connected app, the identity architect can use Salesforce as a service provider (SP) and the pricing application as an identity provider (IdP) for single sign-on (SSO). By setting SAML Initiation Method as Service Provider Initiated, the identity architect can initiate the SSO process from Salesforce and send a SAML request to the pricing application.

References: Connected Apps, Canvas Apps, SAML Single Sign-On Settings

NEW QUESTION 3

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

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

Answer: BC

Explanation:

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

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

NEW QUESTION 4

Northern Trail Outfitters (NTO) has an off-boarding process where a terminated employee is first disabled in the Lightweight Directory Act Protocol (LDAP) directory, then requests are sent to the various application support teams to finish user deactivations. A terminated employee recently was able to login to NTO's Salesforce instance 24 hours after termination, even though the user was disabled in the corporate LDAP directory.

What should an identity architect recommend to prevent this from happening in the future?

- A. Create a Just-in-Time provisioning registration handler to ensure users are deactivated in Salesforce as they are disabled in LDAP.
- B. Configure an authentication provider to delegate authentication to the LDAP directory.
- C. use a login flow to make a callout to the LDAP directory before authenticating the user to Salesforce.
- D. Setup an identity provider (IdP) to authenticate users using LDAP, set up single sign-on to Salesforce and disable Login Form authentication.

Answer: B

Explanation:

Login History allows administrators to view the login attempts of all users in the org, including the status, source IP, login type, and application. This can help identify and troubleshoot any login errors or issues. References: Login History

NEW QUESTION 5

Universal Containers wants Salesforce inbound OAuth-enabled integration clients to use SAML-BASED single Sign-on for authentication. What OAuth flow would be recommended in this scenario?

- A. User-Agent OAuth flow
- B. SAML assertion OAuth flow
- C. User-Token OAuth flow
- D. Web server OAuth flow

Answer: B

Explanation:

The SAML assertion OAuth flow allows a connected app to use a SAML assertion to request an OAuth access token to call Salesforce APIs. This flow provides an alternative for orgs that are currently using SAML to access Salesforce and want to access the web services API in the same way³. This flow can be used for inbound OAuth-enabled integration clients that want to use SAML-based single sign-on for authentication.

References: OAuth 2.0 SAML Bearer Assertion Flow for Previously Authorized Apps, Access Data with AP Integration, Error 'Invalid assertion' in OAuth 2.0 SAML Bearer Flow

NEW QUESTION 6

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

- * 1. User Authenticates and Authorizes Access
- * 2. Request an Access Token
- * 3. Salesforce Grants an Access Token
- * 4. Request an Authorization Code
- * 5. Salesforce Grants Authorization Code

What is the correct sequence for the authorization flow?

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

Answer: B

Explanation:

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

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

NEW QUESTION 7

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 8

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

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

Answer: BC

Explanation:

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

➤ App Launcher is a feature that lets you access all your connected apps from one place in Salesforce. It does not require My Domain or SAML SSO to work, although it can be enhanced by using them.

➤ Login Forensics is a feature that analyzes login behavior and identifies anomalous or suspicious logins. It does not require My Domain or SAML SSO to work, although it can be used with them.

References: My Domain, Deep Linking into Salesforce, Salesforce Mobile App Basics, [App Launc [Login Forensics]

NEW QUESTION 9

Universal Containers (UC) uses Salesforce as a CRM and identity provider (IdP) for their Sales Team to seamlessly login to internaJ portals. The IT team at UC is now evaluating Salesforce to act as an IdP for its remaining employees.

Which Salesforce license is required to fulfill this requirement?

- A. External Identity
- B. Identity Verification
- C. Identity Connect
- D. Identity Only

Answer: D

Explanation:

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

NEW QUESTION 10

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

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

Answer: CD

Explanation:

Two-way SSL is a method of mutual authentication between two parties using digital certificates. A digital certificate is an electronic document that contains information about the identity of the certificate owner and a public key that can be used to verify their signature. A digital certificate can be either self-signed or CA-signed. A self-signed certificate is created and signed by its owner, while a CA-signed certificate is created by its owner but signed by a trusted Certificate Authority (CA). For setting up two-way SSL between Salesforce and an external system, two valid choices for digital certificates are:

➤ Use a self-signed certificate for Salesforce and a self-signed certificate for the external system. This option is simple and cost-effective, but requires both parties to trust each other's self-signed certificates explicitly.

➤ Use a self-signed certificate for Salesforce and a trusted CA-signed certificate for the external system.

This option is more secure and reliable, but requires Salesforce to trust the CA that signed the external system's certificate implicitly.

References: Know more about all the SSL certificates that are supported by Salesforce, two way ssl. How to

NEW QUESTION 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 15

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 messages¹. The identity provider uses the Entity ID to determine which service provider is requesting or receiving authentication information². You can customize the Entity ID for your Salesforce org or Experience Cloud site in the SAML Single Sign-On Settings page³. References: 1: SAML SSO Flows 2: Federated Authentication Using SAML to Log in to Salesforce Org 3: Step 2: Create a SA Single Sign-On Setting in Salesforce

NEW QUESTION 16

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

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

Answer: A

Explanation:

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

NEW QUESTION 18

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

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 19

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

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

Answer: C

Explanation:

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

References: Just-in-Time Provisioning for SAML, [Just-in-Time Deprovisioning], [SOAP API Developer

NEW QUESTION 24

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 28

Which tool should be used to track login data, such as the average number of logins, who logged in more than the average number of times and who logged in during non-business hours?

- A. Login Inspector
- B. Login History
- C. Login Report
- D. Login Forensics

Answer: D

Explanation:

To track login data, such as the average number of logins, who logged in more than the average number of times and who logged in during non-business hours, the identity architect should use Login Forensics. Login Forensics is a tool that analyzes login data and provides insights into user behavior and login patterns. Login Forensics can help identify anomalies, risks, and trends in user login activity. Login Forensics can also generate reports and dashboards to visualize the login data. References: Login Forensics, Analyze Login Data with Login Forensics

NEW QUESTION 32

What are three capabilities of Delegated Authentication? Choose 3 answers

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

Answer: BCE

Explanation:

The three capabilities of delegated authentication are:

➤ It can connect to SOAP services. Delegated authentication is a feature that allows Salesforce to delegate the authentication process to an external service by making a SOAP callout to a web service that verifies the user's credentials. This feature enables Salesforce to integrate with existing identity stores or authentication methods that support SOAP services.

➤ It can be assigned by permission sets. Permission sets are collections of settings and permissions that give users access to various tools and functions in Salesforce. Permission sets can be used to assign delegated authentication to users by enabling the "Is Single Sign-on Enabled" permission. This permission allows users to log in with delegated authentication instead of their Salesforce username and password.

➤ It can connect to REST services. REST services are web services that use HTTP methods to access or manipulate resources on a server. REST services can be used for delegated authentication by creating a custom login page that makes a REST callout to an external service that verifies the user's credentials. This approach requires custom code and configuration, but it provides more flexibility and control over the authentication process.

The other options are not capabilities of delegated authentication. Delegated authentication cannot be assigned by custom permissions or profiles. Custom permissions are settings that can be used in Apex code or validation rules to check whether a user has access to a custom feature or functionality. Custom permissions cannot be used to enable delegated authentication for users. Profiles are collections of settings and permissions that determine what users can do in Salesforce. Profiles cannot be used to enable delegated authentication for users, as this feature is controlled by permission sets. References: [Delegated Authentication], [Permission Sets], [Enable 'Delegated Authentication'], [REST Services], [Custom Login Page for Delegated Authentication], [Custom Permissions], [Profiles]

NEW QUESTION 34

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 37

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

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

Answer: C

Explanation:

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

NEW QUESTION 42

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

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

Answer: A

Explanation:

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

NEW QUESTION 43

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

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

Answer: C

Explanation:

The role of Active Directory in this scenario is an identity provider. An identity provider is an application that authenticates users and provides information about them to service providers⁶. A service provider is an application that provides a service to users and relies on an identity provider for authentication⁶. In this scenario, the employee portal is a service provider that provides collaboration features to employees and relies on Active Directory for authentication. Active Directory is an identity provider that authenticates employees using their corporate credentials and sends information about them to the employee portal⁷.
References: Identity Provider Overview, Configure SSO to Salesforce Using Microsoft AD FS as the Identity Provider

NEW QUESTION 45

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

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

Answer: D

Explanation:

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

NEW QUESTION 46

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

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

Answer: B

Explanation:

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

NEW QUESTION 48

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 50

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

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

Answer: BD

Explanation:

The two statements that are capabilities of Identity Connect are:

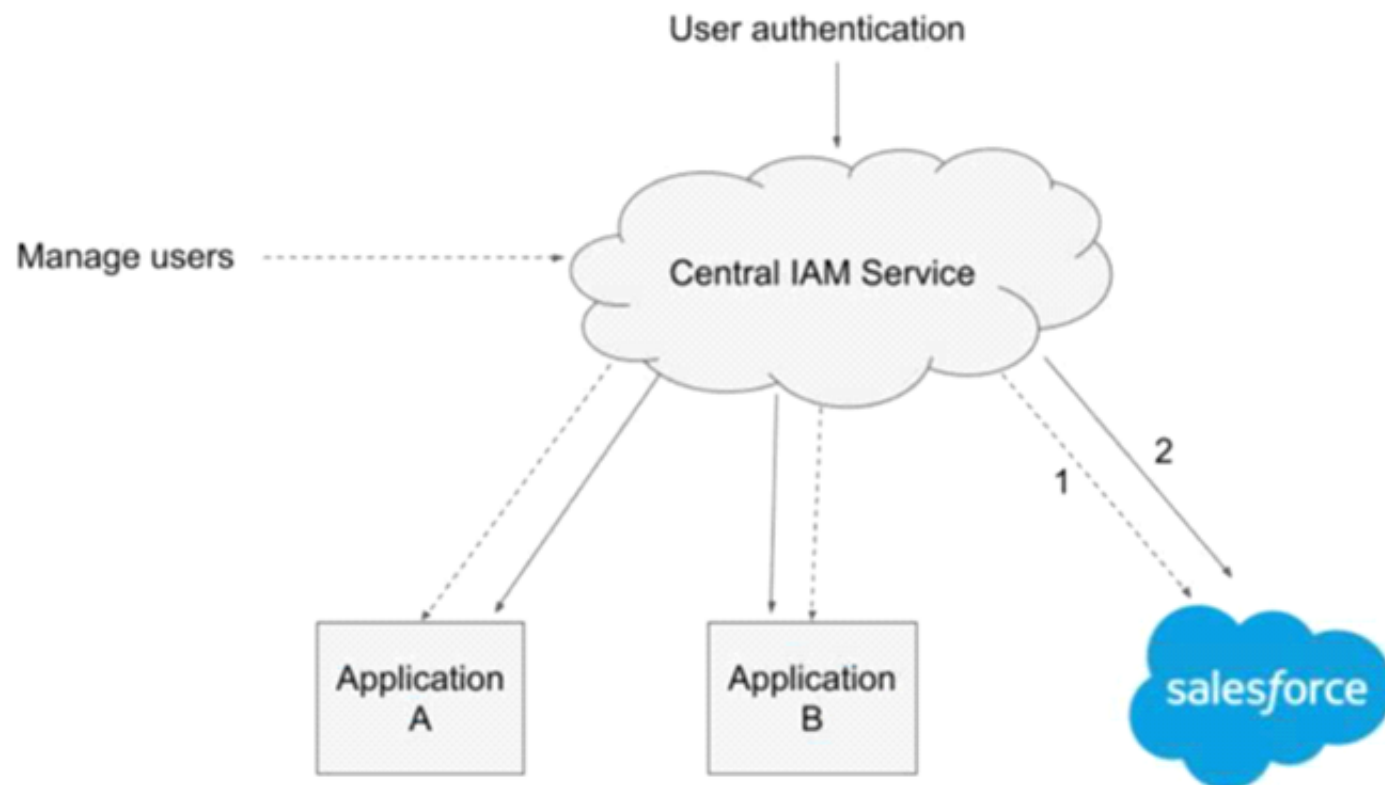
➤ It supports both identity-provider-initiated and service-provider-initiated SSO. Identity Connect is a desktop application that integrates Salesforce with Microsoft Active Directory (AD) and enables single sign-on (SSO) between the two systems. Identity Connect supports both identity-provider-initiated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

➤ It enables automated user synchronization and deactivation. Identity Connect allows administrators to synchronize user accounts and attributes between AD and Salesforce, either manually or on a scheduled basis. Identity Connect also allows administrators to deactivate user accounts in Salesforce when they are disabled or deleted in AD, which helps maintain security and compliance.

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

NEW QUESTION 51

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 52

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

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

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

Answer: AB

Explanation:

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

NEW QUESTION 53

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

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

Answer: AD

Explanation:

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

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

data to log in to Salesforce.

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

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

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

NEW QUESTION 54

Universal Containers (UC) is using Active Directory as its corporate identity provider and Salesforce as its CRM for customer care agents, who use SAML based sign sign-on to login to Salesforce. The default agent profile does not include the Manage User permission. UC wants to dynamically update the agent role and permission sets.

Which two mechanisms are used to provision agents with the appropriate permissions? Choose 2 answers

- A. Use Login Flow in User Context to update role and permission sets.
- B. Use Login Flow in System Context to update role and permission sets.
- C. Use SAML Just-m-Time (JIT) Handler class run as current user to update role and permission sets.
- D. Use SAML Just-in-Time (JIT) handler class run as an admin user to update role and permission sets.

Answer: BD

Explanation:

To dynamically update the agent role and permission sets using Active Directory as the corporate identity provider and Salesforce as the CRM for customer care agents, who use SAML based sign-on to login to Salesforce, the identity architect should use two mechanisms:

➤ Use Login Flow in System Context to update role and permission sets. A Login Flow is a custom post-authentication process that can be used to add additional screens or logic after a user logs in to Salesforce. A System Context is a mode that allows a Login Flow to run as an administrator user with full access to Salesforce data and metadata. By using a Login Flow in System Context, the identity architect can update the agent role and permission sets based on the information from Active Directory or other criteria.

➤ Use SAML Just-in-Time (JIT) handler class run as an admin user to update role and permission sets. A SAML JIT handler class is a class that implements the Auth.SamlJitHandler interface and defines how to handle SAML assertions for Just-in-Time (JIT) provisioning. JIT provisioning is a feature that allows Salesforce to create or update user records on the fly when users log in through an external identity provider. By using a SAML JIT handler class run as an admin user, the identity architect can update the agent role and permission sets based on the information from the SAML assertion. References: Login Flows, SAML Just-in-Time Provisioning, Auth.SamlJitHandler Interface

NEW QUESTION 55

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 56

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 61

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.

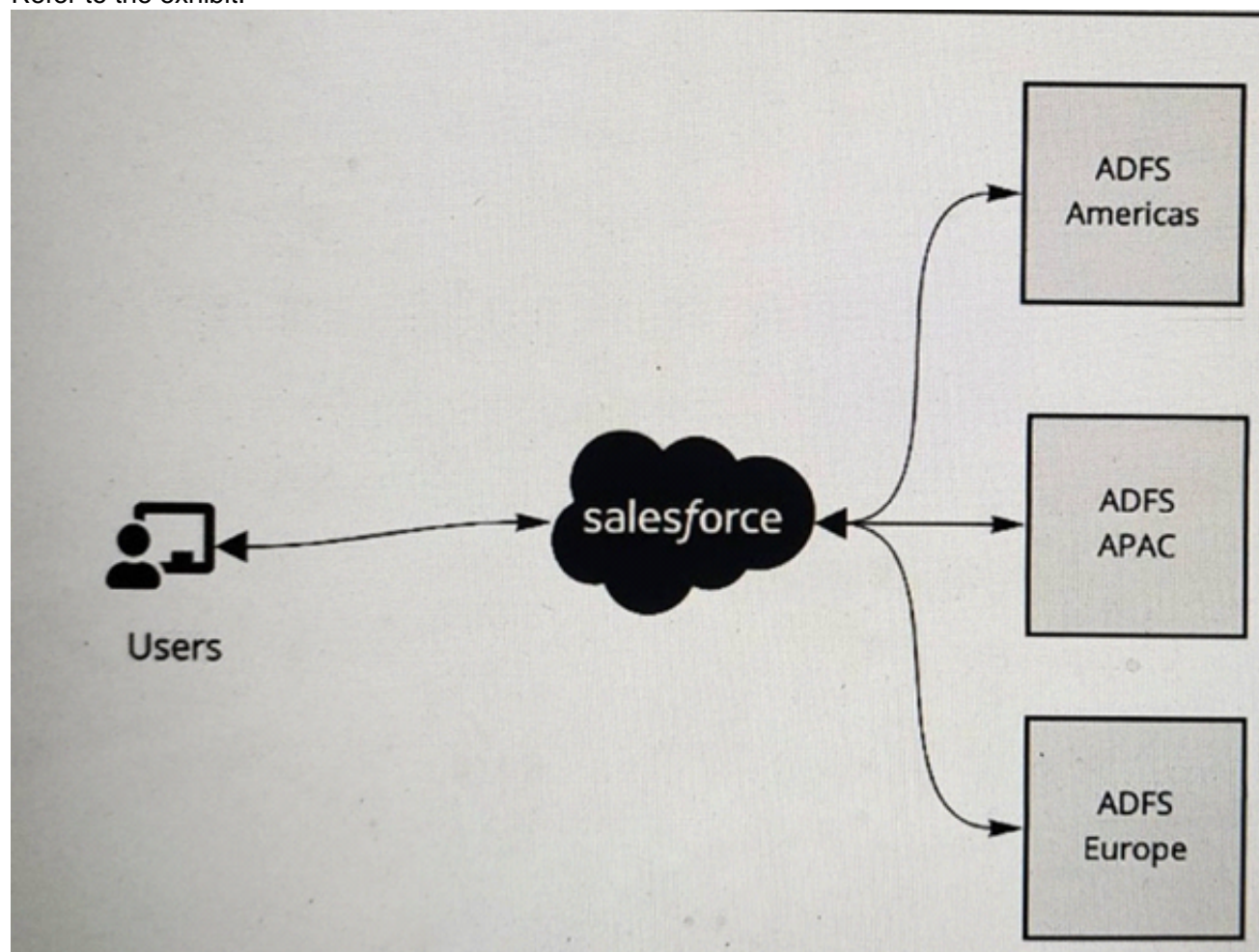
B is incorrect because Salesforce is not a connected app for the SSO. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect1. The Employee portal does not use any of these protocols to 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 63

Refer to the exhibit.



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

What is recommended to ensure these requirements are met ?

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

Answer: B

Explanation:

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

NEW QUESTION 68

Universal Containers (UC) has built a custom time tracking app for its employee. UC wants to leverage Salesforce Identity to control access to the custom app. At a minimum, which Salesforce license is required to support this requirement?

- A. Identity Verification
- B. Identity Connect
- C. Identity Only
- D. External Identity

Answer: C

Explanation:

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

NEW QUESTION 69

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

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

Answer: A

Explanation:

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

NEW QUESTION 73

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 75

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

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

Answer: B

Explanation:

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

NEW QUESTION 76

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

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 79

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

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

Answer: AD

Explanation:

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

- Option A is correct because configuring SAML SSO settings involves specifying the identity provider details, such as the entity ID, login URL, logout URL, and certificate².
- Option D is correct because setting up My Domain enables you to use a custom domain name for your Salesforce org and allows you to use SAML as an authentication method³.
- Option B is incorrect because creating a connected app is not necessary for SP-initiated SSO using a SAML-compliant IdP. A connected app is used for OAuth-based authentication or OpenID Connect-based authentication⁴.
- Option C is incorrect because configuring delegated authentication is not related to SP-initiated SSO using a SAML-compliant IdP. Delegated authentication is a feature that allows Salesforce to delegate user authentication to an external service, such as LDAP or Active Directory⁵.

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

NEW QUESTION 83

Universal Containers (UC) rolling out a new Customer Identity and Access Management Solution will be built on top of their existing Salesforce instance.

Several service providers have been setup and integrated with Salesforce using OpenID Connect to allow for a seamless single sign-on experience. UC has a requirement to limit user access to only a subset of service providers per customer type.

Which two steps should be done on the platform to satisfy the requirement? Choose 2 answers

- A. Manage which connected apps a user has access to by assigning authentication providers to the user's profile.
- B. Assign the connected app to the customer community, and enable the users profile in the Community settings.
- C. Use Profiles and Permission Sets to assign user access to Admin Pre-Approved Connected Apps.
- D. Set each of the Connected App access settings to Admin Pre-Approved.

Answer: CD

Explanation:

To limit user access to only a subset of service providers per customer type, the identity architect should use Profiles and Permission Sets to assign user access to Admin Pre-Approved Connected Apps. Connected apps are frameworks that enable external applications to integrate with Salesforce using APIs and standard protocols, such as OpenID Connect. By setting each of the Connected App access settings to Admin Pre-Approved, the identity architect can control which users can access which connected apps by assigning profiles or permission sets to the connected apps. The other options are not relevant for this scenario. References: Connected Apps, Manage Connected Apps

NEW QUESTION 84

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

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

Answer: CD

Explanation:

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

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

NEW QUESTION 86

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 87

Universal Containers (UC) uses Active Directory (AD) as their identity store for employees and must continue to do so for network access. UC is undergoing a major transformation program and moving all of their enterprise applications to cloud platforms including Salesforce, Workday, and SAP HANA. UC needs to implement an SSO solution for accessing all of the third-party cloud applications and the CIO is inclined to use Salesforce for all of their identity and access management needs.

Which two Salesforce license types does UC need for its employees' Choose 2 answers

- A. Company Community and Identity licenses
- B. Identity and Identity Connect licenses
- C. Chatter Only and Identity licenses
- D. Salesforce and Identity Connect licenses

Answer: BD

Explanation:

The two Salesforce license types that UC needs for its employees are Identity and Identity Connect licenses. According to the Salesforce documentation, "Identity licenses let your employees access any app that supports standards-based single sign-on (SSO). Identity Connect licenses let you integrate your Active Directory with Salesforce." Therefore, option B and D are the correct answers. References: [Identity Licenses]

NEW QUESTION 91

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 95

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

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

E. Permission sets assignment

Answer: ACE

Explanation:

AD groups can control public group assignment, role assignment, and permission set assignment through Identity Connect. Identity Connect is a tool that integrates Microsoft Active Directory (AD) user accounts with Salesforce user records¹. It allows Salesforce admins to leverage the existing user data and group memberships in AD to automate user provisioning and deprovisioning in Salesforce. Identity Connect can map AD groups to Salesforce public groups, roles, and permission sets, and assign them to users based on their group membership². This way, AD groups can control the access level and visibility of users in Salesforce. AD groups cannot control granting report folder access or custom permission assignment through Identity Connect. These are not supported features of Identity Connect. Report folder access is controlled by the folder sharing settings in Salesforce. Custom permission assignment is controlled by the custom permission settings in Salesforce. References: Get to Know Identity Connect, Map Your Data, [Folder Sharing], [Custom Permissions]

NEW QUESTION 100

Northern Trail Outfitters (NTO) is launching a new sportswear brand on its existing consumer portal built on Salesforce Experience Cloud. As part of the launch, emails with promotional links will be sent to existing customers to log in and claim a discount. The marketing manager would like the portal dynamically branded so that users will be directed to the brand link they clicked on; otherwise, users will view a recognizable NTO-branded page.

The campaign is launching quickly, so there is no time to procure any additional licenses. However, the development team is available to apply any required changes to the portal.

Which approach should the identity architect recommend?

- A. Create a full sandbox to replicate the portal site and update the branding accordingly.
- B. Implement Experience ID in the code and extend the URLs and endpoints, as required.
- C. Use Heroku to build the new brand site and embedded login to reuse identities.
- D. Configure an additional community site on the same org that is dedicated for the new brand.

Answer: B

Explanation:

To dynamically brand the portal so that users will be directed to the brand link they clicked on, the identity architect should recommend implementing Experience ID in the code and extending the URLs and endpoints, as required. Experience ID is a parameter that can be used to identify different brands or experiences within a single Experience Cloud site (formerly known as Community). Dynamic branding is a feature that allows Experience Cloud sites to display different branding elements, such as logos, colors, or images, based on the Experience ID or other criteria. By implementing Experience ID in the code, the identity architect can provide a consistent and personalized brand experience for each user without creating multiple sites or sandboxes. References: Experience ID, Dynamic Branding for Experience Cloud Sites

NEW QUESTION 104

Northern Trail Outfitters (NTO) has a number of employees who do NOT need access Salesforce objects. These 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 107

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

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

Answer: BC

Explanation:

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

NEW QUESTION 108

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 111

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 116

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 121

Users logging into Salesforce are frequently prompted to verify their identity.

The identity architect is required to provide recommendations so that frequency of prompt verification can be reduced.

What should the identity architect recommend to meet the requirement?

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

Answer: B

Explanation:

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

NEW QUESTION 124

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 129

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 131

Universal Containers (UC) has implemented SAML-based SSO solution for use with their multi-org Salesforce implementation, utilizing one of the the orgs as the Identity Provider. One user is reporting that they can log in to the Identity Provider org but get a generic SAML error message when accessing the other orgs.

Which two considerations should the architect review to troubleshoot the issue? Choose 2 answers

- A. The Federation ID must be a valid Salesforce Username
- B. The Federation ID must is case sensitive
- C. The Federation ID must be in the form of an email address.
- D. The Federation ID must be populated on the user record.

Answer: BD

Explanation:

The Federation ID is a field on the user object that is used to link a Salesforce user with an external identity provider. When using SAML SSO, Salesforce matches the Federation ID value with the NameID element in the SAML assertion to identify the user. To troubleshoot the issue of getting a generic SAML error message when accessing the other orgs, the architect should review the following considerations:

- The Federation ID must be case sensitive, which means that the value in the user record must match exactly with the value in the SAML assertion. For example, if the Federation ID is "John.Doe", then "john.doe" or "JOHN.DOE" will not work.
- The Federation ID must be populated on the user record, which means that the user must have a value for this field in each org that they want to access via SSO. If the Federation ID is blank or missing, then Salesforce will not be able to match the user with the SAML assertion.

NEW QUESTION 135

Universal Containers (UC) is building an integration between Salesforce and a legacy web application using the canvas framework. The security for UC has determined that a signed request from Salesforce is not an adequate authentication solution for the Third-Party app. Which two options should the Architect consider for authenticating the third-party app using the canvas framework? Choose 2 Answers

- A. Utilize the SAML Single Sign-on flow to allow the third-party to authenticate itself against UC's IdP.
- B. Utilize Authorization Providers to allow the third-party application to authenticate itself against Salesforce as the Idp.
- C. Utilize Canvas OAuth flow to allow the third-party application to authenticate itself against Salesforce as the Idp.
- D. Create a registration handler Apex class to allow the third-party application to authenticate itself against Salesforce as the Idp.

Answer: AC

Explanation:

The Canvas framework supports OAuth 2.0 for authorization1. There are two OAuth flows that can be used to authenticate the third-party app using the canvas framework: User-Agent OAuth Flow and Web Server OAuth Flow2. The User-Agent OAuth Flow uses the Canvas JavaScript SDK to obtain an OAuth token by using the login function in the SDK2. The Web Server OAuth Flow redirects the user to the Salesforce OAuth authorization endpoint and then obtains an OAuth access token by making a POST request to the Salesforce OAuth token endpoint2. Both of these flows allow the third-party app to authenticate itself against Salesforce as the IdP. The SAML Single Sign-on flow can also be used to allow the third-party app to authenticate itself against UC's IdP, which is another option for authentication3.

References: OAuth Authorization, Mastering Salesforce Canvas Apps, Integrate third-party applications vi Canvas App

NEW QUESTION 140

Northern Trail Outfitters (NTO) recently purchased Salesforce Identity Connect to streamline user provisioning across Microsoft Active Directory (AD) and Salesforce Sales Cloud.

NTO has asked an identity architect to identify which salesforce security configurations can map to AD permissions.

Which three Salesforce permissions are available to map to AD permissions? Choose 3 answers

- A. Public Groups
- B. Field-Level Security
- C. Roles
- D. Sharing Rules
- E. Profiles and Permission Sets

Answer: ACE

Explanation:

Salesforce Identity Connect can map AD groups to Salesforce public groups, roles, profiles, and permission sets. These permissions control the access and visibility of data and features in Salesforce. References: Salesforce Identity Connect Implementation Guide

NEW QUESTION 142

When designing a multi-branded Customer Identity and Access Management solution on the Salesforce Platform, how should an identity architect ensure a specific brand experience in Salesforce is presented?

- A. The Experience ID, which can be included in OAuth/Open ID flows and Security Assertion Markup Language (SAML) flows as a URL parameter.
- B. Provide a brand picker that the end user can use to select its sub-brand when they arrive on salesforce.
- C. Add a custom parameter to the service provider's OAuth/SAML call and implement logic on its login page to apply branding based on the parameters value.
- D. The Audience ID, which can be set in a shared cookie.

Answer: A

Explanation:

Configuring an authentication provider to delegate authentication to the LDAP directory ensures that users can only log in to Salesforce if they are active in the LDAP directory. This prevents terminated employees from accessing Salesforce with their old credentials. References: Authentication Providers, Delegated Authentication Single Sign-On

NEW QUESTION 143

Which three types of attacks would a 2-Factor Authentication solution help garden against?

- A. Key logging attacks
- B. Network perimeter attacks
- C. Phishing attacks
- D. Dictionary attacks
- E. Man-in-the-middle attacks

Answer: ACDE

Explanation:

A 2-Factor Authentication (2FA) solution is a type of multi-factor authentication (MFA) that requires users to provide two verification factors to access a system or application. The verification factors can be something the user knows (e.g., password), something the user has (e.g., phone), or something the user is (e.g., fingerprint). A 2FA solution can help prevent common cyberattacks that rely on stealing or guessing passwords, such as:

- Key logging attacks: These are attacks where a malicious program records the keystrokes of a user, including their passwords, and sends them to the attacker. A 2FA solution can prevent this attack by requiring an additional factor that is not typed by the user, such as a verification code sent to their phone or a biometric scan.
- Phishing attacks: These are attacks where an attacker sends a fake email or website that looks like it came from a trusted source, and tricks the user into providing their credentials or other sensitive information. A 2FA solution can prevent this attack by requiring an additional factor that is not known by the attacker, such as a verification code generated by an authenticator app or a hardware token.
- Dictionary attacks: These are attacks where an attacker tries to guess a user's password by using a list of common or likely passwords, such as "password" or "123456". A 2FA solution can prevent this attack by requiring an additional factor that is not based on a password, such as a fingerprint scan or a facial recognition.
- A man-in-the-middle attack is when an attacker intercepts and alters the communication between two parties, such as a user and a website. A 2-Factor Authentication solution can help prevent this type of attack by requiring a second factor of authentication that the attacker cannot access or spoof, such as a code sent to the user's phone or a hardware token

References: 1: What Is Two-Factor Authentication (2FA)? | Microsoft Security 2: What type of attacks doe Multi-Factor Authentication prevent?

NEW QUESTION 147

Universal Containers (UC) has decided to replace the homegrown customer portal with Salesforce Experience Cloud. UC will continue to use its third-party single sign-on (SSO) solution that stores all of its customer and partner credentials.

The first time a customer logs in to the Experience Cloud site through SSO, a user record needs to be created automatically.

Which solution should an identity architect recommend in order to automatically provision users in Salesforce upon login?

- A. Just-in-Time (JIT) provisioning
- B. Custom middleware and web services
- C. Custom login flow and Apex handler
- D. Third-party AppExchange solution

Answer: A

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. This eliminates the need for manual or batch user provisioning in Salesforce. References: Just-in-Time Provisioning for SAML and OpenID Connect, Identity 101: Design Patterns for Access Management

NEW QUESTION 152

Universal Containers (UC) built an integration for their employees to post, view, and vote for ideas in Salesforce from an internal Company portal. When ideas are posted in Salesforce, links to the ideas are created in the company portal pages as part of the integration process. The Company portal connects to Salesforce using OAuth. Everything is working fine, except when users click on links to existing ideas, they are always taken to the Ideas home page rather than the specific idea, after authorization. Which OAuth URL parameter can be used to retain the original requested page so that a user can be redirected correctly after OAuth authorization?

- A. Redirect_uri
- B. State
- C. Scope
- D. Callback_uri

Answer: A

Explanation:

Threedirect_uri parameter is used to specify the URL that the user should be redirected to after OAuth authorization1. The redirect_uri should match the one that was registered with the OAuth client application2. By using the redirect_uri parameter, the user can be redirected to the original requested page instead of the Ideas home page.

NEW QUESTION 154

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

- A. Use the updateUser method on the registration Handler Class.
- B. Develop a scheduled job that calls out to Facebook on a nightly basis.
- C. Use information in the signed Request that is received from facebook.
- D. Use SAML Just-In-Time Provisioning between Facebook and Salesforce.

Answer: A

Explanation:

The best option for UC to ensure that changes in the Facebook profile are reflected on the appropriate customer community user is to use the updateUser method on the registration handler class. A registration handler class is an Apex class that implements the Auth.RegistrationHandler interface and defines the logic for creating or updating a user account when a user logs in with an external authentication provider, such as Facebook. The updateUser method is a method in the registration handler class that takes a user ID and a JSON string as parameters and updates the user record with the information from the JSON string. This method can be used to update the user's profile, email, name, or other attributes based on the changes in the Facebook profile. The other options are not optimal for this scenario. Developing a scheduled job that calls out to Facebook on a nightly basis would introduce a delay in updating the user information and require custom code and API integration. Using information in the signed request that is received from Facebook would only provide limited information about the user, such as name, email, and locale, and not reflect any changes made after the initial login. Using SAML Just-in-Time provisioning between Facebook and Salesforce would require UC to configure Facebook as a SAML identity provider, which is not supported by Facebook. References: [Create a Registration Handler Class], [Auth.RegistrationHandler Interface], [Facebook Signed Request], [Facebook as SAML Identity Provider]

NEW QUESTION 155

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 m 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 158

Containers (UC) has decided to implement a federated single Sign-on solution using a third-party Idp. In reviewing the third-party products, they would like to ensure the product supports the automated provisioning and deprovisioning of users. What are the underlining mechanisms that the UC Architect must ensure are part of the product?

- A. SOAP API for provisioning; Just-in-Time (JIT) for Deprovisioning.
- B. Just-In-time (JIT) for Provisioning; SOAP API for Deprovisioning.
- C. Provisioning API for both Provisioning and Deprovisioning.
- D. Just-in-Time (JIT) for both Provisioning and Deprovisionin

Answer: D

Explanation:

Just-in-Time (JIT) provisioning and deprovisioning can be used to create, update, or deactivate users in Salesforce based on the information in the SAML assertion sent by the IdP. This way, the user lifecycle can be managed automatically without the need for a separate provisioning API. Reference: [Salesforce Help: Just-in-Time Provisioning for SAML]

NEW QUESTION 163

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

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

- * Identity-and-Access-Management-Architect Questions and Answers Updated Frequently
- * Identity-and-Access-Management-Architect Practice Questions Verified by Expert Senior Certified Staff
- * Identity-and-Access-Management-Architect Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * Identity-and-Access-Management-Architect Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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