



Salesforce

Exam Questions Identity-and-Access-Management-Architect

Salesforce Certified Identity and Access Management Architect (SU23)

NEW QUESTION 1

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

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

Answer: BD

Explanation:

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

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

NEW QUESTION 2

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

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

Answer: D

Explanation:

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

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

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

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

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

NEW QUESTION 3

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

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

Answer: ADE

Explanation:

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

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

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

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

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

NEW QUESTION 4

Universal containers (UC) is setting up Delegated Authentication to allow employees to log in using their corporate credentials. UC's security team is concerned about the risk of exposing the corporate login service on the Internet and has asked that a reliable trust mechanism be put in place between the login service and salesforce. What mechanism should an architect put in place to enable a trusted connection between the login services and salesforce?

- A. Include client ID and client secret in the login header callout.
- B. Set up a proxy server for the login service in the DMZ.

- C. Require the use of Salesforce security Tokens on password.
- D. Enforce mutual Authentication between systems using SSL.

Answer: D

Explanation:

To enable a trusted connection between the login services and Salesforce, UC should enforce mutual authentication between systems using SSL. Mutual authentication is a process in which both parties in a communication verify each other's identity using certificates⁷. SSL (Secure Sockets Layer) is a protocol that provides secure communication over the Internet using encryption and certificates⁸. By using mutual authentication with SSL, UC can ensure that only authorized login services can access Salesforce and vice versa. This can prevent unauthorized access, impersonation, or phishing attacks.

References: Mutual Authentication, SSL (Secure Sockets Layer)

NEW QUESTION 5

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 6

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

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

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

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

Answer: BD

Explanation:

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

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

NEW QUESTION 7

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

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

Answer: B

Explanation:

This is an OAuth authorization flow that allows a web server application to obtain an access token to access Salesforce resources on behalf of the user¹. This flow is suitable for integrating a desktop application with Salesforce, as it does not require the user to enter their credentials in the application, but rather redirects them to the Salesforce login page to authenticate and authorize the application². This way, the integration between the desktop application and Salesforce is seamless and secure. The other options are not optimal for this requirement because:

- JWT Bearer Token Flow is an OAuth authorization flow that allows a client application to obtain an access token by sending a signed JSON Web Token (JWT) to Salesforce³. This flow does not involve user interaction, and requires the client application to have a certificate and a private key to sign the JWT. This flow is more suitable for server-to-server integration, not for desktop application integration.
- User Agent Flow is an OAuth authorization flow that allows a user-agent-based application (such as a browser or a mobile app) to obtain an access token by redirecting the user to Salesforce and receiving the token in the URL fragment⁴. This flow is not suitable for desktop application integration, as it requires the application to parse the URL fragment and store the token securely.
- Username and Password Flow is an OAuth authorization flow that allows a client application to obtain an access token by sending the user's username and password to Salesforce⁵. This flow is not recommended for desktop application integration, as it requires the user to enter their credentials in the application, which is not secure or seamless. References: OAuth Authorization Flows, Implement the OAuth 2.0 Web Server Flow, JWT-Based Access Tokens (Beta), User-

Agent Flow, Username-Pass Flow

NEW QUESTION 8

Northern Trail Outfitters (NTO) utilizes a third-party cloud solution for an employee portal. NTO also owns Salesforce Service Cloud and would like employees to be able to login to Salesforce with their third-party portal credentials for a seamless experience. The third-party employee portal only supports OAuth. What should an identity architect recommend to enable single sign-on (SSO) between the portal and Salesforce?

- A. Configure SSO to use the third-party portal as an identity provider.
- B. Create a custom external authentication provider.
- C. Add the third-party portal as a connected app.
- D. Configure Salesforce for Delegated Authentication.

Answer: A

Explanation:

Configuring SSO to use the third-party portal as an identity provider is the best option to enable SSO between the portal and Salesforce. The portal can use OAuth as the protocol to authenticate users and redirect them to Salesforce. The other options are either not feasible or not relevant for this use case. References: Single Sign-On for Desktop and Mobile Applications using SAML and OAuth, Single Sign-On with SAML on Force.com

NEW QUESTION 9

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

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

Answer: BE

Explanation:

Delegated authentication is a feature that allows Salesforce to delegate the authentication process to an external service of your choice¹. When implementing delegated authentication, you should consider the following aspects²:

- The authentication web service can include custom attributes, such as user roles or permissions, in the response to Salesforce. These attributes can be used to update user records or trigger workflows in Salesforce².
- Delegated authentication can be used to authenticate API clients and mobile apps that use the SOAP API or REST API login() methods. However, it does not support OAuth 2.0 flows or other authentication methods².
- Delegated authentication does not require trusted IP ranges at the User Profile level. However, you can use them to restrict access to Salesforce from specific IP addresses or ranges².
- Salesforce servers receive but do not validate a user's credentials. Instead, they pass the credentials to the external authentication service, which validates them and returns a response to Salesforce².
- Just-in-time provisioning can be configured for new users who log in with delegated authentication. This feature allows Salesforce to create or update user accounts based on the information provided by the external authentication service³.

References:

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

NEW QUESTION 10

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 10

Universal Containers is creating a web application that will be secured by Salesforce Identity using the OAuth 2.1 Web Server Flow uses the OAuth 2.0 authorization code grant type).

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

- A. Verification URL
- B. Client Secret

- C. Access Token
- D. Scopes

Answer: BCD

Explanation:

The OAuth 2.0 Web Server Flow requires the client secret to authenticate the web application to Salesforce. The access token is used to access the Salesforce resources on behalf of the user. The scopes define the permissions and access levels for the web application. References: OAuth 2.0 Web Server Authentication Flow, Digging Deeper into OAuth 2.0 on Force.com

NEW QUESTION 14

Universal Containers (UC) employees have Salesforce access from restricted IP ranges only, to protect against unauthorized access. UC wants to roll out 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 with a second factor in the Connect App settings for Salesforce1 mobile app.
- B. Remove existing restrictions on IP ranges for all types of user access.
- C. Relax the IP restrictions in the Connect App settings for the Salesforce1 mobile app.
- D. Use Login Flow to bypass IP range restriction for the mobile app.

Answer: AC

Explanation:

The two options that an architect should recommend for UC to roll out the Salesforce1 mobile app and make it accessible from any location are:

- Relax the IP restriction with a second factor in the Connected App settings for Salesforce1 mobile app. This option allows UC to enable two-factor authentication (2FA) for the Salesforce1 mobile app, which requires users to verify their identity with a second factor, such as a verification code or a mobile app, after entering their username and password. By enabling 2FA in the Connected App settings, UC can relax the IP restriction for the Salesforce1 mobile app, as users can access it from any location as long as they provide the second factor.
- Relax the IP restrictions in the Connected App settings for the Salesforce1 mobile app. This option allows UC to disable or modify the IP restriction for the Salesforce1 mobile app in the Connected App settings, which control how users can access a connected app, such as Salesforce1. By relaxing the IP restrictions, UC can allow users to access the Salesforce1 mobile app from any location without requiring 2FA. The other options are not recommended for this scenario. Removing existing restrictions on IP ranges for all types of user access would compromise security and compliance, as it would expose Salesforce to unauthorized access from any location. Using Login Flow to bypass IP range restriction for the mobile app would require custom code and logic, which could introduce complexity and errors. References: [Connected Apps], [Two-Factor Authentication], [Require a Second Factor of Authentication for Connected Apps], [IP Restrictions for Connected Apps], [Login Flows]

NEW QUESTION 16

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

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

Answer: B

Explanation:

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

NEW QUESTION 21

A third-party app provider would like to have users provisioned via a service endpoint before users access their app from Salesforce. What should an identity architect recommend to configure the requirement with limited changes to the third-party app?

- A. Use a connected app with user provisioning flow.
- B. Create Canvas app in Salesforce for third-party app to provision users.
- C. Redirect users to the third-party app for registration.
- D. Use Salesforce identity with Security Assertion Markup Language (SAML) for provisioning users.

Answer: A

Explanation:

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

NEW QUESTION 24

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 26

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 27

Northern Trail Outfitters (NTO) believes a specific user account may have been compromised. NTO inactivated the user account and needs U perform a forensic analysis and identify signals that could indicate a breach has occurred.

What should NTO's first step be in gathering signals that could indicate account compromise?

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

Answer: D

Explanation:

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

NEW QUESTION 28

An insurance company has a connected app in its Salesforce environment that is used to integrate with a Google Workspace (formerly known 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 29

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

- A. Customer Community license
- B. Identity license

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

Answer: D

Explanation:

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

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

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

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

References: : Salesforce Licensing Module - Trailhead : Free Salesforce

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

NEW QUESTION 33

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

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

Answer: CD

Explanation:

The two options that an architect should recommend to UC are to build a custom web service that is supported by delegated authentication and to implement the OpenID protocol and configure an authentication provider. Delegated authentication is a feature that allows Salesforce to delegate user authentication to an external service instead of using Salesforce credentials³. A custom web service can be built to use the credentials stored in the custom identity store and validate them against Salesforce using SOAP or REST API³. OpenID is an open standard protocol that allows users to authenticate with various web services using an existing account⁴. An authentication provider can be configured in Salesforce to use OpenID and connect with the custom identity store⁵.

References: Delegated Authentication, OpenID, Authentication Providers

NEW QUESTION 37

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

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

Answer: D

Explanation:

Using custom login flows to connect to the existing custom 2fa system for use in salesforce is the recommended solution because it allows you to leverage your existing 2fa infrastructure and provide a consistent user experience across your applications. Custom login flows let you customize the authentication process by adding extra screens or logic before or after the standard login¹. You can use Apex code to call your custom 2fa system and verify the user's identity². This option also gives you more flexibility and control over the 2fa process than using native 2fa or an app exchange app³. References: 1: Customize User Authentication with Login Flows 2: Custom Login Flow Examples 3: Salesforce Multi-Factor Authentic

NEW QUESTION 42

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

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

Answer: D

Explanation:

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

NEW QUESTION 43

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

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

Answer: B

Explanation:

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

NEW QUESTION 46

Northern Trail Outfitters (NTO) uses the Customer 360 Platform implemented on Salesforce Experience Cloud. The development team in charge has learned of a contactless user feature, which can reduce the overhead of managing customers and partners by creating users without contact information. What is the potential impact to the architecture if NTO decides to implement this feature?

- A. Custom registration handler is needed to correctly assign External Identity or Community license for the newly registered contactless user.
- B. If contactless user is upgraded to Community license, the contact record is automatically created and linked to the user record, but not associated with an Account.
- C. Contactless user feature is available only with the External Identity license, which can restrict the Experience Cloud functionality available to the user.
- D. Passwordless authentication cannot be supported because the mobile phone receiving one-time password (OTP) needs to match the number on the contact record.

Answer: B

Explanation:

According to the Salesforce documentation³, contactless user feature allows creating users without contact information, such as email address or phone number. This reduces the overhead of managing customers and partners who don't need or want to provide their contact information. However, if a contactless user is upgraded to a Community license, a contact record is automatically created and linked to the user record, but not associated with an account. This can impact the architecture of NTO's Customer 360 Platform, as they may need to associate contacts with accounts for reporting or other purposes.

NEW QUESTION 47

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 51

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

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

Answer: B

Explanation:

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

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

References:

- OAuth 2.0 Device Flow

NEW QUESTION 54

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

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

Answer: BC

Explanation:

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

NEW QUESTION 59

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 63

Universal Containers built a custom mobile app for their field reps to create orders in Salesforce. OAuth is used for authenticating mobile users. The app is built in such a way that when a user session expires after Initial login, a new access token is obtained automatically without forcing the user to log in again. While that improved the field reps' productivity, UC realized that they need a "logout" feature.

What should the logout function perform in this scenario, where user sessions are refreshed automatically?

- A. Invoke the revocation URL and pass the refresh token.
- B. Clear out the client Id to stop auto session refresh.
- C. Invoke the revocation URL and pass the access token.
- D. Clear out all the tokens to stop auto session refresh.

Answer: A

Explanation:

The refresh token is used to obtain a new access token when the previous one expires. To revoke the user session, the logout function should invoke the revocation URL and pass the refresh token as a parameter. This will invalidate both the refresh token and the access token, and prevent the user from accessing Salesforce without logging in again.

References:

- > Certification Exam Guide
- > Revoke OAuth Tokens

NEW QUESTION 68

IT security at Universal Containers (UC) is concerned about recent phishing scams targeting its users and wants to add additional layers of login protection. What should an Architect recommend to address the issue?

- A. Use the Salesforce Authenticator mobile app with two-step verification
- B. Lock sessions to the IP address from which they originated.
- C. Increase Password complexity requirements in Salesforce.
- D. Implement Single Sign-on using a corporate Identity store.

Answer: A

Explanation:

The Salesforce Authenticator mobile app adds an extra layer of security for online accounts with two-factor authentication. It allows users to respond to push notifications or use location services to verify their logins and other account activity. This can help prevent phishing scams and unauthorized access.

References: Salesforce Authenticator, Salesforce Authenticator: Mobile App Security Features, Salesforce Authenticator

NEW QUESTION 71

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

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

Answer: B

Explanation:

If the third-party authentication provider supports only the OAuth protocol and not OpenID Connect, then an identity architect needs to create a custom external authentication provider for it. A custom external authentication provider is a configuration that allows users to log in to Salesforce using an external identity provider that is not predefined by Salesforce. It requires implementing the Auth.AuthProviderPlugin interface and defining the OAuth endpoints and parameters. References: Custom External Authentication Providers, Create a Custom Authentication Provider

NEW QUESTION 72

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, Twitter)
- 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 75

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

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

Answer: C

Explanation:

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

NEW QUESTION 78

Universal containers (UC) is successfully using Delegated Authentication for their salesforce users. The service supporting Delegated Authentication is written in Java. UC has a new CIO that is requiring all company Web services be RESR-ful and written in .NET. Which two considerations should the UC Architect provide to the new CIO? Choose 2 answers

- A. Delegated Authentication will not work with a.net service.
- B. Delegated Authentication will continue to work with rest services.
- C. Delegated Authentication will continue to work with a.net service.
- D. Delegated Authentication will not work with rest services.

Answer: CD

Explanation:

Delegated Authentication will continue to work with a .NET service as long as it is wrapped in a web service that Salesforce can consume1. Delegated Authentication will not work with REST services because it requires a SOAP-based web service23. Therefore, option C and D are the correct answers. References: Salesforce Documentation, DEV Community, Salesforce Developer Community

NEW QUESTION 82

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

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

Answer: BC

Explanation:

High assurance sessions are sessions that require a stronger level of identity verification, such as two-factor authentication or SAML assertions¹. Google Authenticator is an app that generates verification codes on your mobile device that you can use as a second factor of authentication². These measures can help prevent unauthorized access to the connected app by ensuring that the user is who they claim to be and that they have access to their mobile device. Disallowing the use of single sign-on (SSO) for the mobile app is not a recommendation because SSO can provide a seamless and secure user experience across multiple applications³. Setting login IP ranges to the internal network for the app users profiles is not a recommendation because it can limit the mobility and flexibility of the users who are commonly out of the office. References: 1: Session Security Levels 2: Google Authenticator 3: Connected Apps : [Restrict Access by IP Address]

NEW QUESTION 87

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

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

Answer: B

Explanation:

The users do not have the correct permission set assigned to them is the most likely cause of the issue. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect¹. Connected apps use these protocols to authorize, authenticate, and provide single sign-on (SSO) for external apps¹. To access a connected app, users must have the appropriate permissions assigned to them, either through their profile or a permission set². If the users do not have the required permissions, they will receive an error message when they try to access the connected app. The use of high assurance sessions are required for the connected app is not a valid option, as high assurance sessions are related to multi-factor authentication (MFA), not connected apps³. The connected app setting "All users may self-authorize" is enabled is not a cause of the issue, but a possible solution. This setting allows users to access the connected app without pre-approval from an administrator⁴. The Salesforce administrators have revoked the OAuth authorization is not a likely cause of the issue, as OAuth authorization is granted by the users, not the administrators⁵. Revoking OAuth authorization would also affect all users, not just a group of them.

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

NEW QUESTION 88

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

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

Answer: C

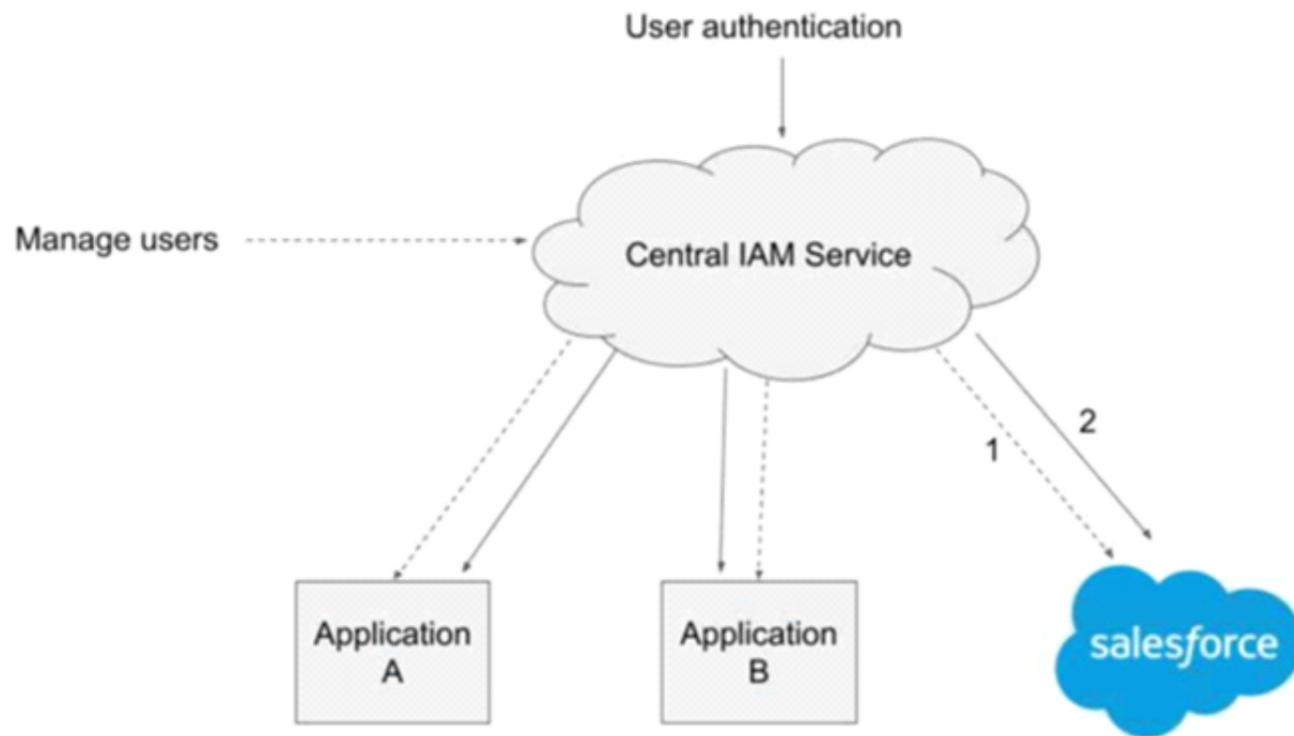
Explanation:

The Entity Id is the SAML SSO setting in Salesforce that provides the capability to differentiate Salesforce from other service providers. The Entity Id is a unique identifier for the service provider that is sent to the identity provider as part of the SSO request⁴. The identity provider uses the Entity Id to determine which service provider configuration to use and which SAML assertion to send back⁵. The other options are not valid SAML SSO settings for this purpose. The Identity Provider Login URL is the URL of the identity provider's SSO service that Salesforce redirects the user to for authentication⁴. The Issuer is the unique identifier for the identity provider that is sent by the identity provider as part of the SAML response⁴. The SAML Identity Location is the location of the user's identity in the SAML assertion, either in the Subject element or in an Attribute element⁴.

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

NEW QUESTION 93

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 95

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

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

Answer: D

Explanation:

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

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

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

NEW QUESTION 99

Universal containers (UC) wants to integrate a Web application with salesforce. The UC team has implemented the Oauth web-server Authentication flow for authentication process. Which two considerations should an architect point out to UC? Choose 2 answers

- A. The web application should be hosted on a secure server.
- B. The web server must be able to protect consumer privacy
- C. The flow involves passing the user credentials back and forth.
- D. The flow will not provide an Oauth refresh token back to the server.

Answer: AB

Explanation:

The web application should be hosted on a secure server and the web server must be able to protect consumer privacy are two considerations that an architect should point out to UC. To integrate an external web app with the Salesforce API, UC can use the OAuth 2.0 web server flow, which implements the OAuth 2.0 authorization code grant type⁴. With this flow, the server hosting the web app must be able to protect the connected app's identity, defined by the client ID and client secret⁴. The web application should be hosted on a secure server to ensure that the communication between the web app and Salesforce is encrypted and protected from unauthorized access or tampering⁶. The web server must be able to protect consumer privacy to comply with data protection laws and regulations, such as GDPR or CCPA . The web server should implement best practices for storing and handling user data, such as encryption, hashing, salting, and anonymization. The flow involves passing the user credentials back and forth is not a correct consideration, as the web server flow does not require the user credentials to be passed between the web app and Salesforce. Instead, it uses an authorization code that is exchanged for an access token and a refresh token⁴. The flow will not provide an OAuth refresh token back to the server is also not a correct consideration as the web server flow does provide a refresh token that can be used to obtain new access tokens without user interaction⁴. References: OAuth 2.0 Web Server Flow for Web App Integration, Secure Your Web Application, [General Data Protection Regulation (GDPR)], [California Consumer Privacy Act (CCPA)], [Data Protection Best Practices]

NEW QUESTION 102

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

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

Answer: C

Explanation:

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

- Purchasing a third-party Identity Provider for all five Salesforce orgs would incur additional cost and maintenance, and would not leverage the existing user base in UC1.
- Not setting up JIT user provisioning for other orgs would require manually creating or updating user accounts in each org, which would be time-consuming and error-prone. References: Salesforce as an Identity Provider, Identity Providers and Service Providers, Just-in-Time Provisioning for SAML

NEW QUESTION 106

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

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

Answer: B

Explanation:

The most likely cause of the issue is that the refresh token expiration policy is set incorrectly in Salesforce. A refresh token is a credential that allows a connected app to obtain a new access token when the previous one expires¹. The refresh token expiration policy determines how long a refresh token is valid for². If the policy is set to a short duration, such as 24 hours, the users have to enter their credentials once a day to get a new refresh token. To prevent this, the policy should be set to a longer duration, such as "Refresh token is valid until revoked" or "Refresh token expires after 90 days of inactivity"².

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

NEW QUESTION 110

Universal containers (UC) has implemented SAML -based single Sign-on for their salesforce application. UC is using PingFederate as the Identity provider. To access salesforce, Users usually navigate to a bookmarked link to my domain URL. What type of single Sign-on is this?

- A. Sp-Initiated
- B. IDP-initiated with deep linking
- C. IDP-initiated
- D. Web server flow.

Answer: A

Explanation:

The type of single sign-on that UC is using is SP-initiated, which means that the service provider (Salesforce) initiates the SSO process by sending a SAML request to the identity provider (PingFederate) when the user navigates to the My Domain URL. Therefore, option A is the correct answer. References: SAML SSO with Salesforce as the Service Provider

NEW QUESTION 112

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

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

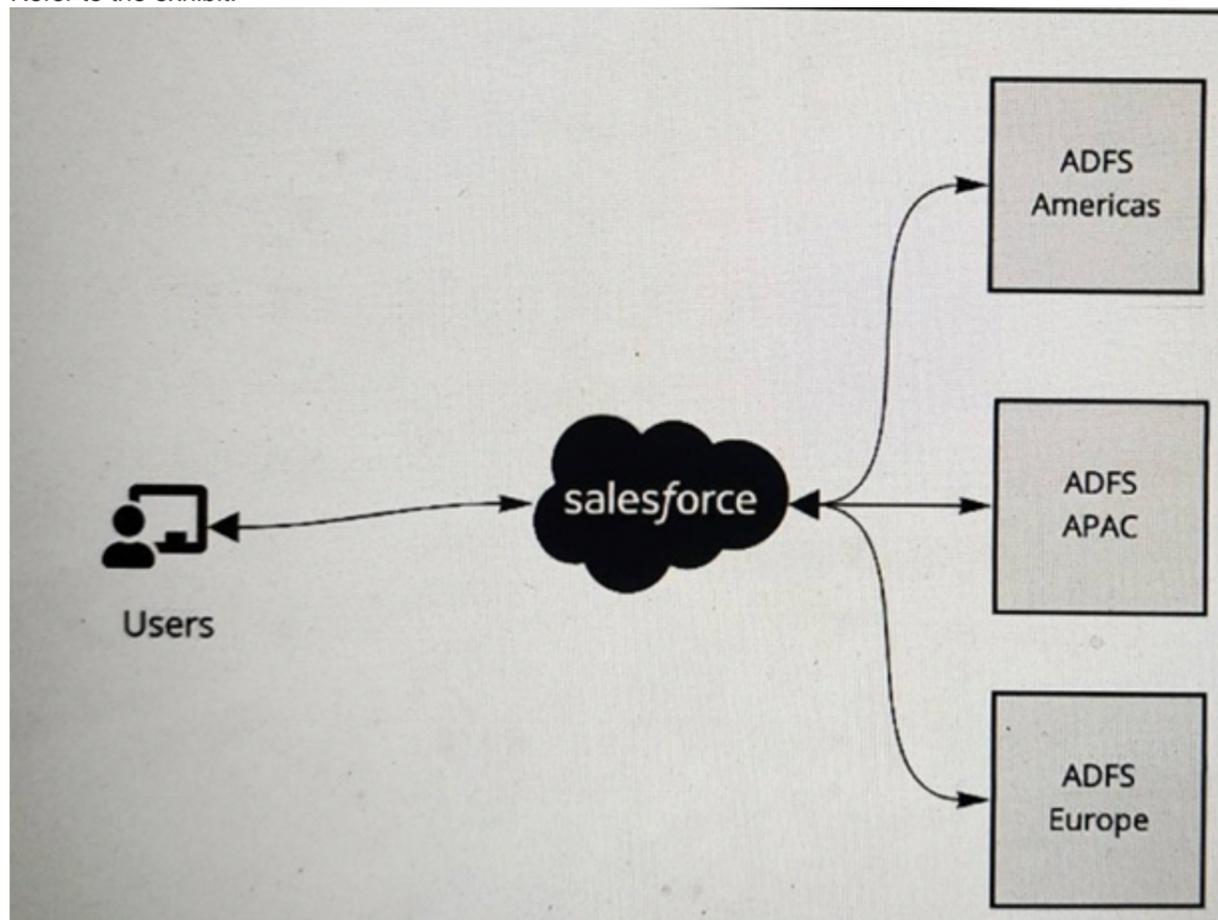
Answer: A

Explanation:

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

NEW QUESTION 113

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 114

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

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

Answer: ABE

Explanation:

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

NEW QUESTION 115

Universal Containers (UC) has decided to use Salesforce as an Identity Provider for multiple external applications. UC wants to use the Salesforce App Launcher to control the Apps that are available to individual users. Which three steps are required to make this happen?

- A. Add each connected App to the App Launcher with a Start URL.
- B. Set up an Auth Provider for each External Application.
- C. Set up Salesforce as a SAML Idp with My Domain.
- D. Set up Identity Connect to Synchronize user data.
- E. Create a Connected App for each external application.

Answer: ACE

Explanation:

These are the steps required to enable Salesforce as a SAML Identity Provider and use the App Launcher to access external applications. According to the Salesforce documentation¹, you need to:

- Enable Salesforce as a SAML Identity Provider with My Domain².
- Create a Connected App for each external application that you want to integrate with Salesforce³.
- Add each Connected App to the App Launcher with a Start URL that points to the external application¹.

Option B is incorrect because setting up an Auth Provider is not necessary for SAML SSO. Auth Providers are used for OAuth SSO, which is a different protocol⁴. Option D is incorrect because Identity Connect is a tool for synchronizing user data between Active Directory and Salesforce, which is not related to SSO or App Launcher⁵.

References: 1: App Launcher - Salesforce 2: Enable Salesforce as a SAML Identity Provider 3: Connect Apps Overview 4: Identity Providers and Service Providers - Salesforce 5: Identity Connect Overview

NEW QUESTION 118

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

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

What should an Identity architect do to fulfill the requirement?

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

Answer: D

Explanation:

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

NEW QUESTION 120

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 123

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 127

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 132

A global company is using the Salesforce Platform as an Identity Provider and needs to integrate a third-party application with its Experience Cloud customer portal. Which two features should be utilized to provide users with login and identity services for the third-party application? Choose 2 answers

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

Answer: AC

Explanation:

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

NEW QUESTION 136

An identity architect is implementing a mobile-first Consumer Identity Access Management (CIAM) for external users. User authentication is the only requirement. The users email or mobile phone number should be supported as a username. Which two licenses are needed to meet this requirement? Choose 2 answers

- A. External Identity Licenses
- B. Identity Connect Licenses
- C. Email Verification Credits
- D. SMS verification Credits

Answer: AD

Explanation:

External Identity Licenses are required to enable external users to access Salesforce resources via a CIAM solution. Email Verification Credits and SMS Verification Credits are required to enable email or mobile phone number verification for user authentication. Identity Connect Licenses are not required for this scenario, as Identity Connect is a tool for synchronizing user data between Salesforce and Active Directory. References: External Identity Implementation Guide, Identity Connect Implementation Guide

NEW QUESTION 138

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 141

How should an identity architect automate provisioning and deprovisioning of users into Salesforce from an external system?

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

Answer: C

Explanation:

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

NEW QUESTION 145

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 147

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 152

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

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

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

Answer: AB

Explanation:

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

NEW QUESTION 153

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

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

Answer: C

Explanation:

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

NEW QUESTION 158

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 159

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

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

Answer: BC

Explanation:

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

NEW QUESTION 162

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

- A. Resource deep linking
- B. App launcher
- C. SSO from salesforce1 mobile app.
- D. Login forensics

Answer: AC

Explanation:

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

NEW QUESTION 163

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 166

Universal Containers is using OpenID Connect to enable a connection from their new mobile app to its production Salesforce org.

What should be done to enable the retrieval of the access token status for the OpenID Connect connection?

- A. Query using OpenID Connect discovery endpoint.
- B. A Leverage OpenID Connect Token Introspection.
- C. Create a custom OAuth scope.
- D. Enable cross-origin resource sharing (CORS) for the /services/oauth2/token endpoint.

Answer: B

Explanation:

According to the Salesforce documentation1, OpenID Connect Token Introspection allows all OAuth connected apps to check the current state of an OAuth 2.0 access or refresh token. The resource server or connected apps send the client app's client ID and secret to the authorization server, initiating an OAuth authorization flow. As part of this flow, the authorization server validates, or introspects, the client app's access token. If the access token is current and valid, the client app is granted access.

NEW QUESTION 168

Universal Containers (UC) uses middleware to integrate multiple systems with Salesforce. UC has a strict, new requirement that usernames and passwords cannot be stored in any UC system. How can UC's middleware authenticate to Salesforce while adhering to this requirement?

- A. Create a Connected App that supports the JWT Bearer Token OAuth Flow.
- B. Create a Connected App that supports the Refresh Token OAuth Flow
- C. Create a Connected App that supports the Web Server OAuth Flow.
- D. Create a Connected App that supports the User-Agent OAuth Flow.

Answer: A

Explanation:

A is correct because creating a connected app that supports the JWT Bearer Token OAuth Flow allows the middleware to authenticate to Salesforce without storing usernames and passwords. The JWT Bearer Token OAuth Flow uses a certificate and a private key to sign a JSON Web Token (JWT) that contains information about the user identity and requested access. The middleware sends the JWT to Salesforce, which verifies it using the certificate and grants an access token2.

B is incorrect because creating a connected app that supports the Refresh Token OAuth Flow requires storing usernames and passwords in the middleware. The Refresh Token OAuth Flow uses a username-password authentication flow to obtain an access token and a refresh token. The middleware can use the refresh token to obtain new access tokens without user interaction, but it still needs to store the username and password for the initial authentication3.

C is incorrect because creating a connected app that supports the Web Server OAuth Flow requires user interaction to authenticate to Salesforce. The Web Server OAuth Flow redirects the user to a Salesforce login page, where they enter their credentials and grant access to the middleware. The middleware then receives an authorization code that it can exchange for an access token and a refresh token4.

D is incorrect because creating a connected app that supports the User-Agent OAuth Flow also requires user interaction to authenticate to Salesforce. The User-Agent OAuth Flow is similar to the Web Server OAuth Flow, except that it does not return a refresh token. The middleware can only use the access token until it expires5.

References: 2: Accessing Salesforce with JWT OAuth Flow 3: OAuth Authorization Flows - Salesforce 4: OAuth Authorization Flows - Salesforce 5: OAuth Authorization Flows - Salesforce

NEW QUESTION 171

Universal Containers (UC) wants to use Salesforce for sales orders and a legacy of system for order fulfillment. The legacy system must update the status of orders in 65* Salesforce in real time as they are fulfilled. UC decides to use OAuth for connecting the legacy system to Salesforce. What OAuth flow should be considered that doesn't require storing credentials, client secret or refresh tokens?

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

Answer: B

Explanation:

The JWT Bearer Token flow is an OAuth flow in which an external app (also called client or consumer app) sends a signed JSON string to Salesforce called JWT to obtain an access token. The access token can then be used by the external app to read & write data in Salesforce1. This flow does not require storing credentials, client secret or refresh tokens, as the JWT is self-contained and includes information about the app and the user2. The other flows require either user interaction (Web Server flow and User Agent flow) or storing credentials (Username-Password flow)3.

References: Salesforce OAuth : JWT Bearer Flow, Accessing Salesforce with JWT OAuth Flow, OAuth Authorization Flows - Salesforce

NEW QUESTION 176

What is one of the roles of an Identity Provider in a Single Sign-on setup using SAML?

- A. Validate token
- B. Create token
- C. Consume token
- D. Revoke token

Answer: B

Explanation:

Creating a token is one of the roles of an Identity Provider in a Single Sign-on setup using SAML. SAML is a standard protocol that allows users to access multiple applications with a single login. In SAML, an Identity Provider (IdP) is a system that authenticates users and issues a security token that contains information about the user's identity and permissions. A Service Provider (SP) is a system that consumes the token and grants access to the user based on the token's attributes. The other options are not roles of an IdP, but rather functions of the SAML protocol or the SP.

NEW QUESTION 181

universal container plans to develop a custom mobile app for the sales team that will use salesforce for authentication and access management. The mobile app access needs to be restricted to only the sales team. What would be the recommended solution to grant mobile app access to sales users?

- A. Use a custom attribute on the user object to control access to the mobile app
- B. Use connected apps OAuth policies to restrict mobile app access to authorized users.
- C. Use the permission set license to assign the mobile app permission to sales users
- D. Add a new identity provider to authenticate and authorize mobile users.

Answer: B

Explanation:

The recommended solution to grant mobile app access to sales users is to use connected apps OAuth policies to restrict mobile app access to authorized users. A connected app is a configuration in Salesforce that allows an external application, such as a mobile app, to connect to Salesforce using OAuth. OAuth is a protocol that allows the mobile app to obtain an access token from Salesforce after the user grants permission. The access token can then be used by the mobile app to access Salesforce data and features. OAuth policies are settings that control how users can access a connected app, such as who can use the app, how long the access token is valid, and what level of access the app requests. By configuring OAuth policies in the connected app settings, Universal Containers can restrict the mobile app access to only the sales team and protect against unauthorized or excessive access.

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

NEW QUESTION 186

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

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

Answer: BD

Explanation:

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

NEW QUESTION 190

A financial enterprise is planning to set up a user authentication mechanism to login to the Salesforce system. Due to regulatory requirements, the CIO of the company wants user administration, including passwords and authentication requests, to be managed by an external system that is only accessible via a SOAP webservice.

Which authentication mechanism should an identity architect recommend to meet the requirements?

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

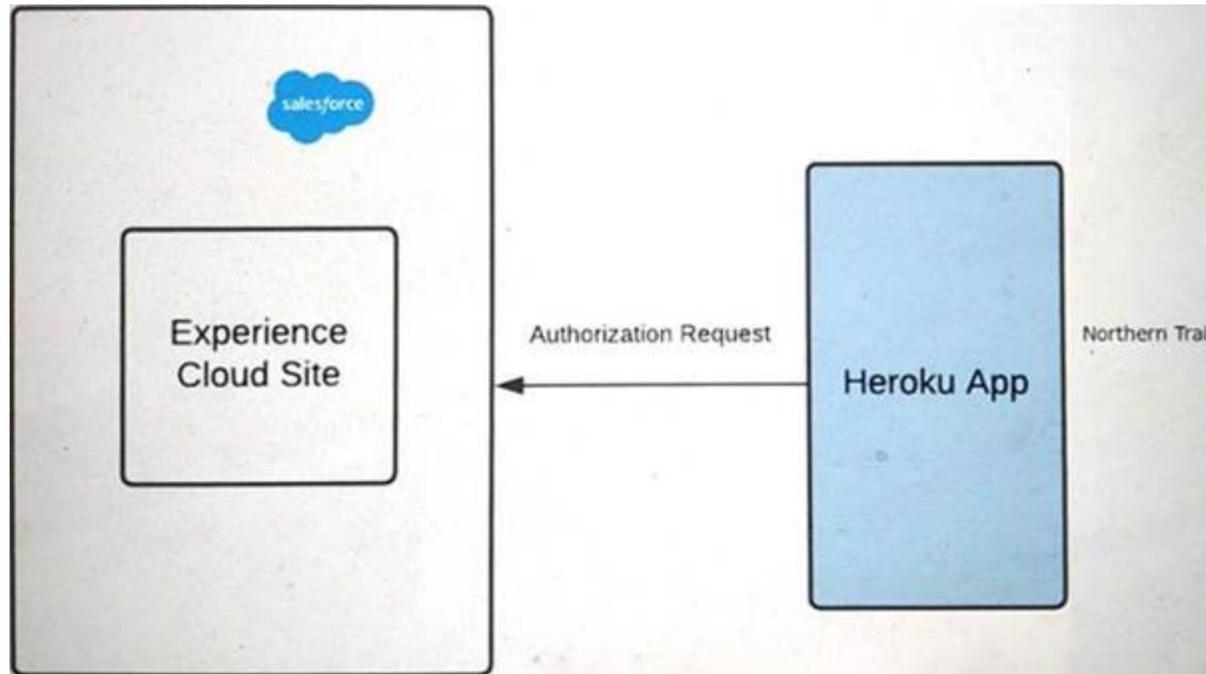
Answer: C

Explanation:

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

NEW QUESTION 192

Refer to the exhibit.



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

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

NTO wants to make sure it renders login page images dynamically based on the user's brand preference selected in Heroku before Authorization. what should an identity architect do to fulfill the above requirements?

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

Answer: D

Explanation:

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

- > Create a connected app for the third-party service in Salesforce. A connected app is an application that integrates with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect. To create a connected app, you need to provide the basic information, such as the app name, logo URL, contact email, and API name. You also need to enable OAuth and configure the OAuth settings, such as the callback URL, the scopes, and the policies.
- > Authorize the third-party service by sending authorization requests to the community-url/services/oauth2/authorize/expid_value. This is a special endpoint that allows you to specify an experience ID (expid) as a query parameter in the authorization request. The experience ID is a unique identifier for each experience (community or site) in Salesforce. By using this endpoint, you can dynamically render the login page images based on the user's brand preference selected in the third-party service before authorization.

References:

- > OAuth 2.0
- > OAuth 2.0 Web Server Authentication Flow
- > Connected Apps
- > Create a Connected App
- > Experience ID
- > Authorize Apps with OAuth

NEW QUESTION 197

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

Choose 2 answers

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

Answer: AD

Explanation:

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

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

NEW QUESTION 202

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 207

Universal Containers (UC) operates in Asia, Europe and North America regions. There is one Salesforce org for each region. UC is implementing Customer 360 in Salesforce and has procured External Identity and Customer Community licenses in all orgs. Customers of UC use Community to track orders and create inquiries. Customers also tend to move across regions frequently. What should an identity architect recommend to optimize license usage and reduce maintenance overhead?

- A. Merge three orgs into one instance of Salesforc
- B. This will no longer require maintaining three separate copies of the same customer.
- C. Delete contact/ account records and deactivate user if user moves from a specific region; Sync will no longer be required.
- D. Contacts are required since Community access needs to be enable
- E. Maintenance is a necessary overhead that must be handled via data integration.
- F. Enable Contactless User in all orgs and downgrade users from Experience Cloud license to External Identity license once users have moved out of that region.

Answer: D

Explanation:

To optimize license usage and reduce maintenance overhead for customers who use Community to track orders and create inquiries and tend to move across regions frequently, the identity architect should recommend enabling Contactless User in all orgs and downgrade users from Experience Cloud license to External Identity license once users have moved out of that region. Contactless User is a feature that allows users to access Experience Cloud sites without having a contact record associated with them. External Identity is a license type that enables users to access Experience Cloud sites using social sign-on or single sign-on, but not access Salesforce objects or data. By enabling Contactless User and downgrading users from Experience Cloud license to External Identity license, the identity architect can reduce the number of contacts and licenses needed for each region and avoid data duplication and synchronization issues. References: Contactless User, External Identity License, User Licenses

NEW QUESTION 211

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

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

Answer: B

Explanation:

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

NEW QUESTION 216

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

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

Answer: AD

Explanation:

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

NEW QUESTION 221

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

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

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

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