Exam Questions Identity-and-Access-Management-Architect

Salesforce Certified Identity and Access Management Architect (SU23)

https://www.2passeasy.com/dumps/Identity-and-Access-Management-Architect/

NEW QUESTION 1
Universal containers(UC) has implemented SAML-BASED single Sign-on for their salesforce application and is planning to provide access to salesforce on mobile devices using the salesforce1 mobile app. UC wants to ensure that single Sign-on is used for accessing the salesforce1 mobile app. Which two recommendations should the architect make? Choose 2 answers

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

Answer: BD

Explanation:
To use SAML SSO for accessing the Salesforce1 mobile app, the architect should recommend configuring the embedded web browser to use the My Domain URL and configuring the Salesforce1 app to use the My Domain URL4. Using the My Domain URL allows Salesforce to identify the identity provider and initiate the SSO process5. Using the existing SAML SSO flow along with user agent flow or web server flow is not necessary because Salesforce Mobile Applications only work with service provider initiated setups46. Therefore, option B and D are the correct answers.
References: Salesforce Mobile Application Single Sign-On overview, SAML SSO with Salesforce as the Service Provider, Single Sign-On

NEW QUESTION 2
In a typical SSL setup involving a trusted party and trusting party, what consideration should an Architect take into account when using digital certificates?

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

Answer: D

Explanation:
D is correct because using a self-signed certificate leads to higher maintenance for the trusting party, which is the client or browser that connects to the server. The trusting party needs to add the self-signed certificate to their truststore, which is a repository of trusted certificates, in order to establish a secure connection with the server. Otherwise, the trusting party will see a warning message or an error when accessing the server.
A is incorrect because using a self-signed certificate leads to higher maintenance for the trusted party, not lower. The trusted party needs to maintain multiple self-signed certificates from different servers in their truststore.
B is incorrect because using a self-signed certificate does not make the trusted party act as the trusted CA (Certificate Authority). The trusted CA is the entity that issues and validates certificates for servers. The trusted party only needs to trust the CA’s root certificate, which is usually pre-installed in their truststore.
C is incorrect because using a self-signed certificate leads to higher maintenance for the trusting party, not lower. The trusting party still needs to maintain a trusted CA cert in their truststore, which is the self-signed certificate itself.
References: 1: SSL Certificate Installation Instructions & Tutorials - DigiCert 2: How To Install an SSL Certificate from a Commercial … - DigitalOcean 3: Setup SSL CSR Creation and SSL Certificate Installatio
- DigiCert

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

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

Answer: ADE

Explanation:
The three features of federated single sign-on (SSO) solutions are:
➢ It establishes trust between identity store and service provider. Federated SSO is a process that allows users to access multiple applications or systems with one set of credentials by using a common identity provider (IdP) that authenticates the user and issues a security token to the service provider (SP) that grants access. This process requires a trust relationship between the IdP and the SP, which is established by exchanging metadata and certificates.
➢ It improves affiliated applications adoption rates. Federated SSO improves the user experience and satisfaction by reducing the number of login prompts, passwords, and authentication failures that users have to deal with when accessing multiple applications or systems. This can increase the usage and adoption rates of the affiliated applications or systems, as users can access them more easily and conveniently.
➢ It enables quick and easy provisioning and deprovisioning of users. Federated SSO enables centralized management of user accounts and access rights by using the IdP as the source of truth for user identity and attributes. This can simplify and automate the provisioning and deprovisioning of users across multiple applications or systems, as changes made in the IdP can be reflected in the SPs without requiring manual intervention or synchronization.
The other option is not a feature of federated SSO solutions. Federated SSO does not solve all identity and access management problems, as it still faces challenges such as security risks, compatibility issues, governance policies, and user education. References: [Federated Single Sign-On], [Set Up Federated Authentication Using SAML], [Benefits of Single Sign-On], [How Single Sign-On Improves Application Adoption Rates], [User Provisioning for Federated Single Sign-On], [Just-in-Time Provisioning for SAML], [Challenges of Single Sign-On]

NEW QUESTION 4
Universal containers (UC) is setting up Delegated Authentication to allow employees to log in using their corporate credentials. UC's security team is concerned about the risk of exposing the corporate login service on the Internet and has asked that a reliable trust mechanism be put in place between the login service and salesforce. What mechanism should an architect put in place to enable a trusted connection between the login services and salesforce?

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

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

Answer: D

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

NEW QUESTION 5
Universal Containers 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
Northern Trail Outfitters (NTO) utilizes a third-party cloud solution for an employee portal. NTO also owns Salesforce Service Cloud and would like employees to be able to login to Salesforce with their third-party portal credentials for a seamless experience. The third-party employee portal only supports OAuth.
What should an identity architect recommend to enable single sign-on (SSO) between the portal and Salesforce?

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

Answer: A

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

NEW QUESTION 7
Which two roles of the systems are involved in an environment where salesforce users are enabled to access Google Apps from within salesforce through App launcher and connected App set up? Choose 2 answers

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

Answer: BC

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

NEW QUESTION 8
Containers (UC) uses an internal system for recruiting and would like to have the candidates' info available in the Salesforce automatically when they are selected.

UC decides to use OAuth to connect to Salesforce from the recruiting system and would like to do the authentication using digital certificates. Which two OAuth flows should be considered to meet the requirement? Choose 2 answers

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

Answer: AC

Explanation:
JWT Bearer Token flow and SAML Bearer Assertion flow are two OAuth flows that can be used to authenticate to Salesforce using digital certificates. JWT Bearer Token flow allows a connected app to request an access token from Salesforce by using a JSON Web Token (JWT) that is signed with a digital certificate. SAML Bearer Assertion flow allows a connected app to request an access token from Salesforce by using a SAML assertion that is signed with a digital certificate. These two flows can meet the requirement of UC to use OAuth and digital certificates to connect to Salesforce from the recruiting system.

NEW QUESTION 9
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 10
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 12
Northern Trail Outfitters (NTO) has an off-boarding process where a terminated employee is first disabled in the Lightweight Directory Act Protocol (LDAP) directory, then requests are sent to the various application support teams to finish user deactivations. A terminated employee recently was able to login to NTO's Salesforce instance 24 hours after termination, even though the user was disabled in the corporate LDAP directory.
What should an identity architect recommend to prevent this from happening in the future?

A. Create a Just-in-Time provisioning registration handler to ensure users are deactivated in Salesforce as they are disabled in LDAP.

B. Configure an authentication provider to delegate authentication to the LDAP directory.
C. use a login flow to make a callout to the LDAP directory before authenticating the user to Salesforce.
D. Setup an identity provider (IdP) to authenticate users using LDAP, set up single sign-on to Salesforce and disable Login Form authentication.

Answer: B

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

NEW QUESTION 15
An identity architect has built a native mobile application and plans to integrate it with a Salesforce Identity solution. The following are the requirements for the solution:
* 1. Users should not have to login every time they use the app.
* 2. The app should be able to make calls to the Salesforce REST API.
* 3. End users should NOT see the OAuth approval page.
How should the identity architect configure the Salesforce connected app to meet the requirements?

A. Enable the API Scope and Offline Access Scope, upload a certificate so JWT Bearer Flow can be used and then set the connected app access settings to "Admin Pre-Approved".
B. Enable the API Scope and Offline Access Scope on the connected app, and then set the connected app to access settings to 'Admin Pre-Approved".
C. Enable the Full Access Scope and then set the connected app access settings to "Admin Pre-Approved".
D. Enable the API Scope and Offline Access Scope on the connected app, and then set the Connected App access settings to "User may self authorize".

Answer: A

Explanation:
JWT Bearer Flow is an OAuth 2.0 flow that allows a client app to obtain an access token without user interaction. It requires a certificate to sign the JWT and the API and Offline Access scopes to access the Salesforce REST API and refresh the token. The connected app must also be pre-approved by the admin to avoid the OAuth approval page. References: OAuth 2.0 JWT Bearer Flow for Server-to-Server Integration, Authorize an Org Using the JWT Flow

NEW QUESTION 18
An Architect has configured a SAML-based SSO integration between Salesforce and an external Identity provider and is ready to test it. When the Architect attempts to log in to Salesforce using SSO, the Architect receives a SAML error. Which two optimal actions should the Architect take to troubleshoot the issue?

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

Answer: BC

Explanation:
these are the optimal actions to troubleshoot a SAML error. According to the Salesforce documentation1, yo can use the following methods to debug a SAML error:
- Use a browser that has an add-on/extension that can inspect SAML. This will allow you to see the SAML request and response messages and identify any issues with the SAML assertion or the SAML response2.
- Paste the SAML Assertion Validator in Salesforce. This is a tool that helps you validate the last SAML operation on your organization and shows you any errors or warnings with the SAML assertion or the SAML response1.

Option A is incorrect because the Callback URL is not related to SAML SSO. The Callback URL is used for OAuth SSO, which is a different protocol3. Option D is incorrect because using the browser’s Development tools to view the Salesforce page’s markup will not help you debug a SAML error. The page’s markup does not contain any information about the SAML request or response4.
References: 1: SAML Login Errors - Salesforce 2: How to Troubleshoot a Single Sign-On Error | Salesfo Ben 3: Identity Providers and Service Providers - Salesforce 4: Single Sign-On - Salesforce

NEW QUESTION 22
Universal Containers (UC) would like to enable self-registration for their Salesforce Partner Community Users. UC wants to capture some custom data elements from the partner user, and based on these data elements, wants to assign the appropriate Profile and Account values.
Which two actions should the Architect recommend to UC1 Choose 2 answers

A. Configure Registration for Communities to use a custom Visualforce Page.
B. Modify the SelfRegistration trigger to assign Profile and Account.
C. Modify the CommunitiesSelfRegController to assign the Profile and Account.
D. Configure Registration for Communities to use a custom Apex Controller.

Answer: CD

Explanation:
To enable self-registration for partner community users, UC should modify the CommunitiesSelfRegController class to assign the Profile and Account values based on the custom data elements captured from the partner user. UC should also configure Registration for Communities to use a custom Apex controller that extends the CommunitiesSelfRegController class and overrides the default registration logic3.
References:
- Customize Self-Registration

NEW QUESTION 26
Which two capabilities does My Domain enable in the context of a SAML SSO configuration? Choose 2 answers

A. App Launcher

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

Answer: BC

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

- App Launcher is a feature that lets you access all your connected apps from one place in Salesforce. It does not require My Domain or SAML SSO to work, although it can be enhanced by using them.
- Login Forensics is a feature that analyzes login behavior and identifies anomalous or suspicious logins.

It does not require My Domain or SAML SSO to work, although it can be used with them.
References: My Domain, Deep Linking into Salesforce, Salesforce Mobile App Basics, [App Launc [Login Forensics]

NEW QUESTION 27
How should an Architect automatically redirect users to the login page of the external Identity provider when using an SP-Initiated SAML flow with Salesforce as a Service Provider?

A. Use visualforce as the landing page for My Domain to redirect users to the Identity Provider login Page.
B. Enable the Redirect to the Identity Provider setting under Authentication Services on the My domainConfiguration.
C. Remove the Login page from the list of Authentication Services on the My Domain configuration.
D. Set the Identity Provider as default and enable the Redirect to the Identity Provider setting on the SAML Configuration.

Answer: D

Explanation:
Setting the Identity Provider as default and enabling the Redirect to the Identity Provider setting on the SAML Configuration will automatically redirect users to the login page of the external Identity Provider when using an SP-Initiated SAML flow with Salesforce as a Service Provider1. Option A is incorrect because Visualforce is not a supported method for redirecting users to the Identity Provider login page2. Option B is incorrect because enabling the Redirect to the Identity Provider setting under Authentication Services on the My Domain Configuration will only redirect users to the Identity Provider login page when using an IdP-Initiated SAML flow3. Option C is incorrect because removing the Login page from the list of Authentication Services on the My Domain configuration will not affect the SP-Initiated SAML flow, and may cause other issues with authentication4.
References: SAML SSO Flows, Set up a Service Provider initiated login flow, Configure SAML single sign-on with an identity provider, SAML Identity Provider Configuration Settings

NEW QUESTION 28
Universal containers (UC) is setting up their customer Community self-registration process. They are uncomfortable with the idea of assigning new users to a default account record. What will happen when customers self-register in the community?

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

Answer: C

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

NEW QUESTION 31
Which two are valid choices for digital certificates when setting up two-way SSL between Salesforce and an external system. Choose 2 answers

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

Answer: CD

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

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

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

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

NEW QUESTION 33
Northern Trail Outfitters (NTO) believes a specific user account may have been compromised. NTO inactivated the user account and needs U perform a forensic analysis and identify signals that could Indicate a breach has occurred.
What should NTO's first step be in gathering signals that could indicate account compromise?

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

Answer: D

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

NEW QUESTION 35
An architect needs to advise the team that manages the identity provider how to differentiate salesforce from other service providers. What SAML SSO setting in salesforce provides this capability?

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

Answer: A

Explanation:
The Entity ID is the SAML SSO setting in Salesforce that provides the capability to differentiate Salesforce from other service providers. The Entity ID is a unique identifier for the service provider that is sent in the SAML request and response messages1. The identity provider uses the Entity ID to determine which service provider is requesting or receiving authentication information2. You can customize the Entity ID for your Salesforce org or Experience Cloud site in the SAML Single Sign-On Settings page3. References: 1: SAML SSO Flows 2: Federated Authentication Using SAML to Log in to Salesforce Org 3: Step 2: Create a SA Single Sign-On Setting in Salesforce

NEW QUESTION 37
Universal containers (UC) has an e-commerce website while customers can buy products, make payments, and manage their accounts. UC decides to build a customer Community on Salesforce and wants to allow the customers to access the community for their accounts without logging in again. UC decides to implement ansp-Initiated SSO using a SAML-BASED complaint IDP. In this scenario where salesforce is the service provider, which two activities must be performed in salesforce to make sp-Initiated SSO work? Choose 2 answers

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

Answer: AD

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

NEW QUESTION 40
A group of users try to access one of Universal Containers' Connected Apps and receive the following error message: " Failed: Not approved for access." What is the most likely cause of this issue?

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

Answer: C

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

NEW QUESTION 45
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 50
Universal containers (UC) wants users to authenticate into their salesforce org using credentials stored in a custom identity store. UC does not want to purchase or use a third-party Identity provider. Additionally, UC is extremely wary of social media and does not consider it to be trust worthy. Which two options should an architect recommend to UC? Choose 2 answers

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

Answer: CD

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

NEW QUESTION 52
Sales users at Universal containers use salesforce for Opportunity management. Marketing uses a third-party application called Nest for Lead nurturing that is accessed using username/password. The VP of sales wants to open up access to nest for all sales uses to provide them access to lead history and would like SSO for better adoption. Salesforce is already setup for SSO and uses Delegated Authentication. Nest can accept username/Password or SAML-based Authentication. IT teams have received multiple password-related issues for nest and have decided to set up SSO access for Nest for Marketing users as well. The CIO does not want to invest in a new IDP solution and is considering using Salesforce for this purpose. Which are appropriate license type choices for sales and marketing users, giving salesforce is using Delegated Authentication? Choose 2 answers

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

Answer: AD

Explanation:
The appropriate license type choices for sales and marketing users, given that Salesforce is using delegated authentication, are:
- Salesforce license for sales users. This license type allows internal users, such as employees, to access standard and custom Salesforce objects and features, such as opportunities and reports. This license type also supports delegated authentication, which is a feature that allows Salesforce to delegate the authentication process to an external service by making a SOAP callout to a web service that verifies the user’s credentials. This license type is suitable for sales users who use Salesforce for opportunity management and need to log in with delegated authentication.
- Platform license for marketing users. This license type allows internal users to access custom Salesforce objects and features, such as custom apps and tabs. This license type also supports delegated authentication and single sign-on (SSO), which are features that allow users to log in with an external identity provider (IdP) or service provider (SP). This license type is suitable for marketing users who use a third-party application called Nest for lead nurturing and need to log in with SSO using Salesforce as the IdP or SP.

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

NEW QUESTION 55

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

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

Answer: ABE

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

NEW QUESTION 58
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 62
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 67
A university is planning to set up an identity solution for its alumni. A third-party identity provider will be used for single sign-on Salesforce will be the system of records. Users are getting error messages when logging in.
Which Salesforce feature should be used to debug the issue?

A. Apex Exception Email
B. View Setup Audit Trail
C. Debug Logs
D. Login History

Answer: D

NEW QUESTION 68
Which two security risks can be mitigated by enabling Two-Factor Authentication (2FA) in Salesforce? Choose 2 answers

A. Users leaving laptops unattended and not logging out of Salesforce.
B. Users accessing Salesforce from a public Wi-Fi access point.
C. Users choosing passwords that are the same as their Facebook password.
D. Users creating simple-to-guess password reset questions.

Answer: BC

Explanation:
Enabling Two-Factor Authentication (2FA) in Salesforce can mitigate the security risks of users accessing Salesforce from a public Wi-Fi access point or choosing passwords that are the same as their Facebook password. 2FA is an additional layer of protection beyond your password that requires users to verify their identity with another factor, such as a mobile app, a security key, or a verification code. This can prevent unauthorized access even if the user’s password is compromised or guessed by a malicious actor. The other options are not directly related to 2FA, but rather to user behavior or password policies.

NEW QUESTION 69
An Identity and Access Management (IAM) architect is tasked with unifying multiple B2C Commerce sites and an Experience Cloud community with a single identity. The solution needs to support more than 1,000 logins per minute.
What should the IAM do to fulfill this requirement?

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

Answer: A

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

NEW QUESTION 71
Universal containers uses an Employee portal for their employees to collaborate. employees access the portal from their company's internal website via SSO. It is set up to work with Active Directory. What is the role of Active Directory in this scenario?

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

Answer: C

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

NEW QUESTION 76
Containers (UC) has implemented SAML-based single Sign-on for their Salesforce application and is planning to provide access to Salesforce on mobile devices using the Salesforce1 mobile app. UC wants to ensure that Single Sign-on is used for accessing the Salesforce1 mobile App. Which two recommendations should the Architect make? Choose 2 Answers

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

Answer: BC

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

NEW QUESTION 80
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 81
IT security at Unversal Containers (UC) us concerned about recent phishing scams targeting its users and wants to add additional layers of login protection. What should an Architect recommend to address the issue?

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

Answer: A

Explanation:
The Salesforce Authenticator mobile app adds an extra layer of security for online accounts with two-factor authentication. It allows users to respond to push notifications or use location services to verify their logins and other account activity1. This can help prevent phishing scams and unauthorized access.
References: Salesforce Authenticator, Salesforce Authenticator: Mobile App Security Features, Salesforce Authenticator

NEW QUESTION 85
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 89
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 92
Universal Containers (UC) is rolling out its new Customer Identity and Access Management Solution built on top of its existing Salesforce instance. UC wants to allow customers to login using Facebook, Google, and other social sign-on providers.
How should this functionality be enabled for UC, assuming ail social sign-on providers support OpenID Connect?

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

Answer: A

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

NEW QUESTION 93
Universal containers (UC) is successfully using Delegated Authentication for their salesforce users. The service supporting Delegated Authentication is written in Java. UC has a new CIO that is requiring all company Web services be RESR-ful and written in. NET. Which two considerations should the UC Architect provide to the new CIO? Choose 2 answers

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

Answer: CD

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

NEW QUESTION 94
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 95
Northern Trail Outfitters (NTO) is planning to implement a community for its customers using Salesforce Experience Cloud. Customers are not able to self-register. NTO would like to have customers set their own passwords when provided access to the community.
Which two recommendations should an identity architect make to fulfill this requirement? Choose 2 answers

A. Add customers as contacts and add them to Experience Cloud site.
B. Enable Welcome emails while configuring the Experience Cloud site.
C. Allow Password reset using the API to update Experience Cloud site membership.
D. Use Login Flows to allow users to reset password in Experience Cloud site.

Answer: CD

Explanation:
Allowing password reset using the API and using login flows are two possible ways to enable customers to set their own passwords in Experience Cloud. The other options are not relevant for this requirement, as they do not address the password issue. References: Allow Password Reset Using the API, Use Login Flows to Allow Users to Reset Passwords in Experience Cloud Sites

NEW QUESTION 100
Universal containers (UC) have a custom, internal-only, mobile billing application for users who are commonly out of the office. The app is configured as a connected App in salesforce. Due to the nature of this app, UC would like to take the appropriate measures to properly secure access to the app. Which two are recommendations to make the UC? Choose 2 answers

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

Answer: BC

Explanation:

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

NEW QUESTION 102
Which two statements are capable of Identity Connect? Choose 2 answers

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

Answer: BD

Explanation:
The two statements that are capabilities of Identity Connect are:

- It supports both identity-provider-initiated and service-provider-initiated SSO. Identity Connect is a desktop application that integrates Salesforce with Microsoft Active Directory (AD) and enables single sign-on (SSO) between the two systems. Identity Connect supports both identity-provider-initiated SSO, which is when the user starts at the AD site and then is redirected to Salesforce with a SAML assertion, and service-provider-initiated SSO, which is when the user starts at the Salesforce site and then is redirected to AD for authentication.
- It enables automated user synchronization and deactivation. Identity Connect allows administrators to synchronize user accounts and attributes between AD and Salesforce, either manually or on a scheduled basis. Identity Connect also allows administrators to deactivate user accounts in Salesforce when they are disabled or deleted in AD, which helps maintain security and compliance.

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

NEW QUESTION 104
Universal Containers (UC) has implemented a multi-org architecture in their company. Many users have licences across multiple orgs, and they are complaining about remembering which org and credentials are tied to which business process. Which two recommendations should the Architect make to address the Complaints? Choose 2 answers

A. Activate My Domain to Brand each org to the specific business use case.
B. Implement SP-Initiated Single Sign-on flows to allow deep linking.
C. Implement IdP-Initiated Single Sign-on flows to allow deep linking.
D. Implement Delegated Authentication from each org to the LDAP provider.

Answer: AB

Explanation:
Activating My Domain allows each org to have a unique domain name that can be branded to the specific business use case2. This can help users identify which org they are logging into and avoid confusion. Implementing SP-Initiated Single Sign-on flows enables users to start from a service provider (such as Salesforce) and be redirected to an identity provider (such as Active Directory) for authentication3. This can also allow deep linking, which means users can access specific resources within the service provider after logging in4. These two recommendations can address the complaints of the users who have licenses across multiple orgs.

NEW QUESTION 107
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 112
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 114
Universal containers (UC) built a customer Community for customers to buy products, review orders, and manage their accounts. UC has provided three different options for customers to log in to the customer Community: salesforce, Google, and Facebook. Which two role combinations are represented by the systems in the scenario? Choose 2 answers

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

Answer: BD

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

NEW QUESTION 118
After a recent audit, universal containers was advised to implement Two-factor Authentication for all of their critical systems, including salesforce. Which two actions should UC consider to meet this requirement? Choose 2 answers

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

Answer: AD

Explanation:
A is correct because requiring users to provide their RSA token along with their credentials is a form of two-factor authentication. An RSA token is a hardware device that generates a one-time password (OTP) that changes every few seconds. The user needs to enter both their password and the OTP to log in to Salesforce.
D is correct because requiring users to use a biometric reader as well as their password is another form of two-factor authentication. A biometric reader is a device that scans a user’s fingerprint, face, iris, or other physical characteristics to verify their identity. The user needs to provide both their password and their biometric data to log in to Salesforce.
B is incorrect because requiring users to supply their email and phone number, which gets validated, is not a form of two-factor authentication. This is a form of identity verification, which is used to confirm that the user owns the email and phone number they provided. However, this does not add an extra layer of protection beyond their password when they log in to Salesforce.
C is incorrect because requiring users to enter a second password after the first authentication is not a form of two-factor authentication. This is a form of single-factor authentication, which only relies on something the user knows (their passwords). This does not increase security against unauthorized account access.
References: 4: Multi-Factor Authentication - Salesforce 5: Salesforce Multi-Factor Authentication 6: Factor Authentication - Salesforce India 7: Customer 360 | Increase Productivity - Salesforce UK 8: Secu Salesforce Login Using Two-Factor Authentication and Salesforce …

NEW QUESTION 119
Universal containers (UC) has a mobile application that calls the salesforce REST API. In order to prevent users from having to enter their credentials everytime they use the app, UC has enabled the use of refresh Tokens as part of the salesforce connected App and updated their mobile app to take advantage of the refresh token. Even after enabling the refresh token, Users are still complaining that they have to enter their credentials once a day. What is the most likely cause of the issue?

A. The Oauth authorizations are being revoked by a nightly batch job.

B. The refresh token expiration policy is set incorrectly in salesforce
C. The app is requesting too many access Tokens in a 24-hour period
D. The users forget to check the box to remember their credentials.

Answer: B

Explanation:
The most likely cause of the issue is that the refresh token expiration policy is set incorrectly in Salesforce. A refresh token is a credential that allows a connected app to obtain a new access token when the previous one expires1. The refresh token expiration policy determines how long a refresh token is valid for2. If the policy is set to a short duration, such as 24 hours, the users have to enter their credentials once a day to get a new refresh token. To prevent this, the policy should be set to a longer duration, such as “Refresh token is valid until revoked” or "Refresh token expires after 90 days of inactivity"2.
References: OAuth 2.0 Refresh Token Flow, Manage OAuth Access Policies for a Connected App

NEW QUESTION 123
Universal Containers (UC) is using its production org as the identity provider for a new Experience Cloud site and the identity architect is deciding which login experience to use for the site. Which two page types are valid login page types for the site?
Choose 2 answers

A. Experience Builder Page
B. lightning Experience Page
C. Login Discovery Page
D. Embedded Login Page

Answer: CD

Explanation:
Login Discovery Page and Embedded Login Page are two valid login page types for Experience Cloud sites. Login Discovery Page allows users to choose their preferred login method, such as username/password, SSO, or social sign-on. Embedded Login Page allows users to log in from any site page without being redirected to a separate login page. References: Login Discovery Page, Embedded Login

NEW QUESTION 125
Universal Containers (UC) has an existing web application that it would like to access from Salesforce without requiring users to re-authenticate. The web application is owned UC and the UC team that is responsible for it is willing to add new javascript code and/or libraries to the application. What implementation should an Architect recommend to UC?

A. Create a Canvas app and use Signed Requests to authenticate the users.
B. Rewrite the web application as a set of Visualforce pages and Apex code.
C. Configure the web application as an item in the Salesforce App Launcher.
D. Add the web application as a ConnectedApp using OAuth User-Agent flow.

Answer: A

Explanation:
A Canvas app is a web application that can be embedded within Salesforce and access Salesforce data using the signed request authentication method. This method allows the Canvas app to receive a signed request that contains the context and OAuth token when it is loaded. The Canvas app can use the SDK to request a new or refreshed signed request on demand2. This way, the users do not need to re-authenticate when accessing the web application from Salesforce.
References: Requesting a Signed Request, SAML Single Sign-On for Canv Apps, Mastering Salesforce Canvas Apps

NEW QUESTION 127
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 129
How should an Architect force user to authenticate with Two-factor Authentication (2FA) for Salesforce only when not connected to an internal company network?

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

Answer: A

Explanation:
Using Custom Login Flows with Apex is the best option to force users to authenticate with 2FA for Salesforce only when not connected to an internal company network. Custom Login Flows allow admins to customize the login process for different scenarios and user types2. Apex code can be used to detect the user’s IP address and prompt for 2FA if it is not within the company’s network range3. The other options are not suitable because they either do not support 2FA or do not

allow conditional logic based on the user's IP address.

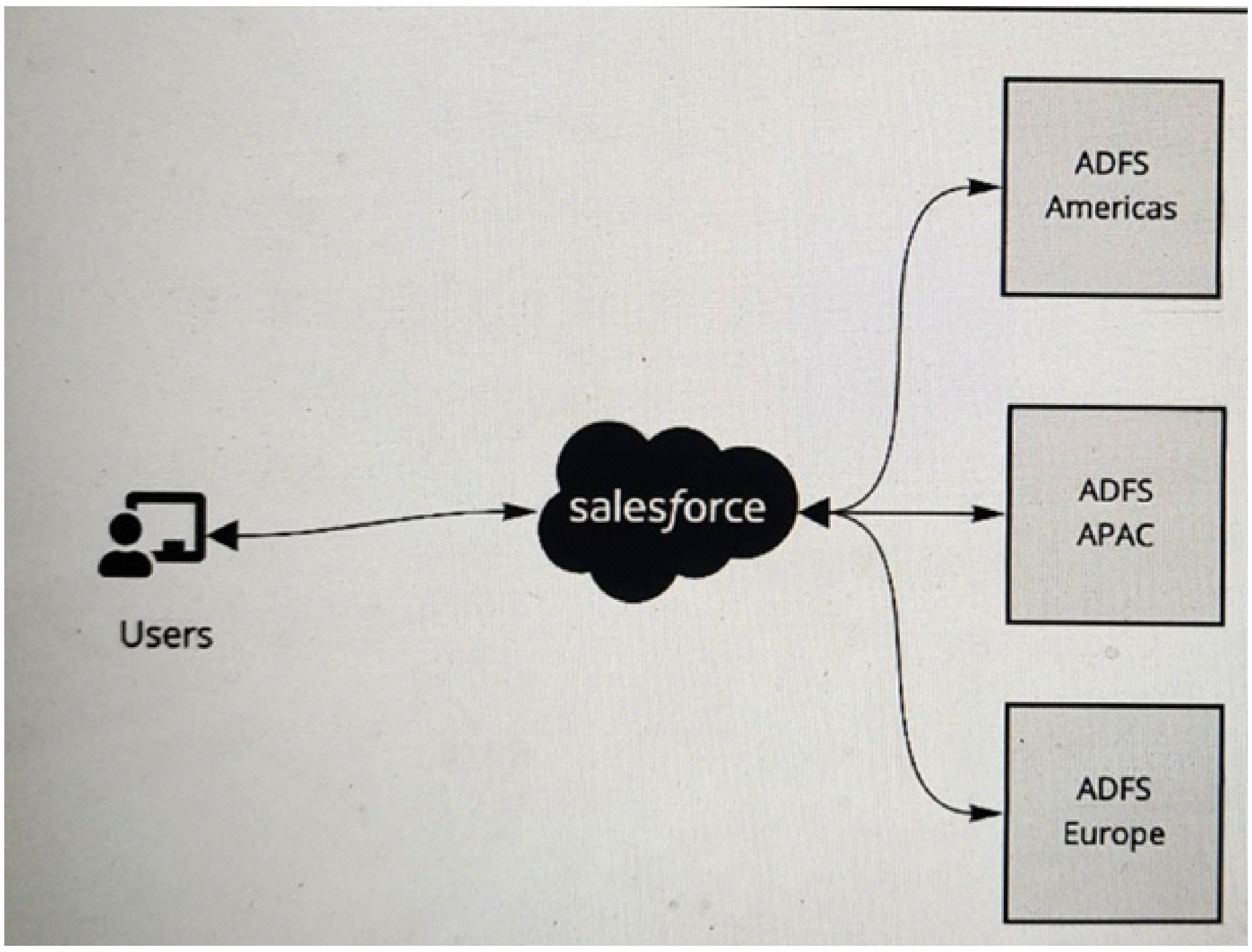
NEW QUESTION 134
Universal containers(UC) wants to integrate a third-party reward calculation system with salesforce to calculate rewards. Rewards will be calculated on a schedule basis and update back into salesforce. The integration between Salesforce and the reward calculation system needs to be secure. 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 137
Refer to the exhibit.



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

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

Answer: B

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

NEW QUESTION 141
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 145
Universal Containers (UC) wants to implement SAML SSO for their internal of Salesforce users using a third-party IdP. After some evaluation, UC decides NOT to 65« set up My Domain for their Salesforce org. How does that decision impact their SSO implementation?

A. IdP-initiated SSO will NOT work.
B. Neither SP- nor IdP-initiated SSO will work.
C. Either SP- or IdP-initiated SSO will work.
D. SP-initiated SSO will NOT work

Answer: D

Explanation:
This is because without My Domain, Salesforce will not know in advance what Identity Provider (IdP) to use for SSO, since it does not even know yet what Organization the user is trying to log in to1. SP-initiated SSO is the scenario where the user starts with a Salesforce link (login page, deep link, Outlook Sync URL, etc.) and then gets redirected to the IdP for authentication2. Without My Domain, SP-initiated SSO requires that the user do an IdP-initiated SSO at least once first so that Salesforce can set a cookie in their browser identifying the IdP1. The other options are not correct for this question because:

- IdP-initiated SSO will work without My Domain, as long as the user starts SSO at the IdP and sends the identity information to Salesforce along with SAML protocol information that identifies the Organization and the IdP2.
- Neither SP- nor IdP-initiated SSO will not work is false, as explained above.
- Either SP- or IdP-initiated SSO will work is false, as explained above.

References: Considerations for setting up My Domain and SSO - Salesforce, SAML SSO with Salesforce as the Service Provider

NEW QUESTION 149
Universal containers (UC) would like to enable SAML-BASED SSO for a salesforce partner community. UC has an existing ldap identity store and a third-party portal. They would like to use the existing portal as the primary site these users' access, but also want to allow seamless access to the partner community. What SSO flow should an architect recommend?

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

Answer: B

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

NEW QUESTION 152
Universal Containers allows employees to use a mobile device to access Salesforce for daily operations using a hybrid mobile app. This app uses Mobile software development kits (SDK), leverages refresh token to regenerate access token when required and is distributed as a private app.
The chief security officer is rolling out an org wide compliance policy to enforce re-verification of devices if an employee has not logged in from that device in the last week.
Which connected app setting should be leveraged to comply with this policy change?

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

Answer: B

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

NEW QUESTION 153
Universal Containers (UC) has decided to use Salesforce as an Identity Provider for multiple external applications. UC wants to use the salesforce App Launcher to control the Apps that are available to individual users. Which three steps are required to make this happen?

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

Answer: ACE

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

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

Option B is incorrect because setting up an Auth Provider is not necessary for SAML SSO. Auth Providers are used for OAuth SSO, which is a different protocol4.
Option D is incorrect because Identity Connect is a tool for synchronizing user data between Active Directory and Salesforce, which is not related to SSO or App Launcher5.
References: 1: App Launcher - Salesforce 2: Enable Salesforce as a SAML Identity Provider 3: Connec Apps Overview 4: Identity Providers and Service Providers - Salesforce 5: Identity Connect Overview

NEW QUESTION 157
Northern Trail Outfitters (NTO) uses Salesforce Experience Cloud sites (previously known as Customer Community) to provide a digital portal where customers can login using their Google account.
NTO would like to automatically create a case record for first time users logging into Salesforce Experience Cloud.
What should an Identity architect do to fulfill the requirement?

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

Answer: D

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

NEW QUESTION 158
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 162
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 166
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 170
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 173
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 176
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 178
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 180
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 184
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 189
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 191
Universal Containers (UC) currently uses Salesforce Sales Cloud and an external billing application. Both Salesforce and the billing application are accessed several times a day to manage customers. UC would like to configure single sign-on and leverage Salesforce as the identity provider. Additionally, UC would like the billing application to be accessible from Salesforce. A redirect is acceptable.
Which two Salesforce tools should an identity architect recommend to satisfy the requirements? Choose 2 answers

A. salesforce Canvas
B. Identity Connect
C. Connected Apps
D. App Launcher

Answer: AD

Explanation:
Salesforce Canvas is a tool that allows external applications to be embedded into Salesforce as iframes, which can provide a seamless user experience. App Launcher is a feature that allows users to access connected apps from a single location in Salesforce. To enable single sign-on and use Salesforce as the identity provider, the external billing application needs to be configured as a connected app and use an OAuth 2.0 or SAML protocol. Identity Connect is not relevant for this scenario, as it is a tool for synchronizing user data between Salesforce and Active Directory. References: Salesforce Canvas Developer Guide, App Launcher, Connect Apps

NEW QUESTION 195
Universal Containers want users to be able to log in to the Salesforce mobile app with their Active Directory password. Employees are unable to use mobile VPN.
Which two options should an identity architect recommend to meet the requirement? Choose 2 answers

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

Answer: AD

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

NEW QUESTION 197
Containers (UC) has an existing Customer Community. UC wants to expand the self-registration capabilities such that customers receive a different community experience based on the data they provide during the registration process. What is the recommended approach an Architect Should recommend to UC?

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

Answer: C

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

NEW QUESTION 199
Northern Trail Outfitters (NTO) has a number of employees who do NOT need access Salesforce objects. Trie employees should sign in to a custom Benefits web app using their Salesforce credentials.
Which license should the identity architect recommend to fulfill this requirement?

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

Answer: A

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

NEW QUESTION 203
An identity architect wants to secure Salesforce APIs using Security Assertion Markup Language (SAML). For security purposes, administrators will need to authorize the applications that will be consuming the APIs.
Which Salesforce OAuth authorization flow should be used?

A. OAuth 2-0 SAML Bearer Assertion Flow
B. OAuth 2.0 JWT Bearer Flow
C. SAML Assertion Flow
D. OAuth 2.0 User-Agent Flow

Answer: C

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

NEW QUESTION 208
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 209
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual Identity-and-Access-Management-Architect Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the Identity-and-Access-Management-Architect Product From:

https://www.2passeasy.com/dumps/Identity-and-Access-Management-Architect/

Money Back Guarantee

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

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

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

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

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