Salesforce

Exam Questions Identity-and-Access-Management-Architect

Salesforce Certified Identity and Access Management Architect (SU23)

NEW QUESTION 1
Universal containers want to build a custom mobile app connecting to salesforce using Oauth, and would like to restrict the types of resources mobile users can access. What Oauth feature of Salesforce should be used to achieve the goal?

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

Answer: D

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

NEW QUESTION 2
Universal Containers (UC) is building an authenticated Customer Community for its customers. UC does not want customer credentials stored in Salesforce and is confident its customers would be willing to use their social media credentials to authenticate to the community. Which two actions should an Architect recommend UC to take?

A. Use Delegated Authentication to call the Twitter login API to authenticate users.
B. Configure an Authentication Provider for LinkedIn Social Media Accounts.
C. Create a Custom Apex Registration Handler to handle new and existing users.
D. Configure SSO Settings For Facebook to serve as a SAML Identity Provider.

Answer: BC

Explanation:
Configuring an Authentication Provider for LinkedIn Social Media Accounts allows UC to use LinkedIn as an external identity provider for its customer community. This means that customers can use their LinkedIn credentials to log in to the community without storing their credentials in Salesforce. Creating a Custom Apex Registration Handler allows UC to customize how new and existing users are handled when they log in with an external identity provider. This means that UC can control how user records are created, updated, or matched when customers use their social media credentials to authenticate to the community. These two actions can meet the requirement of UC to use social media credentials for its customer community.

NEW QUESTION 3
Universal Containers (UC) wants to integrate a third-party Reward Calculation system with Salesforce to calculate Rewards. Rewards will be calculated on a schedule basis and update back into Salesforce. The integration between Salesforce and the Reward Calculation System needs to be secure. Which are two recommended practices for using OAuth flow in this scenario. choose 2 answers

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

Answer: CD

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

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

➤ OAuth JWT Bearer Token Flow, which allows the client app to use a JSON Web Token (JWT) signed by a private key to request an access token from Salesforce. This flow does not require any user interaction or consent, and uses a certificate to verify the identity of the client app.
Verified References: [OAuth 2.0 SAML Bearer Assertion Flow for Server-to-Server Integration], [OAuth 2.0 JWT Bearer Token Flow for Server-to-Server Integration]

NEW QUESTION 4
Universal Containers (UC) has a strict requirement to authenticate users to Salesforce using their mainframe credentials. The mainframe user store cannot be accessed from a SAML provider. UC would also like to have users in Salesforce created on the fly if they provide accurate mainframe credentials.
How can the Architect meet these requirements?

A. Use a Salesforce Login Flow to call out to a web service and create the user on the fly.
B. Use the SOAP API to create the user when created on the mainframe; implement Delegated Authentication.
C. Implement Just-In-Time Provisioning on the mainframe to create the user on the fly.
D. Implement OAuth User-Agent Flow on the mainframe; use a Registration Handler to create the user on the fly.

Answer: C

Explanation:
The best way to meet the requirements of UC is to implement Just-In-Time Provisioning on the mainframe to create the user on the fly. According to the Salesforce documentation, "Just-in-time provisioning lets you create or update user accounts on the fly when users log in to Salesforce using single sign-on (SSO)." This way, UC can authenticate users to Salesforce using their mainframe credentials and also create or update their user accounts in Salesforce without using a SAML

provider. Therefore, option C is the correct answer.
References: [Just-in-Time Provisioning]

NEW QUESTION 5
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 6
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 7
Universal Containers (UC) uses a home-grown Employee portal for their employees to collaborate. UC decides to use Salesforce Ideas to allow employees to post Ideas from the Employee portal. When users click on some of the links in the Employee portal, the users should be redirected to Salesforce, authenticated, and presented with the relevant pages. What OAuth flow is best suited for this scenario?

A. Web Application flow
B. SAML Bearer Assertion flow
C. User-Agent flow
D. Web Server flow

Answer: D

Explanation:
The best OAuth flow for this scenario is the web server flow. The web server flow is an OAuth authorization flow that allows a web application, such as UC's employee portal, to obtain an access token and a refresh token from Salesforce after the user grants permission. The web application can then use the access token to access Salesforce data and features, such as posting ideas, and use the refresh token to obtain a new access token when the previous one expires or becomes invalid. This flow is suitable for UC's scenario because it allows users to be redirected to Salesforce, authenticated, and presented with the relevant pages when they click on some of the links in the employee portal. This flow also provides a secure and seamless user experience by using a confidential client secret that is stored on the web server and not exposed to the browser.
The other options are not valid OAuth flows for this scenario. The web application flow is not a standard term for OAuth, but it could refer to the user-agent flow, which is an OAuth authorization flow that allows a browser or web-view, such as a mobile app or a desktop app, to obtain an access token from Salesforce by using a script or a pop-up window. This flow is not suitable for UC's scenario, as it does not use a web server or a client secret, and it does not provide a refresh token. The SAML bearer assertion flow is an OAuth authorization flow that allows an external application to obtain an access token from Salesforce by using a SAML assertion from an identity provider (IdP) that verifies the user's identity. This flow is not suitable for UC's scenario, as it does not involve user interaction or redirection to Salesforce. The user-agent flow is an OAuth authorization flow that allows a browser or web-view, such as a mobile app or a desktop app, to obtain an access token from Salesforce by using a script or a pop-up window. This flow is not suitable for UC's scenario, as it does not use a web server or a client secret, and it does not provide a refresh token. References: [OAuth Authorization Flows], [OAuth 2.0 Web Server Flow for Web App Integration], [OAuth 2.0 User-Agent Flow for Desktop Apps], [OAuth 2.0 SAML Bearer Assertion Flow for Server-to-Server Integration]

NEW QUESTION 8
Universal Containers (UC) is building a customer community and will allow customers to authenticate using Facebook credentials. The First time the user authenticating using Facebook, UC would like a customer account created automatically in their accounting system. The accounting system has a web service accessible to Salesforce for the creation of accounts. How can the Architect meet these requirements?

A. Create a custom application on Heroku that manages the sign-on process from Facebook.
B. Use JIT Provisioning to automatically create the account in the accounting system.
C. Add an Apex callout in the registration handler of the authorization provider.
D. Use OAuth JWT flow to pass the data from Salesforce to the Accounting System.

Answer: C

Explanation:
The best option for UC to meet the requirements is to add an Apex callout in the registration handler of the authorization provider. An authorization provider is a configuration in Salesforce that allows users to log in with an external authentication provider, such as Facebook. A registration handler is an Apex class that implements the Auth.RegistrationHandler interface and defines the logic for creating or updating a user account when a user logs in with an external authentication provider. An Apex callout is a method that invokes an external web service from Apex code. By adding an Apex callout in the registration handler, UC can create a customer account in their accounting system by calling the web service that is accessible to Salesforce. This option enables UC to automate the account creation process and integrate with their existing accounting system. The other options are not optimal for this scenario. Creating a custom application on Heroku that manages the sign-on process from Facebook would require UC to develop and maintain a separate application and infrastructure, which could increase complexity and cost. Using JIT provisioning to automatically create the account in the accounting system would require UC to configure Facebook as a SAML identity provider, which is not supported by Facebook. Using OAuth JWT flow to pass the data from Salesforce to the accounting system would require UC to obtain an OAuth token from the accounting system and use it to make API calls, which could introduce security and performance issues. References: [Authorization Providers],
[Create a Registration Handler Class], [Auth.RegistrationHandler Interface], [Apex Callouts], [Facebook as SAML Identity Provider], [OAuth 2.0 JWT Bearer Flow for Server-to-Server Integration]

NEW QUESTION 9
A web service is developed that allows secure access to customer order status on the Salesforce Platform. The service connects to Salesforce through a connected app with the web server flow. The following are the required actions for the authorization flow:
* 1. User Authenticates and Authorizes Access
* 2. Request an Access Token
* 3. Salesforce Grants an Access Token
* 4. Request an Authorization Code
* 5. Salesforce Grants Authorization Code
What is the correct sequence for the authorization flow?

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

Answer: B

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

> The client app requests an authorization code from Salesforce by redirecting the user to the authorization endpoint.

> The user authenticates and authorizes access to the client app.

> Salesforce grants an authorization code and redirects the user back to the client app.

> The client app requests an access token from Salesforce by sending the authorization code to the token endpoint.

> Salesforce grants an access token and a refresh token to the client app. References: OAuth Authorization Flows, Authorize Apps with OAuth

NEW QUESTION 10
Universal Containers (UC) uses Salesforce as a CRM and identity provider (IdP) for their Sales Team to seamlessly login to intemaJ portals. The IT team at UC is now evaluating Salesforce to act as an IdP for its remaining employees.
Which Salesforce license is required to fulfill this requirement?

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

Answer: D

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

NEW QUESTION 10
Universal containers (UC) is setting up their customer Community self-registration process. They are uncomfortable with the idea of assigning new users to a default account record. What will happen when customers self-register in the community?

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

Answer: C

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

NEW QUESTION 15
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 19
Northern Trail Outfitters (NTO) wants to give customers the ability to submit and manage issues with their purchases. It is important for to give its customers the ability to login with their Facebook and Twitter credentials.
Which two actions should an identity architect recommend to meet these requirements? Choose 2 answers

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

Answer: BD

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

NEW QUESTION 21
Universal containers (UC) has an e-commerce website while customers can buy products, make payments, and manage their accounts. UC decides to build a customer Community on Salesforce and wants to allow the customers to access the community for their accounts without logging in again. UC decides to implement ansp-Initiated SSO using a SAML-BASED complaint IDP. In this scenario where salesforce is the service provider, which two activities must be performed in salesforce to make sp-Initiated SSO work? Choose 2 answers

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

Answer: AD

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

NEW QUESTION 22
An insurance company has a connected app in its Salesforce environment that is used to integrate with a Google Workspace (formerly knot as G Suite).
An identity and access management (IAM) architect has been asked to implement automation to enable users, freeze/suspend users, disable users, and reactivate existing users in Google Workspace upon similar actions in Salesforce.
Which solution is recommended to meet this requirement?

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

Answer: A

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

NEW QUESTION 24
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 26
Sales users at Universal containers use salesforce for Opportunity management. Marketing uses a third-party application called Nest for Lead nurturing that is accessed using username/password. The VP of sales wants to open up access to nest for all sales uses to provide them access to lead history and would like SSO for better adoption. Salesforce is already setup for SSO and uses Delegated Authentication. Nest can accept username/Password or SAML-based Authentication. IT teams have received multiple password-related issues for nest and have decided to set up SSO access for Nest for Marketing users as well. The CIO does not want to invest in a new IDP solution and is considering using Salesforce for this purpose. Which are appropriate license type choices for sales and marketing users, giving salesforce is using Delegated Authentication? Choose 2 answers

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

Answer: AD

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

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

Platform license for marketing users. This license type allows internal users to access custom Salesforce objects and features, such as custom apps and tabs. This license type also supports delegated authentication and single sign-on (SSO), which are features that allow users to log in with an external identity provider (IdP) or service provider (SP). This license type is suitable for marketing users who use a third-party application called Nest for lead nurturing and need to log in with SSO using Salesforce as the IdP or SP.
The other options are not appropriate license types for this scenario. Identity license for sales or marketing users would not allow them to access standard or custom Salesforce objects and features, as this license type only supports identity features, such as SSO and social sign-on. External Identity license for marketing users would not allow them to access custom Salesforce objects and features, as this license type is designed for external users, such as customers or partners, who access a limited set of standard and custom objects in a community. Identity Connect license for marketing users is not a valid license type, as Identity Connect is a desktop application that integrates Salesforce with Microsoft Active Directory (AD) and enables SSO between the two systems. References: [Salesforce Licenses], [Delegated Authentication], [Platform Licenses], [Single Sign-On], [External Identity Licenses], [Identity Connect]

NEW QUESTION 27
Northern Trail Outfitters would like to use a portal built on Salesforce Experience Cloud for customer self-service. Guests of the portal be able to self-register, but be unable to automatically be assigned to a contact record until verified. External Identity licenses have been purchased for the project.
After registered guests complete an onboarding process, a flow will create the appropriate account and contact records for the user.
Which three steps should an identity architect follow to implement the outlined requirements? Choose 3 answers

A. Enable "Allow customers and partners to self-register".
B. Select the "Configurable Self-Reg Page" option under Login & Registration.
C. Set jp an external login page and call Salesforce APIs for user creation.
D. Customize the self-registration Apex handler to temporarily associate the user to a shared single contact record.
E. Customize me self-registration Apex handler to create only the user record.

Answer: ABE

Explanation:
Enabling "Allow customers and partners to self-register" allows guests to create their own user accounts in the portal. Selecting the "Configurable Self-Reg Page" option allows the administrator to customize the
self-registration page to capture the required fields. Customizing the self-registration Apex handler to create
only the user record prevents the automatic creation of a contact record until verification. References: Enable Self-Registration, Customize Self-Registration

NEW QUESTION 31

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 33
Universal Container's (UC) is using Salesforce Experience Cloud site for its container wholesale business. The identity architect wants to an authentication provider for the new site.
Which two options should be utilized in creating an authentication provider? Choose 2 answers

A. A custom registration handier can be set.
B. A custom error URL can be set.
C. The default login user can be set.
D. The default authentication provider certificate can be set.

Answer: AB

Explanation:
An authentication provider is a configuration that allows users to log in to Salesforce using an external identity provider, such as Facebook, Google, or a custom one. When creating an authentication provider, two options that can be utilized are:

> A custom registration handler, which 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.

> A custom error URL, which is a URL that users are redirected to when an error occurs during the authentication process. References: Authentication Providers, Create an Authentication Provider

NEW QUESTION 34
Universal containers uses an Employee portal for their employees to collaborate. employees access the portal from their company's internal website via SSO. It is set up to work with Active Directory. What is the role of Active Directory in this scenario?

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

Answer: C

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

NEW QUESTION 36
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 39
A company with 15,000 employees is using Salesforce and would like to take the necessary steps to highlight or curb fraudulent activity.
Which tool should be used to track login data, such as the average number of logins, who logged in more than the average number of times and who logged in during non-business hours?

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

Answer: A

Explanation:
To track login data and highlight or curb fraudulent activity, the identity architect should use Login Forensics. Login Forensics is a tool that analyzes login history data and provides insights into user login patterns, such as average number of logins, login outliers, login anomalies, and login risk scores. Login Forensics can help identify suspicious or malicious login attempts and take preventive actions. References: Login Forensics, Login Forensics Implementation Guide

NEW QUESTION 44
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 fading?

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 45
IT security at Unversal Containers (UC) us 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 activity1. This can help prevent phishing scams and unauthorized access.
References: Salesforce Authenticator, Salesforce Authenticator: Mobile App Security Features, Salesforce Authenticator

NEW QUESTION 48
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, Linkedi
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 53
Northern Trail Outfitters (NTO) is planning to build a new customer service portal and wants to use passwordless login, allowing customers to login with a one-time passcode sent to them via email or SMS.
How should the quantity of required Identity Verification Credits be estimated?

A. Each community comes with 10,000 Identity Verification Credits per month and only customers with more than 10,000 logins a month should estimate additional SMS verifications needed.
B. Identity Verification Credits are consumed with each SMS (text message) sent and should be estimated based on the number of login verification challenges for SMS verification users.

C. Identity Verification Credits are consumed with each verification sent and should be estimated based on the number of loginsthat will incur a verification challenge.
D. Identity Verification Credits are a direct add-on license based on the number of existing member-based or login-based Community licenses.

Answer: B

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

NEW QUESTION 57
Universal Containers (UC) is rolling out its new Customer Identity and Access Management Solution built on top of its existing Salesforce instance. UC wants to allow customers to login using Facebook, Google, and other social sign-on providers.
How should this functionality be enabled for UC, assuming ail social sign-on providers support OpenID Connect?

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

Answer: A

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

NEW QUESTION 59
Universal Containers (UC) is building a custom Innovation platform on their Salesforce instance. The Innovation platform will be written completely in Apex and Visualforce and will use custom objects to store the Data. UC would like all users to be able to access the system without having to log in with Salesforce credentials. UC will utilize a third-party idp using SAML SSO. What is the optimal Salesforce licence type for all of the UC employees?

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

Answer: D

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

NEW QUESTION 64
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 : [Restri Access by IP Address]

NEW QUESTION 66

An identity architect is setting up an integration between Salesforce and a third-party system. The third-party system needs to authenticate to Salesforce and then make API calls against the REST API.

One of the requirements is that the solution needs to ensure the third party service providers connected app in Salesforce mini need for end user interaction and maximizes security.

Which OAuth flow should be used to fulfill the requirement?

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

Answer: A

Explanation:
JWT Bearer Flow allows the third-party system to authenticate to Salesforce using a digital certificate and a JSON Web Token (JWT) without any user interaction. It also provides a high level of security as it does not require sharing credentials or storing tokens. References: OAuth 2.0 JWT Bearer Token Flow

NEW QUESTION 67
Universal Containers (UC) is looking to purchase a third-party application as an Identity Provider. UC is looking to develop a business case for the purchase in general and has enlisted an Architect for advice. Which two capabilities of an Identity Provider should the Architect detail to help strengthen the business case?
Choose 2 answers

A. The Identity Provider can authenticate multiple applications.
B. The Identity Provider can authenticate multiple social media accounts.
C. The Identity provider can store credentials for multiple applications.
D. The Identity Provider can centralize enterprise password policy.

Answer: AD

Explanation:
The two capabilities of an identity provider that the architect should detail to help strengthen the business case are that the identity provider can authenticate multiple applications and that the identity provider can centralize enterprise password policy. These capabilities can provide benefits such as reducing login friction, improving user experience, enhancing security, and simplifying administration. Option B is not a good choice because the identity provider can authenticate multiple social media accounts may not be relevant for UC's business case, as it does not specify how UC will use social media for its identity management. Option C is not a good choice because the identity provider can store credentials for multiple applications may not be desirable or secure for UC's business case, as it may imply that the identity provider is using password vaulting or federation rather than single sign-on (SSO) or identity federation. References: Identity Management Concepts, [Single Sign-On Implementation Guide]

NEW QUESTION 69
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 wil be automatically created or updated in the other orgs based on the information from UC11. 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 74
Universal containers (UC) built a customer Community for customers to buy products, review orders, and manage their accounts. UC has provided three different options for customers to log in to the customer Community: salesforce, Google, and Facebook. Which two role combinations are represented by the systems in the scenario? Choose 2 answers

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

Answer: BD

Explanation:
The two role combinations that are represented by the systems in the scenario are Salesforce as the service provider and Google as the identity provider, and Salesforce as the service provider and Facebook as the identity provider. This means that Salesforce hosts the customer community app and relies on Google or Facebook to authenticate the users who log in with those options4. Therefore, option B and D are the correct answers.
References: Salesforce as Service Provider and Identity Provider for SSO

NEW QUESTION 79
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 83
Universal Containers is implementing Salesforce Identity to broker authentication from its enterprise single sign-on (SSO) solution through Salesforce to third party applications using SAML.
What rote does Salesforce Identity play in its relationship with the enterprise SSO system?

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

Answer: C

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

NEW QUESTION 86
Universal Containers (UC) is using Active Directory as its corporate identity provider and Salesforce as its CRM for customer care agents, who use SAML based sign sign-on to login to Salesforce. The default agent profile does not include the Manage User permission. UC wants to dynamically update the agent role and permission sets.
Which two mechanisms are used to provision agents with the appropriate permissions? Choose 2 answers

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

Answer: BD

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

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

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

NEW QUESTION 89
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 types2. 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 range3. 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 91
In an SP-Initiated SAML SSO setup where the user tries to access a resource on the Service Provider, What HTTP param should be used when submitting a SAML Request to the Idp to ensure the user is returned to the intended resourse after authentication?

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

Answer: B

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

NEW QUESTION 95
Universal Containers would like its customers to register and log in to a portal built on Salesforce Experience Cloud. Customers should be able to use their Facebook or LinkedIn credentials for ease of use.
Which three steps should an identity architect take to implement social sign-on? Choose 3 answers

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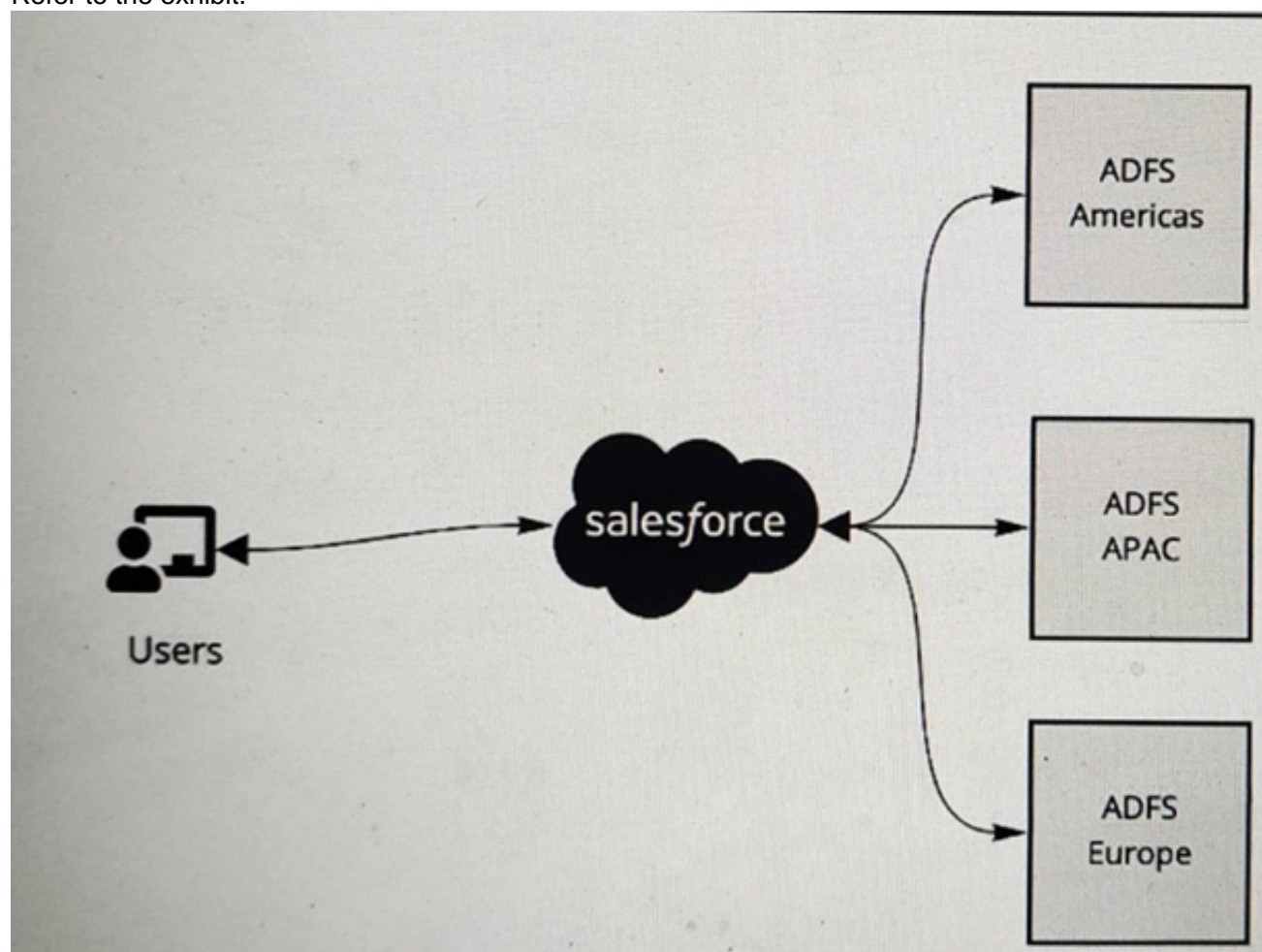
Answer: BCE

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

➤ Create authentication providers for both Facebook and LinkedIn. Authentication providers are configurations that enable users to authenticate with an external identity provider and access Salesforce resources. Salesforce provides predefined authentication providers for some common identity providers, such as Facebook and LinkedIn, which can be easily configured with minimal customization.

➤ Check "Facebook" and "LinkedIn" under Login Page Setup. Login Page Setup is a setting that allows administrators to customize the login page for Experience Cloud sites. By checking "Facebook" and "LinkedIn", the identity architect can enable social sign-on buttons for these identity providers on the login page.

➤ Update the default registration handlers to create and update users. Registration handlers are classes that implement the Auth.RegistrationHandler interface and define how to create or update users in Salesforce based on the information from the external identity provider. The identity architect can update the default registration handlers to link the user's social identity with their Salesforce identity and prevent duplicate accounts. References: Authentication Providers, Social Sign-On with Authentication Providers, Login Page Setup, Create a Custom Registration Handler

NEW QUESTION 99
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 federated 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 102
Northern Trail Outfitters (NTO) has a requirement to ensure all user logins include a single multi-factor authentication (MFA) prompt. Currently, users are allowed the choice to login with a username and password or via single sign-on against NTO's corporate Identity Provider, which includes built-in MFA.
Which configuration will meet this requirement?

A. Create and assign a permission set to all employees that includes "MFA for User Interface Logins."
B. Create a custom login flow that enforces MFA and assign it to a permission se
C. Then assign the permission set to all employees.
D. Enable "MFA for User Interface Logins" for your organization from Setup -> Identity Verification.
E. For all employee profiles, set the Session Level Required at Login to High Assurance and add the corporate identity provider to the High Assurance list for the org's Session Security Levels.

Answer: C

Explanation:
Enabling "MFA for User Interface Logins" for the organization is the simplest way to ensure that all user logins include a single MFA prompt. This setting applies to both direct logins and SSO logins, and overrides any other MFA settings at the profile or permission set level. References: Enable MFA for Direct User Logins, Everything You Need to Know About MFA Auto-Enablement and Enforcement

NEW QUESTION 104
Universal Containers (UC) has an existing e-commerce platform and is implementing a new customer community. They do not want to force customers to register on both applications due to concern over the customers experience. It is expected that 25% of the e-commerce customers will utilize the customer community .
The e-commerce platform is capable of generating SAML responses and has an existing
REST-ful API capable of managing users. How should UC create the identities of its e-commerce users with the customer community?

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

Answer: A

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

NEW QUESTION 107
Universal containers (UC) would like to enable SAML-BASED SSO for a salesforce partner community. UC has an existing ldap identity store and a third-party portal. They would like to use the existing portal as the primary site these users' access, but also want to allow seamless access to the partner community. What SSO flow should an architect recommend?

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

Answer: B

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

NEW QUESTION 112
Universal Containers allows employees to use a mobile device to access Salesforce for daily operations using a hybrid mobile app. This app uses Mobile software development kits (SDK), leverages refresh token to regenerate access token when required and is distributed as a private app.
The chief security officer is rolling out an org wide compliance policy to enforce re-verification of devices if an employee has not logged in from that device in the last week.
Which connected app setting should be leveraged to comply with this policy change?

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

Answer: B

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

NEW QUESTION 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: Connec Apps Overview 4: Identity Providers and Service Providers - Salesforce 5: Identity Connect Overview

NEW QUESTION 116
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 124
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 130
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 131
Universal Containers (UC) has a Customer Community that uses Facebook for of authentication. UC would like to ensure that changes in the Facebook profile are 65. reflected on the appropriate Customer Community user. How can this requirement be met?

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

Answer: D

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

➢ SAML Just-In-Time Provisioning is used to create or update users in Salesforce based on SAML assertions from an identity provider3. Facebook does not support SAML as an identity provider.

➢ The Signed Request is a parameter that contains information about the user who is logging in to Salesforce via Facebook. It does not contain the user's profile information, such as name, email, or photo.

➢ A scheduled job that calls out to Facebook on a nightly basis would not reflect the changes in the Facebook profile in real time, as the requirement states. It would also require storing the user's Facebook access token and making API calls to Facebook, which could be inefficient and insecure. References: Set Up Social Sign-On, Configure a Facebook Authentication Provider, SAML Just-in-Time Provisioning, [Facebook as a SAML Identity Provider], [Facebook Login for Apps - Signed Request], [Facebook Login for Apps - Access Tokens], [Facebook Graph API - User]

NEW QUESTION 133
Universal Containers (UC) uses Salesforce for its customer service agents. UC has a proprietary system for order tracking which supports Security Assertion Markup Language (SAML) based single sign-on. The VP of customer service wants to ensure only active Salesforce users should be able to access the order tracking system which is only visible within Salesforce.
What should be done to fulfill the requirement? Choose 2 answers

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

Answer: AD

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

➢ Setup Salesforce as an identity provider (IdP) for order tracking. An IdP is the system that performs authentication and passes the user's identity and authorization level to the SP, which trusts the IdP and authorizes the user to access the requested resource. To set up Salesforce as an IdP, you need to enable the Identity Provider feature, download the IdP certificate, and configure the SAML settings.

➢ Setup order tracking as a Canvas app in Salesforce to POST IdP initiated SAML assertion. A Canvas app is an application that can be embedded within a Salesforce page and interact with Salesforce data and APIs. To set up order tracking as a Canvas app, you need to create a connected app for order tracking in Salesforce, enable SAML and configure the SAML settings, such as the entity ID, ACS URL, and subject type. You also need to enable IdP initiated SAML assertion POST binding for the connected app, which allows Salesforce to initiate the SSO process by sending a SAML assertion to order tracking.
References:
➢ [SAML Single Sign-On]
➢ [Set Up Your Domain as an Identity Provider]
➢ [Canvas Apps]
➢ [Create a Connected App for Your Canvas App]
➢ [IdP Initiated SAML Assertion POST Binding]

NEW QUESTION 136
Universal containers wants to set up SSO for a selected group of users to access external applications from salesforce through App launcher. Which three steps must be completed in salesforce to accomplish the goal?

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

Answer: ABC

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

➢ Associate user profiles with the connected apps. A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect3. To access a connected app, users must have the appropriate permissions assigned to them, either through their profile or a permission set4. UC can associate user profiles with the connected apps to control which users can access which apps.

➢ Complete My Domain and identity provider setup. My Domain is a feature that lets UC create a custom domain name for their Salesforce org. It is required for setting up SSO with external identity providers. An identity provider is a trusted system that authenticates users for other service providers. UC must set up an identity provider that supports SSO protocols such as SAML or OpenID Connect and configure it to communicate with Salesforce.

➢ Create connected apps for the external applications. UC must create connected apps for each external application that they want to access from Salesforce through App Launcher. A connected app defines the attributes of the external application, such as its name, logo, description, and callback URL4. It also specifies the SSO protocol and settings that are used to authenticate users and grant access tokens4.

➢ References: Learn About Connected Apps, Create a Connected App, [Set Up My Domain], Single Sign-On, [Identity Providers and Service Providers]

NEW QUESTION 140
Northern Trail Outfitters is implementing a business-to-business (B2B) collaboration site using Salesforce Experience Cloud. The partners will authenticate with an existing identity provider and the solution will utilize Security Assertion Markup Language (SAML) to provide single sign-on to Salesforce. Delegated administration will be used in the Expenence Cloud site to allow the partners to administer their users' access.

How should a partner identity be provisioned in Salesforce for this solution?

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

Answer: C

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

NEW QUESTION 143
Universal containers (UC) has implemented a multi-org strategy and would like to centralize the management of their salesforce user profiles. What should the architect recommend to allow salesforce profiles to be managed from a central system of record?

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

Answer: A

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

NEW QUESTION 145
Universal Containers (UC) has Active Directory (AD) as their enterprise identity store and would like to use it for Salesforce user authentication. UC expects to synchronize user data between Salesforce and AD and Assign the appropriate Profile and Permission Sets based on AD group membership. What would be the optimal way to implement SSO?

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

Answer: D

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

NEW QUESTION 148
Universal containers (UC) would like to enable SSO between their existing Active Directory infrastructure and salesforce. The it team prefers to manage all users in Active Directory and would like to avoid doing any initial setup of users in salesforce directly, including the correct assignment of profiles, roles and groups. Which two optimal solutions should UC use to provision users in salesforce? Choose 2 answers

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

Answer: BD

Explanation:
To provision users in Salesforce from Active Directory without doing any initial setup of users in Salesforce, UC can use an app exchange product or Identity Connect. An app exchange product is a third-party application that can synchronize users and groups from Active Directory to Salesforce using a web-based interface1. Identity Connect is a desktop application that can synchronize users and groups from Active Directory to Salesforce using a graphical user interface2. Both solutions can also map Active Directory attributes to Salesforce fields and assign profiles, roles, and permission sets to users12.
References: Active Directory Integration with Salesforce, Identity Connect

NEW QUESTION 153
Universal Containers want users to be able to log in to the Salesforce mobile app with their Active Directory password. Employees are unable to use mobile VPN. Which two options should an identity architect recommend to meet the requirement? Choose 2 answers

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

Answer: AD

Explanation:
Active Directory Password Sync Plugin allows users to log in to Salesforce with their Active Directory password without using a VPN. Salesforce Identity Connect synchronizes users and groups between Active Directory and Salesforce and enables single sign-on. References: Active Directory Password Sync Plugin, Salesforce Identity Connect

NEW QUESTION 157
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 161
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 162
A consumer products company uses Salesforce to maintain consumer information, including orders. The company implemented a portal solution using Salesforce Experience Cloud for its consumers where the consumers can log in using their credentials. The company is considering allowing users to login with their Facebook or LinkedIn credentials.
Once enabled, what role will Salesforce play?

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

Answer: B

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

NEW QUESTION 165
Universal containers (UC) wants to implement a partner community. As part of their implementation, UC would like to modify both the Forgot password and change password experience with custom branding for their partner community users. Which 2 actions should an architect recommend to UC? Choose 2 answers

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

Answer: BC

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

NEW QUESTION 167
Northern Trail Outfitters want to allow its consumer to self-register on it business-to-consumer (B2C) portal that is built on Experience Cloud. The identity architect has recommended to use Person Accounts.
Which three steps need to be configured to enable self-registration using person accounts? Choose 3 answers

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

Answer: ACD

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

➤ Enable access to person and business account record types under Public Access Settings. Public Access Settings are settings that control the access level and permissions for guest users on Experience Cloud sites. By enabling access to person and business account record types, the identity architect can allow guest users to create person accounts or business accounts when they self-register on the portal.

➤ Under Login and Registration settings, ensure that the default account field is empty. Login and Registration settings are settings that control the login and registration options for Experience Cloud sites. By ensuring that the default account field is empty, the identity architect can prevent guest users from being associated with a default account when they self-register on the portal.

➤ Contact Salesforce Support to enable person accounts. Person accounts are a type of account that combines an individual consumer with an account record. Person accounts are not enabled by default in Salesforce orgs and require contacting Salesforce Support to enable them. References: Public Access Settings, Login and Registration Settings, Person Accounts

NEW QUESTION 168
Universal Containers (UC) uses Global Shipping (GS) as one of their shipping vendors. Regional leads of GS need access to UC's Salesforce instance for reporting damage of goods using Cases. The regional leads also need access to dashboards to keep track of regional shipping KPIs. UC internally uses a third-party cloud analytics tool for capacity planning and UC decided to provide access to this tool to a subset of GS employees. In addition to regional leads, the GS capacity planning team would benefit from access to this tool. To access the analytics tool, UC IT has set up Salesforce as the Identity provider for Internal users and would like to follow the same approach for the GS users as well. What are the most appropriate license types for GS Tregional Leads and the GS Capacity Planners? Choose 2 Answers

A. Customer Community Plus license for GS Regional Leads and External Identity for GS Capacity Planners.
B. Customer Community Plus license for GS Regional Leads and Customer Community license for GS Capacity Planners.
C. Identity License for GS Regional Leads and External Identity license for GS capacity Planners.
D. Customer Community license for GS Regional Leads and Identity license for GS Capacity Planners.

Answer: AD

Explanation:
The most appropriate license types for GS regional leads and the GS capacity planners are:

➤ Customer Community Plus license for GS regional leads. This license type allows external users, such as customers or partners, to access standard Salesforce objects, such as cases and dashboards, and custom objects in a community. This license type also supports role hierarchy, sharing rules, and reports. This license type is suitable for GS regional leads who need to report damage of goods using cases and access dashboards to track regional shipping KPIs.

➤ External Identity license for GS capacity planners. This license type allows external users to access a limited set of standard Salesforce objects, such as contacts and documents, and custom objects in a community. This license type also supports identity features, such as single sign-on (SSO) and social sign-on. This license type is suitable for GS capacity planners who need to access the third-party cloud analytics tool using Salesforce as the identity provider.
The other options are not appropriate license types for this scenario. Customer Community license for GS capacity planners would not allow them to access the third-party cloud analytics tool using SSO, as this license type does not support identity features. Identity license for GS regional leads would not allow them to access cases and dashboards in the community, as this license type does not support standard Salesforce objects. References: [Customer Community Plus Licenses], [External Identity Licenses], [Customer Community Licenses], [Identity Licenses]

NEW QUESTION 173
Northern Trail Outfitters wants to implement a partner community. Active community users will need to review and accept the community rules, and update key contact information for each community member before their annual partner event.
Which approach will meet this requirement?

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

Answer: C

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

NEW QUESTION 174
Universal Containers is creating a mobile application that will be secured by Salesforce Identity using the OAuth 2.0 user-agent flow (this flow uses the OAuth 2.0 implicit grant type).
Which three OAuth concepts apply to this flow? Choose 3 answers

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

Answer: AE

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

NEW QUESTION 177
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 181
Universal Containers (UC) implemented SSO to a third-party system for their Salesforce users to access the App Launcher. UC enabled "User Provisioning" on the Connected App so that changes to user accounts can be synched between Salesforce and the third-party system. However, UC quickly notices that changes to user roles in Salesforce are not getting synched to the third-party system. What is the most likely reason for this behavior?

A. User Provisioning for Connected Apps does not support role sync.
B. Required operation(s) was not mapped in User Provisioning Settings.
C. The Approval queue for User Provisioning Requests is unmonitored.
D. Salesforce roles have more than three levels in the role hierarchy.

Answer: B

Explanation:
User Provisioning for Connected Apps supports role sync, but the required operation(s) must be mapped in User Provisioning Settings. According to the Salesforce documentation1, "To provision roles, map the Role operation to a field in the connected app. The field must contain the role's unique name." Therefore, option B is the correct answer.
References: Salesforce Documentation

NEW QUESTION 186
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 190

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 191

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 196

customer service representatives at Universal containers (UC) are complaining that whenever they click on links to case records and are asked to login with SAML SSO, they are being redirected to the salesforce home tab and not the specific case record. What item should an architect advise the identity team at UC to investigate first?

A. My domain is configured and active within salesforce.
B. The salesforce SSO settings are using http post
C. The identity provider is correctly preserving the Relay state
D. The users have the correct Federation ID within salesforce.

Answer: C

Explanation:
The identity provider must correctly preserve the Relay state in order to redirect the user to the specific case record after login with SAML SSO. According to the Salesforce documentation3, "The RelayState parameter is used by SAML to indicate where the user should be redirected after they've been authenticated by the identity provider." Therefore, option C is the correct answer. References: Salesforce Documentation

NEW QUESTION 200

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 risks 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 service and Salesforce?

A. Require the use of Salesforce security tokens on passwords.
B. Enforce mutual authentication between systems using SSL.
C. Include Client Id and Client Secret in the login header callout.
D. Set up a proxy service for the login service in the DMZ.
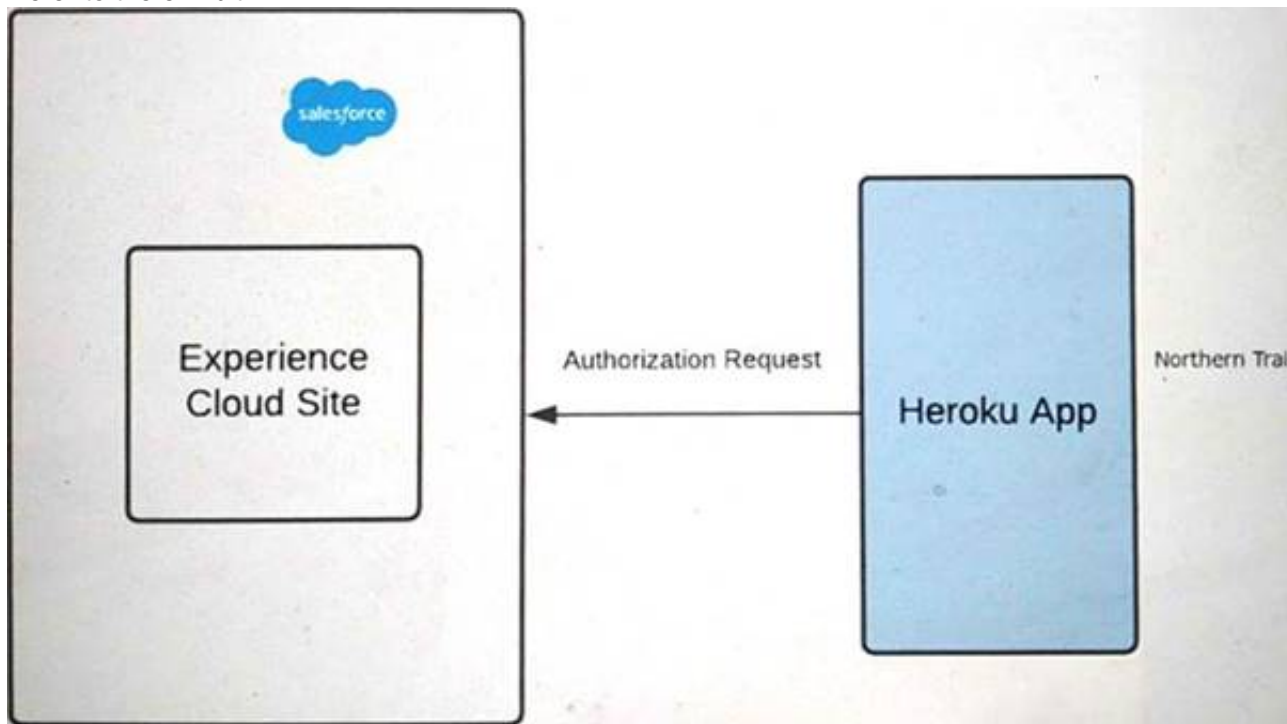
Answer: B

Explanation:
To enable a trusted connection between the login service and Salesforce, an architect should enforce mutual authentication between systems using SSL. Mutual authentication, also known as two-way SSL or client certificate authentication, is a process in which both parties in a communication exchange certificates to verify their identities7. This mechanism ensures that only authorized systems can access each other's resources and prevents unauthorized access or spoofing attacks8. To use mutual authentication with delegated authentication you need to do the following steps9:

⟩ Generate a self-signed certificate in Salesforce and download it.

⟩ Import the certificate into your login service's truststore.

⟩ Configure your login service to require client certificates for incoming requests.

⟩ Generate a certificate for your login service and export it.

⟩ Import the certificate into Salesforce's certificate and key management tool.

> Enable mutual authentication for your login service's endpoint URL in Salesforce. References:

> Mutual Authentication

> Mutual Authentication Overview

> Set Up Mutual Authentication

NEW QUESTION 204

Refer to the exhibit.

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

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

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

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

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

Answer: D

Explanation:

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

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

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

> OAuth 2.0

> OAuth 2.0 Web Server Authentication Flow

> Connected Apps

> Create a Connected App

> Experience ID

> Authorize Apps with OAuth

NEW QUESTION 207

......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

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

* Identity-and-Access-Management-Architect Questions and Answers Updated Frequently

* Identity-and-Access-Management-Architect Practice Questions Verified by Expert Senior Certified Staff

* Identity-and-Access-Management-Architect Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* Identity-and-Access-Management-Architect Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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