Identity-and-Access-Management-Architect Dumps

Salesforce Certified Identity and Access Management Architect (SU23)

https://www.certleader.com/Identity-and-Access-Management-Architect-dumps.html
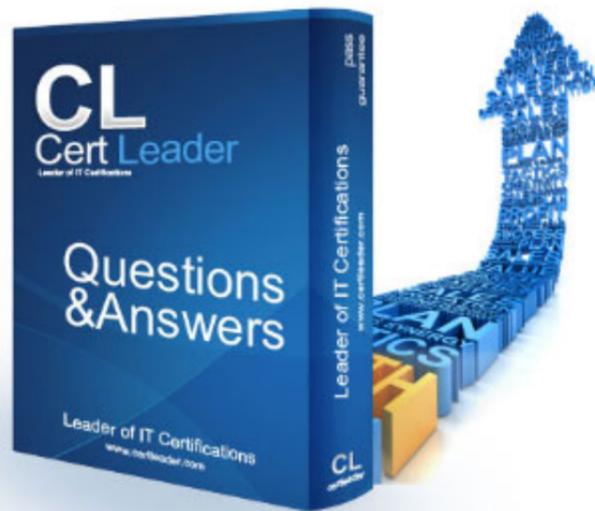
NEW QUESTION 1
Which three are features of federated Single sign-on solutions? Choose 3 Answers

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

Answer: ADE

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

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

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

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

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

NEW QUESTION 2
Universal containers (UC) is setting up Delegated Authentication to allow employees to log in using their corporate credentials. UC's security team is concerned about the risk of exposing the corporate login service on the Internet and has asked that a reliable trust mechanism be put in place between the login service and salesforce. What mechanism should an architect put in place to enable a trusted connection between the login services and salesforce?

A. Include client ID and client secret in the login header callout.
B. Set up a proxy server for the login service in the DMZ.
C. Require the use of Salesforce security Tokens on password.
D. Enforce mutual Authentication between systems using SSL.

Answer: D

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

NEW QUESTION 3
Universal containers want to build a custom mobile app connecting to salesforce using Oauth, and would like to restrict the types of resources mobile users can access. What Oauth feature of Salesforce should be used to achieve the goal?

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

Answer: D

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

NEW QUESTION 4
Universal Containers (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 5
Universal Containers is considering using Delegated Authentication as the sole means of Authenticating of Salesforce users. A Salesforce Architect has been brought in to assist with the implementation. What two risks Should the Architect point out? Choose 2 answers

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

Answer: BC

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

≫ UC will be required to develop and support a custom SOAP web service. Delegated authentication is a feature that allows Salesforce to delegate the authentication process to an external service by making a SOAP callout to a web service that verifies the user's credentials. This feature requires UC to develop and support a custom SOAP web service that can accept and validate the user's username and password, and return a boolean value to indicate whether the authentication is successful or not. This could increase complexity and cost for UC, as they need to write custom code and maintain the web service.

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

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

NEW QUESTION 6
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 7
Northern Trail Outfitters (NTO) uses Salesforce for Sales Opportunity Management. Okta was recently brought in to Just-in-Time (JIT) provision and authenticate NTO users to applications. Salesforce users also use Okta to authorize a Forecasting web application to access Salesforce records on their behalf.
Which two roles are being performed by Salesforce? Choose 2 answers

A. SAML Identity Provider
B. OAuth Client
C. OAuth Resource Server
D. SAML Service Provider

Answer: BD

Explanation:
Salesforce acts as an OAuth client when it uses Okta to authorize a Forecasting web application to access
Salesforce records on behalf of the user. Salesforce acts as a SAML service provider when it accepts SAML assertions from Okta to authenticate NTO users.
References: OAuth 2.0 Web Server Authentication
Flow, SAML Single Sign-On Overview

NEW QUESTION 8
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 9
Universal containers wants to implement single Sign-on for a salesforce org using an external identity provider and corporate identity store. What type of Authentication flow is required to support deep linking?

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

Answer: C

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

NEW QUESTION 10
Universal containers (UC) has implemented SAML SSO to enable seamless access across multiple applications. UC has regional salesforce orgs and wants it's users to be able to access them from their main Salesforce org seamless. Which action should an architect recommend?

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

Answer: B

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

NEW QUESTION 10
Universal Containers (UC) wants to provide single sign-on (SSO) for a business-to-consumer (B2C) application using Salesforce Identity.
Which Salesforce license should UC utilize to implement this use case?

A. Identity Only
B. Salesforce Platform
C. External Identity
D. Partner Community

Answer: C

Explanation:
External Identity is the license that enables SSO for B2C applications using Salesforce Identity. It also provides self-registration, social sign-on, and user profile management features. References: Certification - Identity and Access Management Architect - Trailhead

NEW QUESTION 12
Universal containers (UC) uses an internal company portal for their employees to collaborate. UC decides to use salesforce ideas and provide the ability for employees to post ideas from the company portal. They use SAML-BASED SSO to get into the company portal and would like to leverage it to access salesforce. Most of the users don't exist in salesforce and they would like the user records created in salesforce communities the first time they try to access salesforce. What recommendation should an architect make to meet this requirement?

A. Use on-the-fly provisioning

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

Answer: B

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

NEW QUESTION 15
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 16
Northern Trail Outfitters (NTO) wants to improve its engagement with existing customers to boost customer loyalty. To get a better understanding of its customers, NTO establishes a single customer view including their buying behaviors, channel preferences and purchasing history. All of this information exists but is spread across different systems and formats.
NTO has decided to use Salesforce as the platform to build a 360 degree view. The company already uses Microsoft Active Directory (AD) to manage its users and company assets.
What should an Identity Architect do to provision, deprovision and authenticate users?

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

Answer: D

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

NEW QUESTION 17
Universal Containers (UC) uses Salesforce to allow customers to keep track of the order status. The customers can log in to Salesforce using external authentication providers, such as Facebook and Google. UC is also leveraging the App Launcher to let customers access an of platform application for generating shipping labels. The label generator application uses OAuth to provide users access. What license type should an Architect recommend for the customers?

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

Answer: D

Explanation:
D is correct because External Identity license is designed for customers who need to log in to Salesforce using external authentication providers, such as Facebook and Google. External Identity license also supports App Launcher, which allows customers to access other applications from Salesforce using OAuth or OpenID Connect .
A is incorrect because Customer Community license is designed for customers who need to access data and records in Salesforce, such as cases, accounts, and contacts. Customer Community license does not support App Launcher or external authentication providers.
B is incorrect because Identity license is designed for employees who need to access multiple applications from Salesforce using SSO and App Launcher. Identity license does not support external authentication providers or customer data access.

C is incorrect because Customer Community Plus license is designed for customers who need to access data and records in Salesforce, as well as collaborate with other customers and partners. Customer Community Plus license does not support App Launcher or external authentication providers.
References: : Salesforce Licensing Module - Trailhead : Free Salesforce
Identity-and-Access-Management-Architect Questions … : Salesforce Licensing Module - Trailhead : Salesforce Licensing Module - Trailhead : Salesforce Licensing Module - Trailhead

NEW QUESTION 22
Which tool should be used to track login data, such as the average number of logins, who logged in more than the average number of times and who logged in during non-business hours?

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

Answer: D

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

NEW QUESTION 25
What are three capabilities of Delegated Authentication? Choose 3 answers

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

Answer: BCE

Explanation:
The three capabilities of delegated authentication are:

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

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

 It can connect to REST services. REST services are web services that use HTTP methods to access or manipulate resources on a server. REST services can be used for delegated authentication by creating a custom login page that makes a REST callout to an external service that verifies the user's credentials. This approach requires custom code and configuration, but it provides more flexibility and control over the authentication process.
The other options are not capabilities of delegated authentication. Delegated authentication cannot be assigned by custom permissions or profiles. Custom permissions are settings that can be used in Apex code or validation rules to check whether a user has access to a custom feature or functionality. Custom permissions cannot be used to enable delegated authentication for users. Profiles are collections of settings and permissions that determine what users can do in Salesforce. Profiles cannot be used to enable delegated authentication for users, as this feature is controlled by permission sets. References: [Delegated Authentication], [Permission Sets], [Enable 'Delegated Authentication'], [REST Services], [Custom Login Page for Delegated Authentication], [Custom Permissions], [Profiles]

NEW QUESTION 30
A financial services company uses Salesforce and has a compliance requirement to track information about devices from which users log in. Also, a Salesforce Security Administrator needs to have the ability to revoke the device from which users log in.
What should be used to fulfill this requirement?

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

Answer: B

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

NEW QUESTION 35
A global company has built an external application that uses data from its Salesforce org via an OAuth 2.0 authorization flow. Upon logout, the existing Salesforce OAuth token must be invalidated.
Which action will accomplish this?

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

D. Enable Single Logout with a secure logout URL.

Answer: C

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

NEW QUESTION 38
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 42
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 44
Universal Containers built a custom mobile app for their field reps to create orders in Salesforce. OAuth is used for authenticating mobile users. The app is built in such a way that when a user session expires after Initial login, a new access token is obtained automatically without forcing the user to log in again. While that improved the field reps' productivity, UC realized that they need a "logout" feature.
What should the logout function perform in this scenario, where user sessions are refreshed automatically?

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

Answer: A

Explanation:
The refresh token is used to obtain a new access token when the previous one expires. To revoke the user session, the logout function should invoke the revocation URL and pass the refresh token as a parameter. This will invalidate both the refresh token and the access token, and prevent the user from accessing Salesforce without logging in again2.
References:
> Certification Exam Guide
> Revoke OAuth Tokens

NEW QUESTION 46
Universal Containers wants to allow its customers to log in to its Experience Cloud via a third-party authentication provider that supports only the OAuth protocol.
What should an identity architect do to fulfill this requirement?

A. Contact Salesforce Support and enable delegate single sign-on.
B. Create a custom external authentication provider.

C. Use certificate-based authentication.
D. Configure OpenID Connect authentication provider.

Answer: B

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

NEW QUESTION 47
Universal Containers (UC) wants its closed Won opportunities to be synced to a Data warehouse in near real time. UC has implemented Outbound Message to enable near real-time data sync. UC wants to ensure that communication between Salesforce and Target System is secure. What certificate is sent along with the Outbound Message?

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

Answer: C

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

NEW QUESTION 49
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 53
The security team at Universal containers(UC) has identified exporting reports as a high-risk action and would like to require users to be logged into salesforce with their active directory (AD) credentials when doing so. For all other uses of Salesforce, Users should be allowed to use AD credentials or salesforce credentials. What solution should be recommended to prevent exporting reports except when logged in using AD credentials while maintaining the ability to view reports when logged in with salesforce credentials?

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

Answer: B

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

NEW QUESTION 56
Universal Containers (UC) is looking to build a Canvas app and wants to use the corresponding Connected App to control where the app is visible. Which two options are correct in regards to where the app can be made visible under the Connected App setting for the Canvas app? Choose 2 answers

A. As part of the body of a Salesforce Knowledge article.
B. In the mobile navigation menu on Salesforce for Android.
C. The sidebar of a Salesforce Console as a console component.
D. Included in the Call Control Tool that's part of Open CTI.

Answer: CD

Explanation:
The sidebar of a Salesforce Console as a console component and included in the Call Control Tool that's part of Open CTI are two options that are correct in regards to where the app can be made visible under the connected app settings for the Canvas app. A Canvas app is an external application that can be embedded within Salesforce using an iframe. A connected app is an application that integrates with Salesforce using APIs and uses OAuth as the authentication protocol. You can control where a Canvas app can be displayed in Salesforce by configuring the locations in the connected app settings. The sidebar of a Salesforce Console as a console component is a valid location for a Canvas app because it allows you to display the app as a collapsible panel on the side of any console app. Included in the Call Control Tool that's part of Open CTI is a valid location for a Canvas app because it allows you to display the app as part of the softphone panel that integrates with your telephony system. As part of the body of a Salesforce Knowledge article is not a valid location for a Canvas app because it is not supported by the connected app settings. In the mobile navigation menu on Salesforce for Android is not a valid location for a Canvas app because it is not supported by the connected app settings. References: : [Canvas Developer Guide] : [Connected Apps Overview] : [Add or Remove Components from Your Console Apps] : [Open CTI Developer Guide]

NEW QUESTION 61
What item should an Architect consider when designing a Delegated Authentication implementation?

A. The Web service should be secured with TLS using Salesforce trusted certificates.
B. The Web service should be able to accept one to four input method parameters.
C. The web service should use the Salesforce Federation ID to identify the user.
D. The Web service should implement a custom password decryption method.

Answer: A

Explanation:
The web service that is used for delegated authentication should be secured with TLS using Salesforce trusted certificates4. This ensures that the communication between Salesforce and the external authentication method is encrypted and authenticated. The other options are not relevant for designing a delegated authentication implementation. The web service does not need to accept one to four input method parameters, as it can accept any number of parameters as long as they are wrapped in a SOAP envelope5. The web service does not need to use the Salesforce Federation ID to identify the user, as it can use any identifier that is unique and consistent across systems6. The web service does not need to implement a custom password decryption method, as it can use any encryption or hashing algorithm that is supported by both systems7. References: Delegated Authentication, Enable 'Delegated Authentication', Delegated Authentication Flow in Salesforce, FAQs fo Delegated Authentication

NEW QUESTION 65
An organization has a central cloud-based Identity and Access Management (IAM) Service for authentication and user management, which must be utilized by all applications as follows:
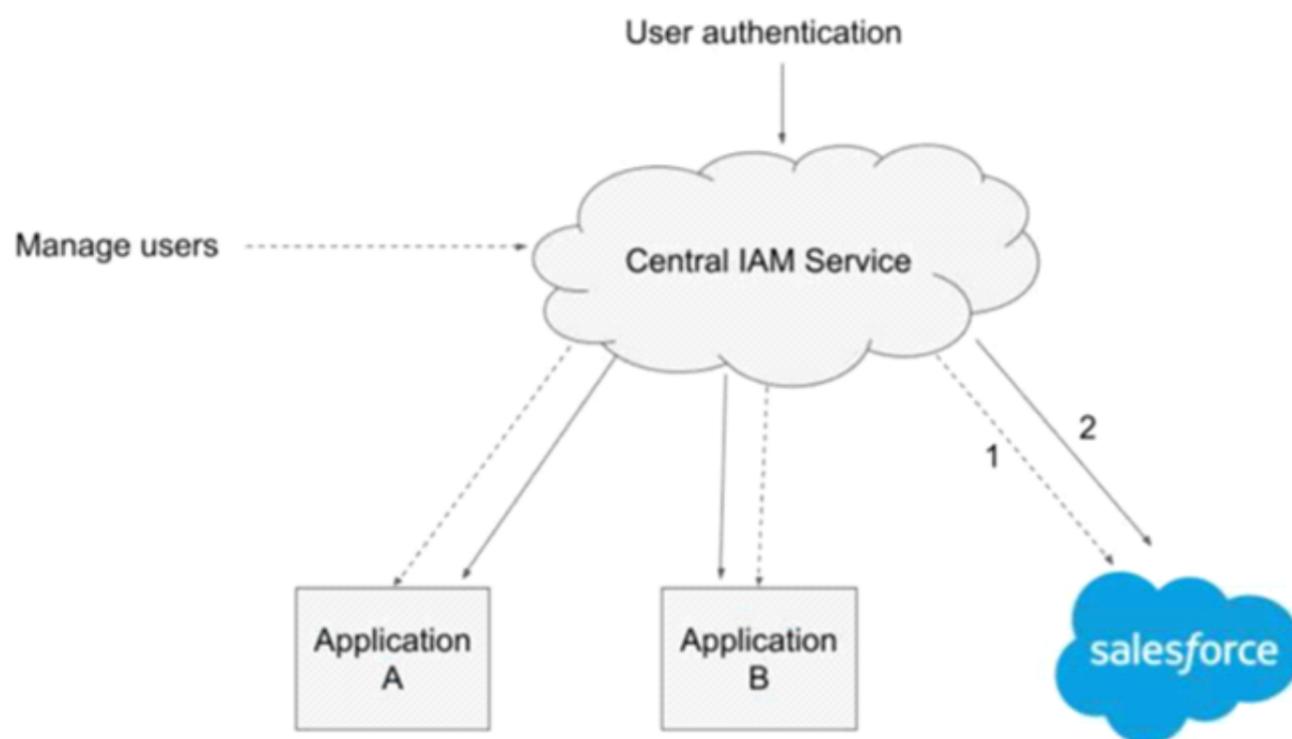
1 - Change of a user status in the central IAM Service triggers provisioning or deprovisioning in the integrated cloud applications.
2 - Security Assertion Markup Language single sign-on (SSO) is used to facilitate access for users authenticated at identity provider (Central IAM Service).
Which approach should an IAM architect implement on Salesforce Sales Cloud to meet the requirements?

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

Answer: A

Explanation:
To meet the requirements of using a central cloud-based IAM service for authentication and user management, the IAM architect should implement Salesforce Sales Cloud as a SAML service provider and enable SCIM for provisioning and deprovisioning of users. SAML is a protocol that allows users to authenticate and

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

NEW QUESTION 68
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 70
Universal Containers (UC) has built a custom token-based Two-factor authentication (2FA) system for their existing on-premise applications. They are now implementing Salesforce and would like to enable a
Two-factor login process for it, as well. What is the recommended solution as Architect should consider?

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

Answer: D

Explanation:
The recommended solution for UC to enable a two-factor login process for Salesforce and their existing
on-premise applications is to replace the custom 2FA system with Salesforce 2FA for on-premise applications and Salesforce. Salesforce 2FA is a feature that requires users to verify their identity with a second factor, such as a verification code or a mobile app, after entering their username and password. Salesforce 2FA can be enabled for both Salesforce and on-premise applications by using one of the following methods:
» Use Salesforce Authenticator, a mobile app that generates verification codes or sends push notifications to users' devices.
» Use a third-party authenticator app, such as Google Authenticator or Microsoft Authenticator, that generates verification codes based on a shared secret key.
» Use a verification code sent by email or SMS to users' registered email address or phone number.
» Use a U2F security key, such as YubiKey, that plugs into users' devices and provides a physical token. By replacing the custom 2FA system with Salesforce 2FA, UC can benefit from the following advantages:
» Improved security and compliance by using a standard and proven 2FA solution that protects against
phishing, credential theft, and brute force attacks.
» Reduced complexity and cost by eliminating the need to maintain a custom 2FA system and integrating it with Salesforce.
» Enhanced user experience and convenience by providing multiple options for verifying identity and allowing users to remember trusted devices or browsers. The other options are not recommended solutions for this scenario. Using the custom 2FA system for
on-premise applications and native 2FA for Salesforce would create inconsistency and confusion for users who have to use different methods of verification for different applications. Replacing the custom 2FA system with an AppExchange app that supports on-premise applications and Salesforce would require UC to find an app that meets their specific needs and pay for its license and maintenance. Using custom login flows to connect to the existing custom 2FA system for use in Salesforce would require UC to write custom code and logic to invoke the custom 2FA system from Salesforce, which could introduce security and performance issues. References: [Two-Factor Authentication], [Salesforce Authenticator], [Third-Party Authenticator Apps], [Verification Code via Email or SMS], [U2F Security Keys], [Custom Login Flows]

NEW QUESTION 72
Universal Containers (UC) wants to build a mobile application that twill be making calls to the Salesforce REST API. UC's Salesforce implementation relies heavily on custom objects and custom Apex code. UC does not want its users to have to enter credentials every time they use the app. Which two scope values should an Architect recommend to UC? Choose 2 answers.

A. Custom_permissions
B. Api
C. Refresh_token
D. Full

Answer: BC

Explanation:
The two scope values that an architect should recommend to UC are api and refresh_token. The api scope allows the app to access the Salesforce REST API and use custom objects and custom Apex code. The refresh_token scope allows the app to obtain a refresh token that can be used to get new access tokens without requiring the user to re-enter credentials. Option A is not a good choice because the custom_permissions scope allows the app to access custom permissions in

Salesforce, but it does not affect how the app can access the REST API or avoid user re-authentication. Option D is not a good choice because the full scope allows the app to access all data accessible by the user, including the web UI and the API, but it may be unnecessary or insecure for UC's requirement.
References: OAuth 2.0 Web Server Authentication Flow, Digging Deeper int OAuth 2.0 on Force.com

NEW QUESTION 76
Universal Containers wants to secure its Salesforce APIs by using an existing Security Assertion Markup Language (SAML) configuration supports the company's single sign-on process to Salesforce,
Which Salesforce OAuth authorization flow should be used?

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

Answer: A

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

NEW QUESTION 81
Universal containers (UC) has multiple salesforce orgs and would like to use a single identity provider to access all of their orgs. How should UC'S architect enable this behavior?

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

Answer: C

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

NEW QUESTION 86
Universal containers (UC) has implemented SAML -based single Sign-on for their salesforce application. UC is using PingFederate as the Identity provider. To access salesforce, Users usually navigate to a bookmarked link to my domain URL. What type of single Sign-on is this?

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

Answer: A

Explanation:
The type of single sign-on that UC is using is SP-initiated, which means that the service provider (Salesforce) initiates the SSO process by sending a SAML request to the identity provider (PingFederate) when the user navigates to the My Domain URL3. Therefore, option A is the correct answer. References: SAML SSO with Salesforce as the Service Provider

NEW QUESTION 89
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 the recommended best practices for using Oauth flows in this scenario? Choose 2 answers

A. Oauth refresh token flow
B. Oauth SAML bearer assertion flow
C. Oauthjwt bearer token flow
D. Oauth Username-password flow

Answer: AC

Explanation:
OAuth refresh token flow and OAuth JWT bearer token flow are the recommended best practices for using OAuth flows in this scenario. These flows are suitable for server-to-server integration scenarios where the client application needs to access Salesforce resources on behalf of a user. The OAuth refresh token flow allows the client application to obtain a long-lived refresh token that can be used to request new access tokens without requiring user interaction. The OAuth JWT bearer token flow allows the client application to use a JSON Web Token (JWT) to assert its identity and request an access token. Both flows provide a secure and efficient way to integrate with Salesforce and the reward calculation system. OAuth SAML bearer assertion flow is not a recommended best practice for using OAuth flows in this scenario because it requires the client application to obtain a SAML assertion from an identity provider, which adds an extra layer of complexity and dependency. OAuth username-password flow is not a recommended best practice for using OAuth flows in this scenario because it requires the client application to store the user's credentials, which poses a security risk and does not support two-factor authentication. References: : [Which OAuth Flow to Use] :

[Digging Deeper into OAuth 2.0 on Force.com] : [OAuth 2.0 JWT Bearer Token Flow] : [OAuth 2.0 SAML Bearer Assertion Flow] : [OAuth 2.0 Username-Password Flow]

NEW QUESTION 93
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 (UC) has an existing Salesforce org configured for SP-Initiated SAML SSO with their Idp. A second Salesforce org is being introduced into the environment and the IT team would like to ensure they can use the same Idp for new org. What action should the IT team take while implementing the second org?

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

Answer: B

Explanation:
The Entity ID is a unique identifier for a service provider or an identity provider in SAML SSO. It is used to differentiate between different service providers or identity providers that may share the same issuer or login URL. In Salesforce, the Entity ID is automatically generated based on the organization ID and can be viewed in the Single Sign-On Settings page1. If you have a custom domain set up, you can use https:// [customDomain].my.salesforce.com as the Entity ID2. If you want to use the same IdP for two Salesforce orgs, you need to use different Entity IDs for each org, otherwise the IdP will not be able to distinguish them and may send incorrect assertions. You can also use different certificates, issuers, or login URLs for each org, but using different Entity IDs is the simplest and recommended way3.

NEW QUESTION 100
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 a Desktop application to collect leads for marketing campaigns. UC wants to extend this application to integrate with Salesforce to create leads. Integration between the desktop application and salesforce should be seamless. What Authorization flow should the Architect recommend?

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

Answer: A

Explanation:
The JWT Bearer Token flow is an OAuth flow in which an external app (also called client or consumer app) sends a signed JSON string to Salesforce called JWT to obtain an access token. The access token can then be used by the external app to read and write data in Salesforce1. This flow is suitable for UC's scenario because it allows seamless integration between the desktop application and Salesforce without requiring user interaction or login credentials2. The other options are not valid authorization flows for this scenario. The Web Server Authentication Flow and the User Agent Flow both require user interaction and redirection to the Salesforce OAuth authorization endpoint, which is not seamless3. The Username and Password Flow requires the external app to store the user's login

credentials, which is not secure or recommended3.
References: OAuth 2.0 JWT Bearer Flow for Server-to-Server Integration, OAuth Authorization Flows, Salesforce OAuth : JWT Bearer Flow

NEW QUESTION 105
Universal Containers (UC) has built a custom time tracking app for its employee. UC wants to leverage Salesforce Identity to control access to the custom app.
At a minimum, which Salesforce license is required to support this requirement?

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

Answer: C

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

NEW QUESTION 109
Universal Containers (UC) has a mobile application for its employees that uses data from Salesforce as well as uses Salesforce for Authentication purposes. UC wants its mobile users to only enter their credentials the first time they run the app. The application has been live for a little over 6 months, and all of the users who were part of the initial launch are complaining that they have to re-authenticate. UC has also recently changed the URI Scheme associated with the mobile app. What should the Architect at UC first investigate?Universal Containers (UC) has a mobile application for its employees that uses data from Salesforce as well as uses Salesforce for Authentication purposes. UC wants its mobile users to only enter their credentials the first time they run the app. The application has been live for a little over 6 months, and all of the users who were part of the initial launch are complaining that they have to re-authenticate. UC has also recently changed the URI Scheme associated with the mobile app. What should the Architect at UC first investigate?

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

Answer: A

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

NEW QUESTION 110
Northern Trail Outfitters manages application functional permissions centrally as Active Directory groups. The CRM_SuperUser and CRM_Reportmg_SuperUser groups should respectively give the user the SuperUser and Reportmg_SuperUser permission set in Salesforce. Salesforce is the service provider to a Security Assertion Markup Language (SAML) identity provider.
Mow should an identity architect ensure the Active Directory groups are reflected correctly when a user accesses Salesforce?

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

Answer: B

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

NEW QUESTION 115
Universal Containers (UC) is implementing Salesforce and would like to establish SAML SSO for its users to log in. UC stores its corporate user identities in a Custom Database. The UC IT Manager has heard good things about Salesforce Identity Connect as an Idp, and would like to understand what limitations they may face if they decided to use Identity Connect in their current environment. What limitation Should an Architect inform the IT Manager about?

A. Identity Connect will not support user provisioning in UC's current environment.
B. Identity Connect will only support Idp-initiated SAML flows in UC's current environment.
C. Identity Connect will only support SP-initiated SAML flows in UC's current environment.
D. Identity connect is not compatible with UC's current identity environment.

Answer: A

Explanation:

Identity Connect will not support user provisioning in UC's current environment. Identity Connect is a tool that synchronizes user data between Active Directory and Salesforce, but it does not work with other identity sources such as a Custom Database5. Therefore, if UC wants to use Identity Connect as an Idp, they will not be able to provision users from their Custom Database to Salesforce.

Options B, C, and D are incorrect because Identity Connect does not have any limitations on the type of SAML flow or the compatibility with UC's current identity environment. Identity Connect supports both Idp-initiated and SP-initiated SAML flows6, and it can act as an Idp for any external service provider that supports SAML 2.07.

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

NEW QUESTION 118

A global fitness equipment manufacturer uses Salesforce to manage its sales cycle. The manufacturer has a custom order fulfillment app that needs to request order data from Salesforce. The order fulfillment app needs to integrate with the Salesforce API using OAuth 2.0 protocol.

What should an identity architect use to fulfill this requirement?

A. Canvas App Integration
B. OAuth Tokens
C. Authentication Providers
D. Connected App and OAuth scopes

Answer: D

Explanation:
To integrate the order fulfillment app with the Salesforce API using OAuth 2.0 protocol, the identity architect should use a Connected App and OAuth scopes. A Connected App is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as OAuth 2.0. OAuth scopes are permissions that define the specific data that an external application can access or modify in Salesforce. To use OAuth 2.0 protocol, the identity architect needs to configure a Connected App in Salesforce and assign the appropriate OAuth scopes to it, such as "api" or "full". References: Connected Apps, OAuth Scopes

NEW QUESTION 121

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 122

Universal Containers (UC) is considering a Customer 360 initiative to gain a single source of the truth for its customer data across disparate systems and services. UC wants to understand the primary benefits of Customer 360 Identity and how it contributes ato successful Customer 360 Truth project.

What are two are key benefits of Customer 360 Identity as it relates to Customer 360? Choose 2 answers

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

Answer: BC

Explanation:
Customer 360 Identity is a cloud-based identity service that provides a single, trusted identity for customers across all your digital properties and applications2. Customer 360 Identity has several benefits that relate to Customer 360, such as3:

> Customer 360 Identity enables an organization to build a single login for each of its customers, giving the organization an understanding of the user's login activity across all its digital properties and applications. This helps to create a unified customer profile and deliver personalized experiences based on user preferences and behaviors3.

> Customer 360 Identity supports multiple brands so you can deliver centralized identity services and correlation of user activity, even if it spans multiple corporate brands and user experiences. This helps to maintain brand consistency and loyalty while providing seamless access to your products and services3.
References:
> Customer 360 Identity
> Customer 360 Identity Benefits

NEW QUESTION 125

Universal Containers (UC) is using a custom application that will act as the Identity Provider and will generate SAML assertions used to log in to Salesforce. UC is considering including custom parameters in the SAML assertion. These attributes contain sensitive data and are needed to authenticate the users. The assertions

are submitted to salesforce via a browser form post. The majority of the users will only be able to access Salesforce via UC's corporate network, but a subset of admins and executives would be allowed access from outside the corporate network on their mobile devices. Which two methods should an Architect consider to ensure that the sensitive data cannot be tampered with, nor accessible to anyone while in transit?

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

Answer: CD

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

NEW QUESTION 126
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 128
Universal Containers wants to implement Single Sign-on for a Salesforce org using an external Identity Provider and corporate identity store.
What type of authentication flow is required to support deep linking'

A. Web Server OAuth SSO flow
B. Service-Provider-Initiated SSO
C. Identity-Provider-initiated SSO
D. StartURL on Identity Provider

Answer: B

Explanation:
Single sign-on (SSO) is an authentication method that enables users to access multiple applications with one login and one set of credentials4. There are two types of SSO flows that can be used with Salesforce as the service provider (SP) and an external identity provider (IdP)5:

> Service-provider-initiated SSO: The user requests a resource from the SP, such as a Salesforce URL. The SP redirects the user to the IdP for authentication. The IdP authenticates the user and sends a SAML response to the SP. The SP validates the SAML response and grants access to the user5. This type of SSO flow supports deep linking, which means that the user can access a specific page within Salesforce without logging in again6.

> Identity-provider-initiated SSO: The user logs in to the IdP and selects an app from a list of available apps. The IdP sends a SAML response to the SP. The SP validates the SAML response and grants access to the user5. This type of SSO flow does not support deep linking, which means that the user can only access the default landing page of Salesforce6.
References:

> Single Sign-On

> SAML SSO Flows

> Deep Linking

NEW QUESTION 129
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 133
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 134
Universal Containers (UC) would like its community users to be able to register and log in with Linkedin or Facebook Credentials. UC wants users to clearly see Facebook &Linkedin Icons when they register and login. What are the two recommended actions UC can take to achieve this Functionality? Choose 2 answers

A. Enable Facebook and Linkedin as Login options in the login section of the Community configuration.
B. Create custom Registration Handlers to link Linkedin and facebook accounts to user records.
C. Store the Linkedin or Facebook user IDs in the Federation ID field on the Salesforce User record.
D. Create custom buttons for Facebook and inkedin using JAVAscript/CSS on a custom Visualforce page.

Answer: AB

Explanation:
The two recommended actions UC can take to achieve the functionality of allowing community users to register and log in with LinkedIn or Facebook credentials are:

➤ Enable Facebook and LinkedIn as login options in the login section of the community configuration.
This action allows UC to configure Facebook and LinkedIn as authorization providers in Salesforce, which are external services that authenticate users and provide information about their identity and
attributes. By enabling these login options in the community configuration, UC can display Facebook and LinkedIn icons on the community login page and allow users to log in with their existing credentials from these services.

➤ Create custom registration handlers to link LinkedIn and Facebook accounts to user records. This action allows UC to create Apex classes that implement the Auth.RegistrationHandler interface and define the logic for creating or updating user accounts in Salesforce when users log in with LinkedIn or Facebook. By creating custom registration handlers, UC can map the information from the authorization providers to the user fields in Salesforce, such as name, email, profile, or contact.

The other options are not recommended actions for this scenario. Storing the LinkedIn or Facebook user IDs in the Federation ID field on the Salesforce user record is not necessary or sufficient for enabling SSO with these services, as the Federation ID is used for SAML-based SSO, not OAuth-based SSO. Creating custom buttons for Facebook and LinkedIn using JavaScript/CSS on a custom Visualforce page is not advisable, as it would require custom code and UI development, which could increase complexity and maintenance efforts. Moreover, it would not leverage the built-in functionality of authorization providers and registration handlers that Salesforce provides. References: [Authorization Providers], [Enable Social Sign-On for Your Community], [Create a Registration Handler Class], [Auth.RegistrationHandler Interface], [Federation ID]

NEW QUESTION 139
A division of a Northern Trail Outfitters (NTO) purchased Salesforce. NTO uses a third party identity provider (IdP) to validate user credentials against Its corporate

Lightweight Directory Access Protocol (LDAP) directory. NTO wants to help employees remember as passwords as possible.
What should an identity architect recommend?

A. Setup Salesforce as a Service Provider to the existing IdP.
B. Setup Salesforce as an IdP to authenticate against the LDAP directory.
C. Use Salesforce connect to synchronize LDAP passwords to Salesforce.
D. Setup Salesforce as an Authentication Provider to the existing IdP.

Answer: A

Explanation:
To help employees remember fewer passwords, an identity architect should recommend setting up Salesforce as a service provider (SP) to the existing IdP. A SP is the system that relies on the IdP for authentication and provides access to its services based on the SAML assertions from the IdP. To set up Salesforce as a SP, you need to create a connected app for Salesforce in the IdP, enable SAML and configure the SAML settings, such as the entity ID, ACS URL, and subject type. You also need to enable SSO for your Salesforce org, upload the IdP certificate, and configure the SSO settings, such as the issuer, identity type, and service provider initiated request binding.
References:
≫ [SAML Single Sign-On]
≫ [Set Up Salesforce as a Service Provider]
≫ [Enable Single Sign-On for Your Org]

NEW QUESTION 141
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 145
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 147
Universal Containers (UC) wants its closed Won opportunities to be synced to a Data Warehouse in near real time. UC has implemented Outbound Message to enable near real-time data sync. UC wants to ensure that communication between Salesforce and Target System is Secure. What Certificate is sent along with the Outbound Message?

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

Answer: A

Explanation:
The CA-Signed Certificate from the Certificate and Key Management menu is the certificate that is sent along with the outbound message. An outbound message is a SOAP message that is sent from Salesforce to an external endpoint when a workflow rule or approval process is triggered. To ensure that the communication between Salesforce and the target system is secure, the outbound message can be signed with a certificate that is generated or uploaded in the Certificate and Key Management menu. The certificate must be CA-Signed, which means that it is issued by a trusted certificate authority (CA) that verifies the identity of the

sender. The other options are not valid certificates for this purpose. The default client certificate from the Develop–> API Menu is a self-signed certificate that is used for testing purposes only and does not provide adequate security. The default client certificate or a certificate from Certificate and Key Management menu is too vague and does not specify whether the certificate is CA-Signed or self-signed. The self-signed certificates from the Certificate & Key Management menu are certificates that are generated by Salesforce without any verification by a CA, and they are not recommended for production use.
References: [Outbound Messages], [Sign Outbound Messages with a Certificate], [CA-Signed Certificates], [Default Client Certificate], [Self-Signed Certificates]

NEW QUESTION 152
Universal containers (UC) has decided to use identity connect as it's identity provider. UC uses active directory(AD) and has a team that is very familiar and comfortable with managing ad groups. UC would like to use AD groups to help configure salesforce users. Which three actions can AD groups control through identity connect? Choose 3 answers

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

Answer: ACE

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

NEW QUESTION 153
Northern Trail Outfitters (NTO) is launching a new sportswear brand on its existing consumer portal built on Salesforce Experience Cloud. As part of the launch, emails with promotional links will be sent to existing customers to log in and claim a discount. The marketing manager would like the portal dynamically branded so that users will be directed to the brand link they clicked on; otherwise, users will view a recognizable NTO-branded page.
The campaign is launching quickly, so there is no time to procure any additional licenses. However, the development team is available to apply any required changes to the portal.
Which approach should the identity architect recommend?

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

Answer: B

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

NEW QUESTION 154
A technology enterprise is planning to implement single sign-on login for users. When users log in to the Salesforce User object custom field, data should be populated for new and existing users.
Which two steps should an identity architect recommend? Choose 2 answers

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

Answer: AB

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

NEW QUESTION 159
Universal Containers (UC) plans to use a SAML-based third-party IdP serving both of the Salesforce Partner Community and the corporate portal. UC partners will log in 65* to the corporate portal to access protected resources, including links to Salesforce resources. What would be the recommended way to configure the IdP so that seamless access can be achieved in this scenario?

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

Answer: D

Explanation:
The recommended way to configure the IdP for seamless access is to use IdP-initiated SSO that passes the SAML token upon Salesforce resource access request. This means that the user logs in to the corporate portal first, and then clicks a link to access a Salesforce resource. The IdP sends a SAML response to Salesforce with the user's identity and other attributes. Salesforce verifies the SAML response and logs in the user to the appropriate Salesforce org and community12. This way, the user does not have to log in again to Salesforce or enter any credentials3. References: 1: SAML SSO with Salesforce as the Service Provider 2: Set Up Single Sign-On for Your Internal Users Unit | Salesforce - Trailhead 3: What is IdP-Initiated Single Sign-On? – OneLogin

NEW QUESTION 163
Universal Containers is creating a mobile application that will be secured by Salesforce Identity using the OAuth 2.0 user-agent flow. Application users will authenticate using username and password. They should not be forced to approve API access in the mobile app or reauthenticate for 3 months.
Which two connected app options need to be configured to fulfill this use case?
Choose 2 answers

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

Answer: BD

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

➤ Set Permitted Users to "All users may self-authorize". Permitted Users is a setting that controls how users can access a connected app. By setting it to "All users may self-authorize", the identity architect can allow users to access the connected app without requiring administrator approval or API access confirmation.

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

NEW QUESTION 167
The security team at Universal Containers (UC) has identified exporting reports as a high-risk action and would like to require users to be logged into Salesforce with their Active Directory (AD) credentials when doing so. For all other users of Salesforce, users should be allowed to use AD Credentials or Salesforce credentials. What solution should be recommended to prevent exporting reports except when logged in using AD credentials while maintaining the ability to view reports when logged in with Salesforce credentials?

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

Answer: C

Explanation:
The best solution to prevent exporting reports except when logged in using AD credentials while maintaining the ability to view reports when logged in with Salesforce credentials is to use SAML federated authentication, treat SAML sessions as high assurance, and raise the session level required for exporting reports. SAML federated authentication is a process that allows users to log in to Salesforce with an external identity provider (IdP), such as AD, that authenticates the user and issues a security token to Salesforce. By treating SAML sessions as high assurance, Salesforce assigns a higher level of trust and security to the sessions that are established by SAML federated authentication. By raising the session level required for exporting reports, Salesforce requires users to have a high assurance session before they can export reports. This solution ensures that only users who log in with AD credentials can export reports, while users who log in with Salesforce credentials can still view reports but not export them.
The other options are not valid solutions for this scenario. Using SAML federated authentication and blocking access to reports when accessed through a standard assurance session would prevent users who log in with Salesforce credentials from viewing reports at all, which is not the desired outcome. Using SAML federated authentication and custom SAML JIT provisioning to dynamically add or remove a permission set that grants the export reports permission would require UC to write custom code and logic to implement the JIT provisioning and manage the permission set, which could increase complexity and cost. Using SAML federated authentication with a login flow to dynamically add or remove a permission set that grants the export reports permission would also require UC to write custom code and logic to implement the login flow and manage the permission set, which could introduce errors and performance issues. References: [SAML Single Sign-On], [Session Security Levels], [Set Session Security Levels for Your Org], [Just-in-Time Provisioning for SAML], [Login Flows]

NEW QUESTION 171
An Identity architect works for a multinational, multi-brand organization. As they work with the organization to understand their Customer Identity and Access Management requirements, the identity architect learns that the brand experience is different for each of the customer's sub-brands and each of these branded experiences must be carried through the login experience depending on which sub-brand the user is logging into.
Which solution should the architect recommend to support scalability and reduce maintenance costs, if the organization has more than 150 sub-brands?

A. Assign each sub-brand a unique Experience ID and use the Experience ID to dynamically brand the login experience.
B. Use Audiences to customize the login experience for each sub-brand and pass an audience ID to the community during the OAuth and Security Assertion Markup Language (SAML) flows.
C. Create a community subdomain for each sub-brand and customize the look and feel of the Login page for each community subdomain to match the brand.
D. Create a separate Salesforce org for each sub-brand so that each sub-brand has complete control over the user experience.

Answer: A

Explanation:
To support scalability and reduce maintenance costs for a multinational, multi-brand organization, the architect should recommend assigning each sub-brand a

unique Experience ID and using the Experience ID to dynamically brand the login experience. Experience ID is a parameter that can be used to identify different brands or experiences within a single Experience Cloud site (formerly known as Community). Dynamic branding is a feature that allows Experience Cloud sites to display different branding elements, such as logos, colors, or images, based on the Experience ID or other criteria. This solution can provide a consistent and personalized brand experience for each sub-brand without creating multiple subdomains or orgs. References: Experience ID, Dynamic Branding for Experience Cloud Sites

NEW QUESTION 172
An identity architect has been asked to recommend a solution that allows administrators to configure personalized alert messages to users before they land on the Experience Cloud site (formerly known as Community) homepage.
What is recommended to fulfill this requirement with the least amount of customization?

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

Answer: B

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

NEW QUESTION 176
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 179
Universal containers (UC) does my domain enable in the context of a SAML SSO configuration? Choose 2 answers

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

Answer: AC

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

NEW QUESTION 181
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 183
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 188
The CIO of universal containers(UC) wants to start taking advantage of the refresh token capability for the UC applications that utilize Oauth 2.0. UC has listed an architect to analyze all of the applications that use Oauth flows to. See where refresh Tokens can be applied. Which two OAuth flows should the architect consider in their evaluation? Choose 2 answers

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

Answer: AC

Explanation:
The two OAuth flows that support refresh tokens are Web server and User-Agent. According to the Salesforce documentation2, "The web server authentication flow and user-agent flow both provide a refresh token that can be used to get a new access token." Therefore, option A and C are the correct answers.
References: Salesforce Documentation

NEW QUESTION 189
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
Users logging into Salesforce are frequently prompted to verify their identity.
The identity architect is required to provide recommendations so that frequency of prompt verification can be reduced.
What should the identity architect recommend to meet the requirement?

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

Answer: B

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

NEW QUESTION 193
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your Identity-and-Access-Management-Architect Exam with Our Prep Materials Via below:

https://www.certleader.com/Identity-and-Access-Management-Architect-dumps.html