

Salesforce

Exam Questions Identity-and-Access-Management-Designer

Salesforce Certified Identity and Access Management Designer (SP19)



NEW QUESTION 1

A farming enterprise offers smart farming technology to its farmer customers, which includes a variety of sensors for livestock tracking, pest monitoring, climate monitoring etc. They plan to store all the data in Salesforce. They would also like to ensure timely maintenance of the installed sensors. They have engaged a Salesforce Architect to propose an appropriate way to generate sensor information in Salesforce.

Which OAuth flow should the architect recommend?

- A. OAuth 2.0 Asset Token Flow
- B. OAuth 2.0 Device Authentication Flow
- C. OAuth 2.0 JWT Bearer Token Flow
- D. OAuth 2.0 SAML Bearer Assertion Flow

Answer: A

NEW QUESTION 2

Universal Containers wants Salesforce inbound OAuth-enabled integration clients to use SAML-BASED single sign-on for authentication. What OAuth flow would be recommended in this scenario?

- A. User-Agent OAuth flow
- B. SAML assertion OAuth flow
- C. User-Token OAuth flow
- D. Web server OAuth flow

Answer: B

NEW QUESTION 3

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

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

Answer: C

NEW QUESTION 4

Northern Trail Outfitters (NTO) is planning to roll out a partner portal for its distributors using Experience Cloud. NTO would like to use an external identity provider (IdP) and for partners to register for access to the portal. Each partner should be allowed to register only once to avoid duplicate accounts with Salesforce. What should a identity architect recommend to create partners?

- A. On successful creation of Partners using Self Registration page in Experience Cloud, create identity in Ping.
- B. Create a custom page in Experience Cloud to self register partner with Experience Cloud and Ping identity store.
- C. Create a custom web page in the Portal and create users in the IdP and Experience Cloud using published APIs.
- D. Allow partners to register through the IdP and create partner users in Salesforce through an API.

Answer: B

NEW QUESTION 5

Universal Containers (UC) is rolling out its new Customer Identity and Access Management Solution built on top of its existing Salesforce instance. UC wants to allow customers to login using Facebook, Google, and other social sign-on providers.

How should this functionality be enabled for UC, assuming all social sign-on providers support OpenID Connect?

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

Answer: A

NEW QUESTION 6

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

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

Answer: ABE

NEW QUESTION 7

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

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

Answer: C

NEW QUESTION 8

Universal Containers (UC) is setting up delegated authentication to allow employees to log in using their corporate credentials. UC's security team is concerned about the risks of exposing the corporate login service on the internet and has asked that a reliable trust mechanism be put in place between the login service and Salesforce.

What mechanism should an Architect put in place to enable a trusted connection between the login service and Salesforce?

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

Answer: A

NEW QUESTION 9

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

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

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

Answer: AB

NEW QUESTION 10

How should an Architect force users 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

NEW QUESTION 10

Universal Containers (UC) rolling out a new Customer Identity and Access Management Solution will be built on top of their existing Salesforce instance. Several service providers have been setup and integrated with Salesforce using OpenID Connect to allow for a seamless single sign-on experience. UC has a requirement to limit user access to only a subset of service providers per customer type.

Which two steps should be done on the platform to satisfy the requirement? Choose 2 answers

- A. Manage which connected apps a user has access to by assigning authentication providers to the users profile.
- B. Assign the connected app to the customer community, and enable the users profile in the Community settings.
- C. Use Profiles and Permission Sets to assign user access to Admin Pre-Approved Connected Apps.
- D. Set each of the Connected App access settings to Admin Pre-Approved.

Answer: CD

NEW QUESTION 11

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 Experience 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

NEW QUESTION 14

Universal Containers wants to implement SAML SSO for their internal Salesforce users using a third-party IdP. After some evaluation, UC decides not to set up My Domain for their Salesforce org. How does that decision impact their SSO implementation?

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

Answer: B

NEW QUESTION 16

An Identity and Access Management (IAM) Architect is recommending Identity Connect to integrate Microsoft Active Directory (AD) with Salesforce for user provisioning, deprovisioning and single sign-on (SSO).

Which feature of Identity Connect is applicable for this scenario?

- A. When Identity Connect is in place, if a user is deprovisioned in an on-premise AD, the user's Salesforce session is revoked immediately.
- B. If the number of provisioned users exceeds Salesforce license allowances, Identity Connect will start disabling the existing Salesforce users in First-in, First-out (FIFO) fashion.
- C. Identity Connect can be deployed as a managed package on Salesforce org, leveraging High Availability of Salesforce Platform out-of-the-box.
- D. When configured, Identity Connect acts as an identity provider to both Active Directory and Salesforce, thus providing SSO as a default feature.

Answer: A

NEW QUESTION 17

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 users 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

NEW QUESTION 21

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

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

Answer: A

NEW QUESTION 23

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

NEW QUESTION 27

Universal Containers (UC) would like to enable self-registration for their Salesforce partner community users. UC wants to capture some custom data elements from the partner user, and based on these data elements, wants to assign the appropriate profile and account values. Which two actions should the architect recommend to UC? Choose 2 answers

- A. Modify the community self-reg controller to assign the profile and account.
- B. Modify the self-registration trigger to assign profile and account.
- C. Configure registration for communities to use a custom Visualforce page.
- D. Configure registration for communities to use a custom Apex controller.

Answer: AC

NEW QUESTION 32

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

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

What should an identity architect do to fulfill the requirement?

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

Answer: D

NEW QUESTION 33

Which two things should be done to ensure end users can only use single sign-on (SSO) to login in to Salesforce?
 Choose 2 answers

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

Answer: AD

NEW QUESTION 35

Universal containers (UC) employees have salesforce access from restricted ip ranges only, to protect against unauthorised access. UC wants to rollout the salesforce1 mobile app and make it accessible from any location. Which two options should an architect recommend? Choose 2 answers

- A. Relax the ip restriction in the connect app settings for the salesforce1 mobile app
- B. Use login flow to bypass ip range restriction for the mobile app.
- C. Relax the ip restriction with a second factor in the connect app settings for salesforce1 mobile app
- D. Remove existing restrictions on ip ranges for all types of user access.

Answer: AB

NEW QUESTION 37

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

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

Answer: A

NEW QUESTION 42

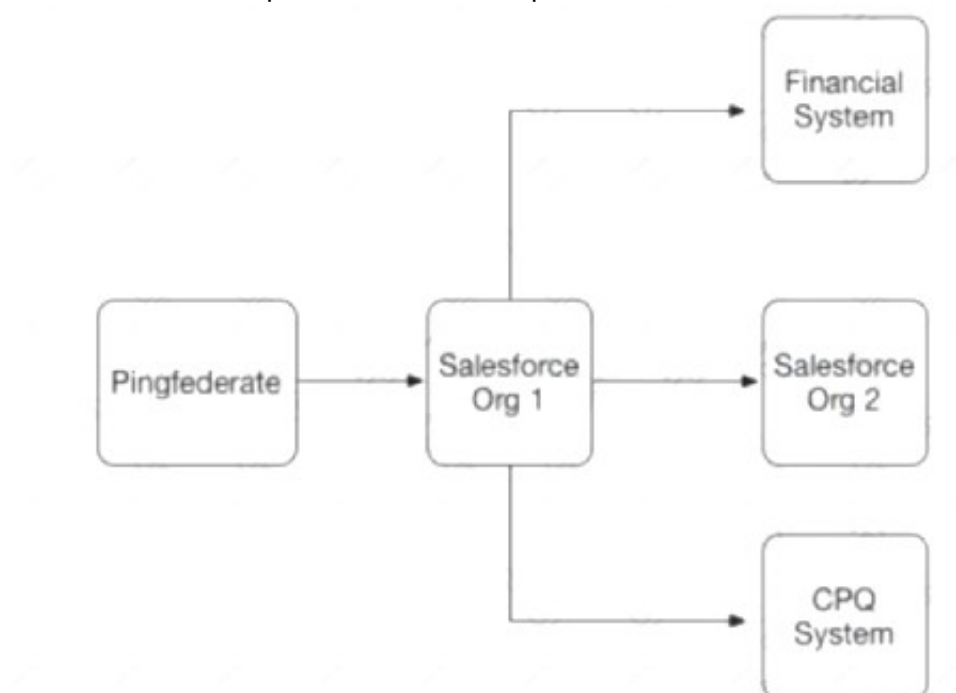
Users logging into Salesforce are frequently prompted to verify their identity.
 The identity architect is required to provide recommendations so that frequency of prompt verification can be reduced.
 What should the identity architect recommend to meet the requirement?

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

Answer: B

NEW QUESTION 45

Universal Containers (UC) has implemented SAML-based Single Sign-On to provide seamless access to its Salesforce Orgs, financial system, and CPQ system. Below is the SSO implementation landscape.



What role combination is represented by the systems in this scenario"

- A. Financial System and CPQ System are the only Service Providers.
- B. Salesforce Org1 and Salesforce Org2 are the only Service Providers.
- C. Salesforce Org1 and Salesforce Org2 are acting as Identity Providers.
- D. Salesforce Org1 and PingFederate are acting as Identity Providers.

Answer: D

NEW QUESTION 47

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

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

Answer: ABC

NEW QUESTION 51

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

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

Answer: B

NEW QUESTION 54

Universal Containers is using OpenID Connect to enable a connection from their new mobile app to its production Salesforce org. What should be done to enable the retrieval of the access token status for the OpenID Connect connection?

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

Answer: B

NEW QUESTION 59

Universal Containers (UC) has a customer Community that uses Facebook for authentication. UC would like to ensure that changes in the Facebook profile are reflected on the appropriate customer Community user. How can this requirement be met?

- A. Use the updateUser() method on the registration handler class.
- B. Use SAML just-in-time provisioning between Facebook and Salesforce
- C. Use information in the signed request that is received from Facebook.
- D. Develop a schedule job that calls out to Facebook on a nightly basis.

Answer: A

NEW QUESTION 64

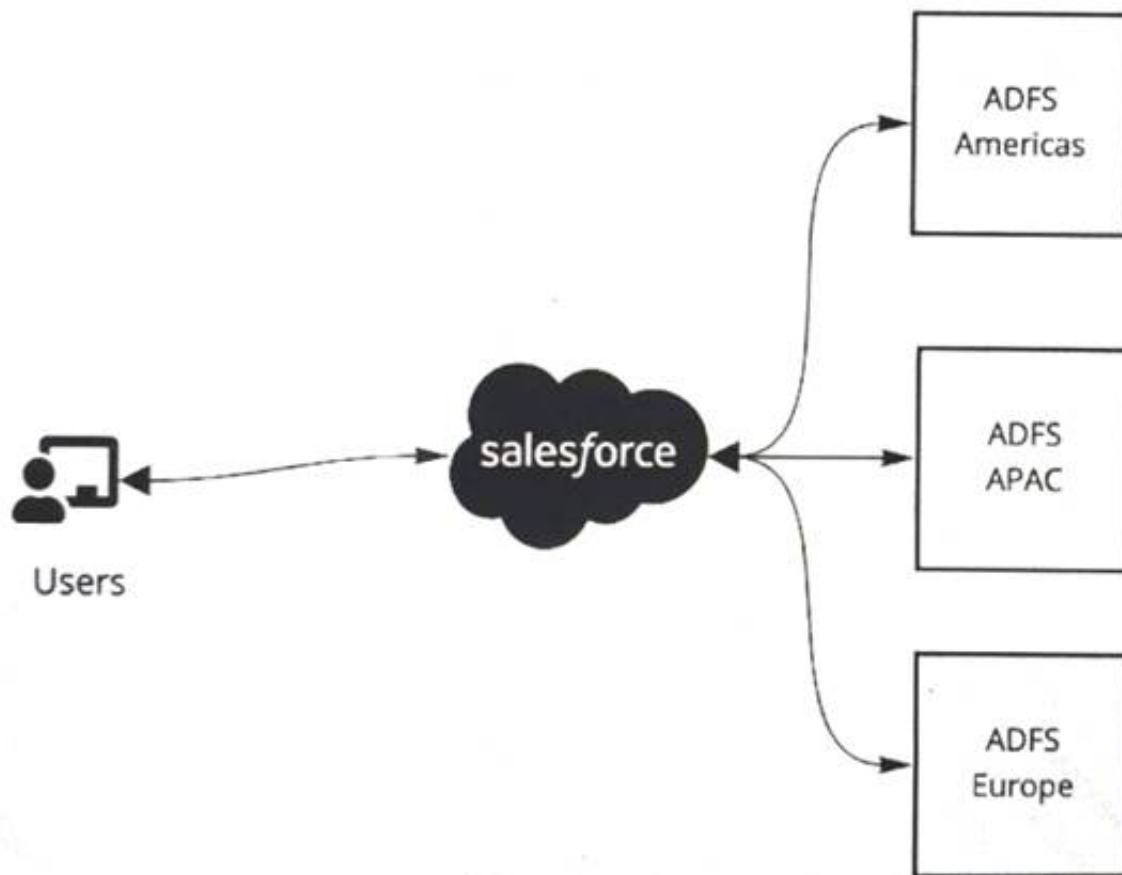
Universal Containers (UC) has an e-commerce website where customers can buy products, make payments, and manage their accounts. UC decides to build a customer Community on Salesforce and wants to allow the customers to access the community for their accounts without logging in again. UC decides to implement sp-Initiated SSO using a SAML-BASED 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. Configure Delegated Authentication
- C. Create a connected App
- D. Set up my domain

Answer: AD

NEW QUESTION 67

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



What is recommended to ensure these requirements are met ?

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

Answer: B

NEW QUESTION 68

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

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

Answer: BD

NEW QUESTION 71

Northern Trail Outfitters (NTO) uses a Security Assertion Markup Language (SAML)-based Identity Provider (IdP) to authenticate employees to all systems. The IdP authenticates users against a Lightweight Directory Access Protocol (LDAP) directory and has access to user information. NTO wants to minimize Salesforce license usage since only a small percentage of users need Salesforce.

What is recommended to ensure new employees have immediate access to Salesforce using their current IdP?

- A. Install Salesforce Identity Connect to automatically provision new users in Salesforce the first time they attempt to login.
- B. Build an integration that queries LDAP periodically and creates new active users in Salesforce.
- C. Configure Just-in-Time provisioning using SAML attributes to create new Salesforce users as necessary when a new user attempts to login to Salesforce.
- D. Build an integration that queries LDAP and creates new inactive users in Salesforce and use a login flow to activate the user at first login.

Answer: C

NEW QUESTION 76

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

NEW QUESTION 77

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

- A. IdP-initiated SSO will NOT work.
- B. Neither SP- nor IdP-initiated SSO will work.

- C. Either SP- or IdP-initiated SSO will work.
- D. SP-initiated SSO will NOT work

Answer: B

NEW QUESTION 78

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

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

Answer: BC

NEW QUESTION 79

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

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

Answer: D

NEW QUESTION 84

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

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

Answer: C

NEW QUESTION 87

Universal Containers (UC) has implemented SSO according to the diagram below. uses SAML while Salesforce Org 1 uses OAuth 2.0. Users usually start their day by first attempting to log into Salesforce Org 2 and then later in the day, they will log into either the Financial System or CPQ system depending upon their job position. Which two systems are acting as Identity Providers?

- A. Financial System
- B. Pingfederate
- C. Salesforce Org 2
- D. Salesforce Org 1

Answer: BD

NEW QUESTION 89

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

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

Answer: B

NEW QUESTION 91

Universal containers (UC) has a mobile application that it wants to deploy to all of its salesforce users, including customer Community users. UC would like to minimize the administration overhead, which two items should an architect recommend? Choose 2 answers

- A. Enable the "Refresh Tokens is valid until revoked " setting in the Connected App.
- B. Enable the "Enforce Ip restrictions" settings in the connected App.
- C. Enable the "All users may self-authorize" setting in the Connected App.
- D. Enable the "High Assurance session required" setting in the Connected App.

Answer: AC

NEW QUESTION 92

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

NEW QUESTION 96

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

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

Answer: D

NEW QUESTION 97

Universal Containers (UC) wants to build a custom mobile app for their field reps to create orders in salesforce. After the first time the users log in, they must be able to access salesforce upon opening the mobile app without being prompted to log in again. What Oauth flows should be considered to support this requirement?

- A. Web Server flow with a Refresh Token.
- B. Mobile Agent flow with a Bearer Token.
- C. User Agent flow with a Refresh Token.
- D. SAML Assertion flow with a Bearer Token.

Answer: C

NEW QUESTION 101

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

NEW QUESTION 105

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

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

Answer: D

NEW QUESTION 109

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

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

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

Answer: D

NEW QUESTION 112

Universal Containers (UC) is building an integration between Salesforce and a legacy web applications using the canvas framework. The security for UC has determined that a signed request from Salesforce is not an adequate authentication solution for the Third-Party app. Which two options should the Architect consider for authenticating the third-party app using the canvas framework? Choose 2 Answers

- A. Utilize the SAML Single Sign-on flow to allow the third-party to authenticate itself against UC's IdP.
- B. Utilize Authorization Providers to allow the third-party application to authenticate itself against Salesforce as the Idp.
- C. Utilize Canvas OAuth flow to allow the third-party application to authenticate itself against Salesforce as the Idp.
- D. Create a registration handler Apex class to allow the third-party application to authenticate itself against Salesforce as the Idp.

Answer: AC

NEW QUESTION 116

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

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

Answer: B

NEW QUESTION 120

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

NEW QUESTION 124

Containers (UC) has decided to implement a federated single Sign-on solution using a third-party Idp. In reviewing the third-party products, they would like to ensure the product supports the automated provisioning and deprovisioning of users. What are the underlining mechanisms that the UC Architect must ensure are part of the product?

- A. SOAP API for provisioning; Just-in-Time (JIT) for Deprovisioning.
- B. Just-In-time (JIT) for Provisioning; SOAP API for Deprovisioning.
- C. Provisioning API for both Provisioning and Deprovisioning.
- D. Just-in-Time (JIT) for both Provisioning and Deprovisioning.

Answer: D

NEW QUESTION 125

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

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

Answer: AB

NEW QUESTION 130

Universal Containers is creating a mobile application that will be secured by Salesforce Identity using the OAuth 2.0 user-agent flow (this flow uses the OAuth 2.0 implicit grant type).

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

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

Answer: ABE

NEW QUESTION 132

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

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

Answer: D

NEW QUESTION 135

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

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

Answer: AD

NEW QUESTION 138

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

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

Answer: B

NEW QUESTION 141

Universal containers (UC) is concerned that having a self-registration page will provide a means for "bots" or unintended audiences to create user records, thereby consuming licences and adding dirty data. Which two actions should UC take to prevent unauthorised form submissions during the self-registration process? Choose 2 answers

- A. Use open-ended security questions and complex password requirements
- B. Primarily use lookup and picklist fields on the self registration page.
- C. Require a captcha at the end of the self-registration process.
- D. Use hidden fields populated via java script events in the self-registration page.

Answer: CD

NEW QUESTION 145

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

NEW QUESTION 148

Universal Containers (UC) has a classified information system that its call center team uses only when they are working on a case with a record type "Classified". They are only allowed to access the system when they own an open "Classified" case, and their access to the system is removed at all other times. They would like to implement SAML SSO with Salesforce as the IdP, and automatically allow or deny the staff's access to the classified information system based on whether they currently own an open "Classified" case record when they try to access the system using SSO. What is the recommended solution for automatically allowing or denying the access to the classified information system based on the open "classified" case record criteria?

- A. Use Salesforce reports to identify users that currently owns open "Classified" cases and should be granted access to the Classified information system.
- B. Use Apex trigger on case to dynamically assign permission Sets that Grant access when an user is assigned with an open "Classified" case, and remove it when the case is closed.
- C. Use Custom SAML JIT Provisioning to dynamically query the user's open "Classified" cases when attempting to access the classified information system.
- D. Use a Common Connected App Handler using Apex to dynamically allow access to the system based on whether the staff owns any open "Classified" Cases.

Answer: D

NEW QUESTION 149

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

What should be done to fulfill the requirement? Choose 2 answers

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

Answer: AB

NEW QUESTION 153

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

NEW QUESTION 155

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

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

Answer: AC

NEW QUESTION 159

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

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

Answer: B

NEW QUESTION 160

Universal Containers (UC) currently uses Salesforce Sales Cloud and an external billing application. Both Salesforce and the billing application are accessed several times a day to manage customers. UC would like to configure single sign-on and leverage Salesforce as the identity provider. Additionally, UC would like the billing application to be accessible from Salesforce. A redirect is acceptable.

Which two Salesforce tools should an identity architect recommend to satisfy the requirements? Choose 2 answers

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

Answer: AD

NEW QUESTION 164

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

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

Answer: A

NEW QUESTION 165

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

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

Answer: C

NEW QUESTION 169

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

NEW QUESTION 172

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

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

Answer: BC

NEW QUESTION 177

Universal containers (UC) uses a legacy Employee portal for their employees to collaborate and post their ideas. UC decides to use salesforce ideas for voting and better tracking purposes. To avoid provisioning users on Salesforce, UC decides to push ideas posted on the Employee portal to salesforce through API. UC decides to use an API user using Oauth Username - password flow for the connection. How can the connection to salesforce be restricted only to the employee portal server?

- A. Add the Employee portals IP address to the Trusted IP range for the connected App
- B. Use a digital certificate signed by the employee portal Server.
- C. Add the employee portals IP address to the login IP range on the user profile.
- D. Use a dedicated profile for the user the Employee portal uses.

Answer: A

NEW QUESTION 182

architect is troubleshooting some SAML-based SSO errors during testing. The Architect confirmed that all of the Salesforce SSO settings are correct. Which two issues outside of the Salesforce SSO settings are most likely contributing to the SSO errors the Architect is encountering? Choose 2 Answers

- A. The Identity Provider is also used to SSO into five other applications.
- B. The clock on the Identity Provider server is twenty minutes behind Salesforce.
- C. The Issuer Certificate from the Identity Provider expired two weeks ago.
- D. The default language for the Identity Provider and Salesforce are Different.

Answer: BC

NEW QUESTION 187

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

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

Answer: AB

NEW QUESTION 190

Universal containers (UC) has a classified information system that it's call centre team uses only when they are working on a case with a record type of "classified". They are only allowed to access the system when they own an open "classified" case, and their access to the system is removed at all other times. They would like to implement SAML SSO with salesforce as the IDP, and automatically allow or deny the staff's access to the classified information system based on whether they currently own an open "classified" case record when they try to access the system using SSO. What is the recommended solution for automatically allowing or denying access to the classified information system based on the open "classified" case record criteria?

- A. Use a custom connected App handler using apex to dynamically allow access to the system based on whether the staff owns any open "classified" cases.
- B. Use apex trigger on case to dynamically assign permission sets that grant access when a user is assigned with an open "classified" case, and remove it when the case is closed.
- C. Use custom SAML jit provisioning to dynamically query the user's open "classified" cases when attempting to access the classified information system
- D. Use salesforce reports to identify users that currently owns open "classified" cases and should be granted access to the classified information system.

Answer: A

NEW QUESTION 192

Universal Containers (UC) built an integration for their employees to post, view, and vote for ideas in Salesforce from an internal Company portal. When ideas are posted in Salesforce, links to the ideas are created in the company portal pages as part of the integration process. The Company portal connects to Salesforce using OAuth. Everything is working fine, except when users click on links to existing ideas, they are always taken to the Ideas home page rather than the specific idea, after authorization. Which OAuth URL parameter can be used to retain the original requested page so that a user can be redirected correctly after OAuth authorization?

- A. Redirect_uri
- B. State
- C. Scope
- D. Callback_uri

Answer: A

NEW QUESTION 197

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: D

NEW QUESTION 198

Universal Containers (UC) has decided to replace the homegrown customer portal with Salesforce Experience Cloud. UC will continue to use its third-party single sign-on (SSO) solution that stores all of its customer and partner credentials.

The first time a customer logs in to the Experience Cloud site through SSO, a user record needs to be created automatically.

Which solution should an identity architect recommend in order to automatically provision users in Salesforce upon login?

- A. Just-in-Time (JIT) provisioning
- B. Custom middleware and web services
- C. Custom login flow and Apex handler
- D. Third-party AppExchange solution

Answer: A

NEW QUESTION 199

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

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

Answer: B

NEW QUESTION 203

Universal Containers is implementing Salesforce Identity to broker authentication from its enterprise single sign-on (SSO) solution through Salesforce to third party applications using SAML.

What role does Salesforce Identity play in its relationship with the enterprise SSO system?

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

Answer: C

NEW QUESTION 204

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

- A. Disallow the use of Single Sign-on for any users of the mobile app.
- B. Require High Assurance sessions in order to use the Connected App.
- C. Set Login IP Ranges to the internal network for all of the app users Profiles.
- D. Use Google Authenticator as an additional part of the login process

Answer: BD

NEW QUESTION 206

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: B

NEW QUESTION 207

Universal Containers (UC) employees have Salesforce access from restricted IP ranges only, to protect against unauthorised 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

NEW QUESTION 212

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

NEW QUESTION 217

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

NEW QUESTION 219

A company's external application is protected by Salesforce through OAuth. The identity architect for the project needs to limit the level of access to the data of the protected resource in a flexible way.
What should be done to improve security?

- A. Select "Admin approved users are pre-authorized" and assign specific profiles.
- B. Create custom scopes and assign to the connected app.
- C. Define a permission set that grants access to the app and assign to authorized users.
- D. Leverage external objects and data classification policies.

Answer: B

NEW QUESTION 222

Universal containers wants 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

NEW QUESTION 223

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

NEW QUESTION 228

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

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

Answer: B

NEW QUESTION 231

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

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

Answer: A

NEW QUESTION 234

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

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

Answer: C

NEW QUESTION 237

.....

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-Designer Practice Exam Features:

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

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