

Salesforce

Exam Questions Identity-and-Access-Management-Architect

Salesforce Certified Identity and Access Management Architect (SU23)



NEW QUESTION 1

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.

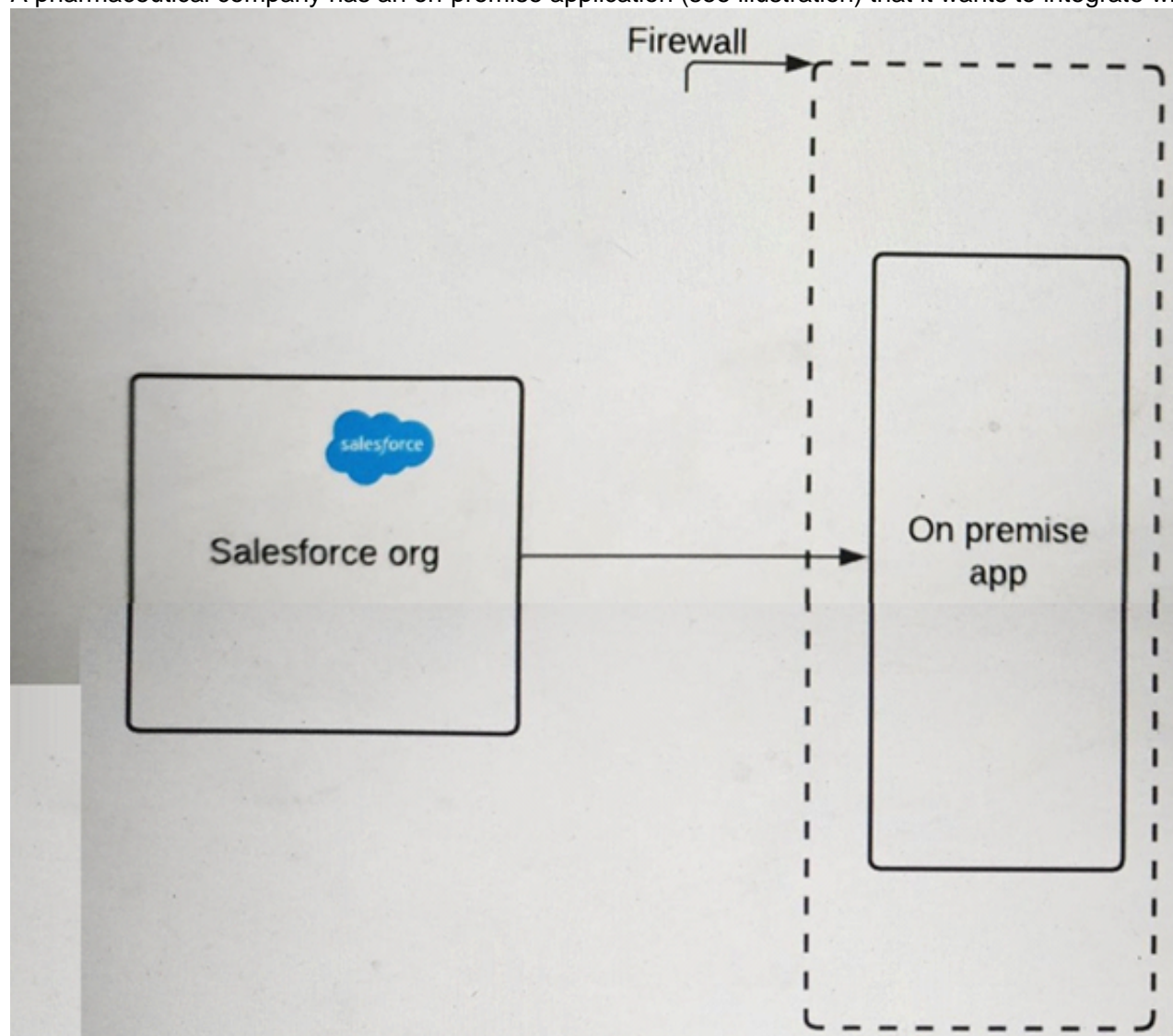
B is incorrect because using a self-signed certificate does not make the trusted party act as the trusted CA (Certificate Authority). The trusted CA is the entity that issues and validates certificates for servers. The trusted party only needs to trust the CA's root certificate, which is usually pre-installed 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 2

A pharmaceutical company has an on-premise application (see illustration) that it wants to integrate with Salesforce.



The IT director wants to ensure that requests must include a certificate with a trusted certificate chain to access the company's on-premise application endpoint. What should an Identity architect do to meet this requirement?

- A. Use open SSL to generate a Self-signed Certificate and upload it to the on-premise app.
- B. Configure the company firewall to allow traffic from Salesforce IP ranges.
- C. Generate a certificate authority-signed certificate in Salesforce and uploading it to the on-premise application Truststore.
- D. Upload a third-party certificate from Salesforce into the on-premise server.

Answer: C

Explanation:

To ensure that requests must include a certificate with a trusted certificate chain to access the company's on-premise application endpoint, the identity architect should generate a certificate authority-signed certificate in Salesforce and upload it to the on-premise application Truststore. A certificate authority-signed certificate is a certificate that is issued by a trusted third-party entity, such as VeriSign or Thawte, that verifies the identity and authenticity of the certificate holder. A Truststore is a repository that stores trusted certificates and public keys. By generating a certificate authority-signed certificate in Salesforce and uploading it to the on-premise application Truststore, the identity architect can enable mutual authentication and secure communication between Salesforce and the on-premise application. The other options are not recommended for this scenario, as they either do not provide a trusted certificate chain, do not enable mutual authentication, or do not secure the communication. References: Create Certificate Authority-Signed Certificates, Mutual Authentication

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

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

Answer: D

Explanation:

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

NEW QUESTION 5

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

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

Answer: BC

Explanation:

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

NEW QUESTION 6

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

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

Answer: C

Explanation:

Service-provider-initiated SSO is required to support deep linking, which is the ability to direct users to a specific page within Salesforce from a different app. With service-provider-initiated SSO, the user requests a resource from Salesforce (the service provider), which then redirects the user to the identity provider for authentication. After the user is authenticated, the identity provider sends a SAML response back to Salesforce, which then grants access to the requested

resource. Web server OAuth SSO flow is used for OAuth 2.1 authentication, not SAML. Identity-provider-initiated SSO is when the user logs in to the identity provider first and then selects a service provider to access. Start URL on identity provider is not a type of authentication flow, but a parameter that can be used to specify the landing page after SSO. References: Certification - Identity and Access Management Architect - Trailhead, Deep Linking, Single Sign On Deep Linking - Salesforce Developer Community

NEW QUESTION 7

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 8

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

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

Answer: BE

Explanation:

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

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

References:

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

NEW QUESTION 9

Universal Containers (UC) employees have Salesforce access from restricted IP ranges only, to protect against unauthorized access. UC wants to roll out the Salesforce¹ mobile app and make it accessible from any location. Which two options should an Architect recommend? Choose 2 answers

- A. Relax the IP restriction with a second factor in the Connect App settings for Salesforce¹ mobile app.
- B. Remove existing restrictions on IP ranges for all types of user access.
- C. Relax the IP restrictions in the Connect App settings for the Salesforce¹ mobile app.
- D. Use Login Flow to bypass IP range restriction for the mobile app.

Answer: AC

Explanation:

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

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

NEW QUESTION 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 10

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 14

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

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

Answer: A

Explanation:

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

NEW QUESTION 19

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 20

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, you 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 | Salesforce Ben 3: Identity Providers and Service Providers - Salesforce 4: Single Sign-On - Salesforce

NEW QUESTION 21

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

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

What is the correct sequence for the authorization flow?

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

Answer: B

Explanation:

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

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

NEW QUESTION 22

Northern Trail Outfitters (NTO) wants its customers to use phone numbers to log in to their new digital portal, which was designed and built using Salesforce Experience Cloud. In order to access the portal, the user will need to do the following:

- * 1. Enter a phone number and/or email address
- * 2. Enter a verification code that is to be sent via email or text.

What is the recommended approach to fulfill this requirement?

- A. Create a Login Discovery page and provide a Login Discovery Handler Apex class.
- B. Create a custom login page with an Apex controller
- C. The controller has logic to send and verify the identity.
- D. Create an authentication provider and implement a self-registration handler class.
- E. Create a custom login flow that uses an Apex controller to verify the phone numbers with the company's verification service.

Answer: A

Explanation:

To allow customers to use phone numbers to log in to their new digital portal, the identity architect should create a Login Discovery page and provide a Login Discovery Handler Apex class. A Login Discovery page is a custom page that allows users to enter their phone number or email address and receive a verification code via email or text. A Login Discovery Handler is a class that implements the Auth.LoginDiscoveryHandler interface and defines how to handle the user input and verification code. This approach can provide a passwordless login experience for the customers. References: Login Discovery, Create a Login Discovery Page

NEW QUESTION 26

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 27

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 28

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 30

Northern Trail Outfitters (NTO) wants to give customers the ability to submit and manage issues with their purchases. It is important for to give its customers the ability to login with their Facebook and Twitter credentials.

Which two actions should an identity architect recommend to meet these requirements? Choose 2 answers

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

Answer: BD

Explanation:

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

NEW QUESTION 35

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 36

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). 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 41

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 43

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, given 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 45

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 up 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 the 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 48

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

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

Answer: D

Explanation:

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

NEW QUESTION 53

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 58

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 60

Universal Containers has multiple Salesforce instances where users receive emails from different instances. Users should be logged into the correct Salesforce instance authenticated by their IdP when clicking on an email link to a Salesforce record. What should be enabled in Salesforce as a prerequisite?

- A. My Domain
- B. External Identity
- C. Identity Provider
- D. Multi-Factor Authentication

Answer: A

Explanation:

My Domain is a feature that allows you to personalize your Salesforce org with a subdomain within the Salesforce domain. For example, instead of using a generic URL like <https://na30.salesforce.com>, you can use a custom URL like <https://somethingReallycool.my.salesforce.com>. My Domain should be enabled in Salesforce as a prerequisite for the following reasons:

- My Domain lets you work in multiple Salesforce orgs in the same browser. Without My Domain, you can only log in to one org at a time in the same browser.
- My Domain lets you set up single sign-on (SSO) with third-party identity providers (IdPs). SSO is an authentication method that allows users to access multiple applications with one login and one set of credentials. With My Domain and SSO, users can log in to Salesforce using their corporate credentials or social accounts.
- My Domain lets you customize your login page with your brand. You can add your logo, background image, right-frame content, and authentication service buttons to your login page.

References:

- My Domain
- [Customize Your Login Process with My Domain]

NEW QUESTION 64

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 65

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

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

Answer: B

Explanation:

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

NEW QUESTION 67

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 69

A multinational industrial products manufacturer is planning to implement Salesforce CRM to manage their business. They have the following requirements:

- * 1. They plan to implement Partner communities to provide access to their partner network .
- * 2. They have operations in multiple countries and are planning to implement multiple Salesforce orgs.
- * 3. Some of their partners do business in multiple countries and will need information from multiple Salesforce communities.
- * 4. They would like to provide a single login for their partners.

How should an Identity Architect solution this requirement with limited custom development?

- A. Create a partner login for the country of their operation and use SAML federation to provide access to other orgs.
- B. Consolidate Partner related information in a single org and provide access through Salesforce community.
- C. Allow partners to choose the Salesforce org they need information from and use login flows to authenticate access.
- D. Register partners in one org and access information from other orgs using APIs.

Answer: A

Explanation:

SAML federation allows partners to log in to multiple Salesforce orgs with a single identity provider. The partner login can be created for the country of their operation and then federated to other orgs using SAML assertions. References: SAML Single Sign-On Overview, Federated Authentication Using SAML

NEW QUESTION 73

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 78

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

Which feature should an identity architect recommend to meet the requirements?

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

Answer: D

Explanation:

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

NEW QUESTION 80

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 83

A technology enterprise is setting up an identity solution with an external vendors wellness application for its employees. The user attributes need to be returned to the wellness application in an ID token.

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

- A. OpenID Connect
- B. User Agent Flow
- C. JWT Bearer Token Flow
- D. Web Server Flow

Answer: A

Explanation:

OpenID Connect is an authentication protocol that allows a service provider to obtain user attributes in an ID token from an IdP. The other flows are OAuth 2.0 flows that are used for authorization, not authentication. References: Configure an Authentication Provider Using OpenID Connect, Integrate Service Providers as Connected Apps with OpenID Connect

NEW QUESTION 87

The executive sponsor for an organization has asked if Salesforce supports the ability to embed a login widget into its service providers in order to create a more seamless user experience.

What should be used and considered before recommending it as a solution on the Salesforce Platform?

- A. OpenID Connect Web Server Flo
- B. Determine if the service provider is secure enough to store the client secret on.
- C. Embedded Logi
- D. Identify what level of UI customization will be required to make it match the service providers look and feel.
- E. Salesforce REST api
- F. Ensure that Secure Sockets Layer (SSL) connection for the integration is used.
- G. Embedded Logi
- H. Consider whether or not it relies on third party cookies which can cause browser compatibility issues.

Answer: D

Explanation:

Embedded Login is a feature that allows Salesforce to embed a login widget into any web page, such as a service provider's site, to enable users to log in with their Salesforce credentials. However, Embedded Login relies on third-party cookies, which can cause browser compatibility issues and require users to adjust their browser settings. Therefore, this should be considered before recommending it as a solution on the Salesforce Platform. References: Embedded Login, Embedded Login Implementation Guide

NEW QUESTION 91

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

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

Answer: B

Explanation:

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

NEW QUESTION 96

Universal Containers (UC) wants its users to access Salesforce and other SSO-enabled applications from a custom web page that UC magnets. UC wants its users to use the same set of credentials to access each of the applications. what SAML SSO flow should an Architect recommend for UC?

- A. SP-Initiated with Deep Linking
- B. SP-Initiated
- C. IdP-Initiated
- D. User-Agent

Answer: C

Explanation:

The SAML SSO flow that an architect should recommend for UC is IdP-initiated. IdP-initiated SSO is a process that allows users to start at the IdP site, such as UC's custom web page, and then be redirected to Salesforce or other SPs with a SAML assertion that contains information about the user's identity and attributes. This flow enables UC to provide a single point of entry for its users to access multiple applications with the same credentials, as they do not need to enter their username and password again for each application. This flow also simplifies the configuration and maintenance of SSO, as UC does not need to create or manage deep links or URLs for each application.

The other options are not valid SAML SSO flows for this scenario. SP-initiated with deep linking is a process that allows users to start at a specific resource on the SP site, such as a report or dashboard, and then be redirected to the IdP for authentication and back to the resource with a SAML assertion. This flow is not suitable for UC's scenario, as they want their users to start at their custom web page, not at a specific resource on Salesforce or other SPs. SP-initiated is a process that allows users to start at the SP site, such as Salesforce or other applications, and then be redirected to the IdP for authentication and back to the SP site with a SAML assertion. This flow is not suitable for UC's scenario, as they want their users to start at their custom web page, not at each application separately. User-agent is not a standard term for SAML SSO, but it could refer to user-agent flow, which is an OAuth authorization flow that allows users to obtain an access token from Salesforce by using a browser or web-view. This flow is not suitable for UC's scenario, as it does not use SAML or IdP for authentication.

References: [SAML Single Sign-On], [IdP-Initiated Login], [SP-Initiated Login], [Deep Linking], [OAuth User-Agent Flow]

NEW QUESTION 97

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 98

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

- A. Identity License.
- B. Salesforce License.
- C. External Identity License.
- D. Salesforce Platform License.

Answer: D

Explanation:

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

References: Salesforce Help: User License Types, [Salesforce Help: Single Sign-On for Desktop and Mobile Applications using SAML and OAuth]

NEW QUESTION 100

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 for Delegated Authentication

NEW QUESTION 101

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 102

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

- A. Synchronization of Salesforce Permission Set License 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 103

Universal Containers (UC) has implemented a multi-org architecture in their company. Many users have licenses 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 104

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

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

Which OAuth flow should be used to fulfill the requirement?

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

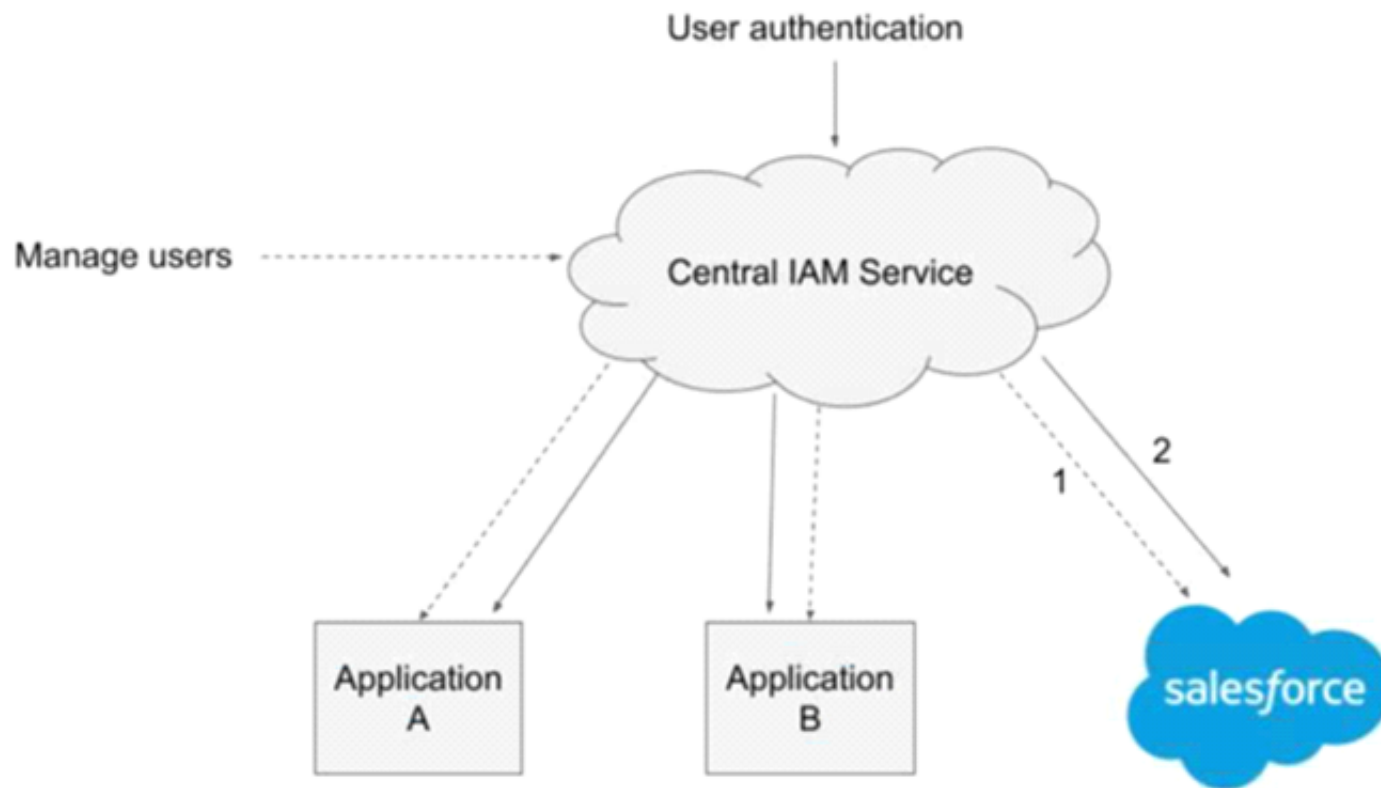
Answer: A

Explanation:

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

NEW QUESTION 107

An organization has a central cloud-based Identity and Access Management (IAM) Service for authentication and user management, which must be utilized by all applications as follows:



1 - Change of a user status in the central IAM Service triggers provisioning or deprovisioning in the integrated cloud applications.

2 - Security Assertion Markup Language single sign-on (SSO) is used to facilitate access for users authenticated at identity provider (Central IAM Service).

Which approach should an IAM architect implement on Salesforce Sales Cloud to meet the requirements?

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

Answer: A

Explanation:

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

NEW QUESTION 108

A global fitness equipment manufacturer is planning to sell fitness tracking devices and has the following requirements:

- 1) Customer purchases the device.
 - 2) Customer registers the device using their mobile app.
 - 3) A case should automatically be created in Salesforce and associated with the customer's account in cases where the device registers issues with tracking.
- Which OAuth flow should be used to meet these requirements?

- A. OAuth 2.0 Asset Token Flow
- B. OAuth 2.0 Username-Password Flow
- C. OAuth 2.0 User-Agent Flow
- D. OAuth 2.0 SAML Bearer Assertion Flow

Answer: A

Explanation:

OAuth 2.0 Asset Token Flow is the flow that allows customers to register their devices with Salesforce and get an access token that can be used to create cases. The other flows are not suitable for this use case.

References: OAuth Authorization Flows Trailblazer Community Documentation

NEW QUESTION 109

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

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

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

Answer: AB

Explanation:

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

NEW QUESTION 110

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 113

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 117

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 122

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 125

In an SP-Initiated SAML SSO setup where the user tries to access a resource on the Service Provider, What HTTP param should be used when submitting a SAML Request to the IdP to ensure the user is returned to the intended resource after authentication?

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

Answer: B

Explanation:

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

NEW QUESTION 126

Containers (UC) uses a legacy Employee portal for their employees to collaborate. Employees access the portal from their company's internal website via SSO. It is set up to work with SiteMinder and Active Directory. The Employee portal has features to support posing ideas. UC decides to use Salesforce Ideas for voting and better tracking purposes. To avoid provisioning users on Salesforce, UC decides to integrate Employee portal ideas with Salesforce idea through the API. What is the role of Salesforce in the context of SSO, based on this scenario?

- A. Service Provider, because Salesforce is the application for managing ideas.
- B. Connected App, because Salesforce is connected with Employee portal via API.
- C. Identity Provider, because the API calls are authenticated by Salesforce.
- D. An independent system, because Salesforce is not part of the SSO setup.

Answer: D

Explanation:

D is correct because Salesforce is an independent system that is not part of the SSO setup between the Employee portal and Active Directory. Salesforce does not act as an IdP or an SP for the SSO, nor does it use a connected app to integrate with the Employee portal. Salesforce only exposes its API to allow the Employee portal to access its ideas feature.

A is incorrect because Salesforce is not a service provider for the SSO. The SSO is between the Employee portal and Active Directory, not between the Employee portal and Salesforce.

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

C is incorrect because Salesforce is not an identity provider for the SSO. The IdP is the system that authenticates users and issues tokens or assertions to allow access to other systems. In this scenario, the IdP is Active Directory, not Salesforce.

References: 1: OAuth Authorization flows in Salesforce - Apex Hours

NEW QUESTION 127

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

Which configuration will meet this requirement?

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

Answer: C

Explanation:

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

NEW QUESTION 131

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

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

Answer: C

Explanation:

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

NEW QUESTION 135

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

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

Answer: A

Explanation:

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

NEW QUESTION 137

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

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

Answer: A

Explanation:

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

NEW QUESTION 138

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

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

Answer: B

Explanation:

Using the Apex Just-in-Time handler to query custom SAML attributes and set permission sets is the best way to ensure that the Active Directory groups are reflected correctly when a user accesses Salesforce. The Apex Just-in-Time handler is a custom class that can process the SAML response from the identity

provider and assign permission sets based on the user's AD groups. The other options are either not feasible or not effective for this use case. References: Just-in-Time Provisioning for SAML, Apex Just-in-Time Handler

NEW QUESTION 139

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 143

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 146

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

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

Answer: AD

Explanation:

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

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

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

NEW QUESTION 151

Universal containers(UC) has decided to build a new, highly sensitive application on Force.com platform. The security team at UC has decided that they want users to provide a fingerprint in addition to username/Password to authenticate to this application. How can an architect support fingerprint as a form of identification for salesforce Authentication?

- A. Use salesforce Two-factor Authentication with callouts to a third-party fingerprint scanning application.
- B. Use Delegated Authentication with callouts to a third-party fingerprint scanning application.
- C. Use an AppExchange product that does fingerprint scanning with native salesforce identity confirmation.
- D. Use custom login flows with callouts to a third-party fingerprint scanning application.

Answer: D

Explanation:

D is correct because using custom login flows with callouts to a third-party fingerprint scanning application allows UC to support fingerprints as a form of identification for Salesforce authentication. Custom login flows allow UC to implement custom logic and UI elements for authentication, such as calling an external web service that performs fingerprint scanning and verification. A is incorrect because using Salesforce two-factor authentication with callouts to a third-party fingerprint scanning application does not support fingerprints as a form of identification for Salesforce authentication. Salesforce two-factor authentication requires users to enter a verification code or use an app like Salesforce Authenticator, not a fingerprint. B is incorrect because using delegated authentication with callouts to a third-party fingerprint scanning application does not support fingerprints as a form of identification for Salesforce authentication. Delegated authentication requires users to enter their username and password, not a fingerprint. C is incorrect because using an AppExchange product that does fingerprint scanning with native Salesforce identity confirmation does not support fingerprints as a form of identification for Salesforce authentication. AppExchange products are third-party applications that integrate with Salesforce, not native Salesforce features. Verified References: [Custom Login Flows], [Two-Factor Authentication], [Delegated Authentication], [AppExchange]

NEW QUESTION 152

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

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

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

Answer: BC

Explanation:

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

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

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

References:

- Customer 360 Identity
- Customer 360 Identity Benefits

NEW QUESTION 154

Northern Trail Outfitters (NTO) wants to give customers the ability to submit and manage issues with their purchases. It is important for NTO to give its customers the ability to login with their Amazon credentials.

What should an identity architect recommend to meet these requirements?

- A. Configure a predefined authentication provider for Amazon.
- B. Create a custom external authentication provider for Amazon.
- C. Configure an OpenID Connect Authentication Provider for Amazon.
- D. Configure Amazon as a connected app.

Answer: C

Explanation:

Amazon supports OpenID Connect as an authentication protocol, which allows users to sign in with their Amazon credentials and access Salesforce resources. To enable this, an identity architect needs to configure an OpenID Connect Authentication Provider for Amazon and link it to a connected app. References: OpenID Connect Authentication Providers, Social Sign-On with OpenID Connect

NEW QUESTION 159

A global company is using the Salesforce Platform as an Identity Provider and needs to integrate a third-party application with its Experience Cloud customer portal.

Which two features should be utilized to provide users with login and identity services for the third-party application?

Choose 2 answers

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

Answer: AC

Explanation:

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

NEW QUESTION 161

Northern Trail Outfitters recently acquired a company. Each company will retain its Identity Provider (IdP). Both companies rely extensively on Salesforce processes that send emails to users to take specific actions in Salesforce.

How should the combined companys' employees collaborate in a single Salesforce org, yet authenticate to the appropriate IdP?

- A. Configure unique MyDomains for each company and have generated links use the appropriate MyDomam in the URL.
- B. Have generated links append a querystnng parameter indicating the Id
- C. The login service will redirect to the appropriate IdP.
- D. Have generated links be prefixed with the appropriate IdP URL to invoke an IdP-initiated Security Assertion Markup Language flow when clicked.
- E. Enable each IdP as a login option in the MyDomain Authentication Service setting
- F. Users will then click on the appropriate IdP button.

Answer: D

Explanation:

To allow employees to collaborate in a single Salesforce org, yet authenticate to the appropriate IdP, the identity architect should enable each IdP as a login option in the MyDomain Authentication Service settings. Users will then click on the appropriate IdP button. MyDomain is a feature that allows administrators to customize the Salesforce login URL with a unique domain name. Authentication Service is a setting that allows administrators to enable different authentication options for users, such as social sign-on or single sign-on with an external IdP. By enabling each IdP as a login option in the MyDomain Authentication Service settings, the identity architect can provide a user-friendly and secure way for employees to log in to Salesforce using their preferred IdP. References: MyDomain, Authentication Service

NEW QUESTION 166

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

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

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

Answer: BD

Explanation:

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

NEW QUESTION 171

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

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

Answer: C

Explanation:

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

NEW QUESTION 172

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 176

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 OAuth JWT 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 177

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 182

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 183

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

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

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

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