

Exam Questions Identity-and-Access-Management-Designer

Salesforce Certified Identity and Access Management Designer (SP19)

<https://www.2passeasy.com/dumps/Identity-and-Access-Management-Designer/>



NEW QUESTION 1

Universal Container's (UC) is using Salesforce Experience Cloud site for its container wholesale business. The identity architect wants to an authentication provider for the new site.

Which two options should be utilized in creating an authentication provider? Choose 2 answers

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

Answer: AB

NEW QUESTION 2

Universal Containers (UC) is both a Salesforce and Google Apps customer. The UC IT team would like to manage the users for both systems in a single place to reduce administrative burden. Which two optimal ways can the IT team provision users and allow Single Sign-on between Salesforce and Google Apps ? Choose 2 answers

- A. Build a custom app running on Heroku as the Identity Provider that can sync user information between Salesforce and Google Apps.
- B. Use a third-party product as the Identity Provider for both Salesforce and Google Apps and manage the provisioning from there.
- C. Use Identity Connect as the Identity Provider for both Salesforce and Google Apps and manage the provisioning from there.
- D. Use Salesforce as the Identity Provider and Google Apps as a Service Provider and configure User Provisioning for Connected Apps.

Answer: BD

NEW QUESTION 3

universal container plans to develop a custom mobile app for the sales team that will use salesforce for authentication and access management. The mobile app access needs to be restricted to only the sales team. What would be the recommended solution to grant mobile app access to sales users?

- A. Use a custom attribute on the user object to control access to the mobile app
- B. Use connected apps OAuth policies to restrict mobile app access to authorized users.
- C. Use the permission set license to assign the mobile app permission to sales users
- D. Add a new identity provider to authenticate and authorize mobile users.

Answer: B

NEW QUESTION 4

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 5

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 6

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 m 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 7

Universal Containers (UC) wants to build a few applications that leverage the Salesforce REST API. UC has asked its Architect to describe how the API calls will be authenticated to a specific user. Which two mechanisms can the Architect provide? Choose 2 Answers

- A. Authentication Token
- B. Session ID

- C. Refresh Token
- D. Access Token

Answer: CD

NEW QUESTION 8

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 9

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 10

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 10

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 11

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. Identity Provider Login URL.
- B. Issuer.
- C. Entity ID
- D. SAML Identity Location.

Answer: C

NEW QUESTION 13

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

NEW QUESTION 18

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 22

Universal Containers (UC) uses middleware to integrate multiple systems with Salesforce. UC has a strict, new requirement that usernames and passwords cannot be stored in any UC system. How can UC's middleware authenticate to Salesforce while adhering to this requirement?

- A. Create a Connected App that supports the JWT Bearer Token OAuth Flow.
- B. Create a Connected App that supports the Refresh Token OAuth Flow
- C. Create a Connected App that supports the Web Server OAuth Flow.
- D. Create a Connected App that supports the User-Agent OAuth Flow.

Answer: A

NEW QUESTION 27

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 32

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 33

A global company has built an external application that uses data from its Salesforce org via an OAuth 2.0 authorization flow. Upon logout, the existing Salesforce OAuth token must be invalidated.

Which action will accomplish this?

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

Answer: C

NEW QUESTION 36

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 `CommunitiesSelfRegController` to assign the profile and account.
- B. Modify the selfregistration 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 41

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 43

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

NEW QUESTION 47

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

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

Answer: BC

NEW QUESTION 51

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 53

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 54

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 can not be supported because the mobile phone receiving one-time password (OTP) needs to match the number on the contact record.

Answer: C

NEW QUESTION 58

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 63

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

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

Answer: D

NEW QUESTION 67

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

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

Answer: C

NEW QUESTION 68

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 scheduled job that calls out to Facebook on a nightly basis.

Answer: A

NEW QUESTION 71

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

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

Answer: BC

NEW QUESTION 75

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

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

Answer: ACE

NEW QUESTION 77

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

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

Answer: A

NEW QUESTION 78

An Identity architect works for a multinational, multi-brand organization. As they work with the organization to understand their Customer Identity and Access Management requirements, the identity architect learns that the brand experience is different for each of the customer's sub-brands and each of these branded experiences must be carried through the login experience depending on which sub-brand the user is logging into.

Which solution should the architect recommend to support scalability and reduce maintenance costs, if the organization has more than 150 sub-brands?

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

Answer: A

NEW QUESTION 82

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

NEW QUESTION 83

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

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

Answer: A

NEW QUESTION 88

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 89

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 90

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 93

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 95

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

NEW QUESTION 96

Universal containers (UC) has built a custom based Two-factor Authentication (2fa) system for their existing on-premise applications. Thru are now implementing salesforce and would like to enable a Two-factor login process for it, as well. What is the recommended solution an architect should consider?

- A. Replace the custom 2fa system with salesforce 2fa for on-premise application and salesforce.
- B. Use the custom 2fa system for on-premise applications and native 2fa for salesforce.
- C. Replace the custom 2fa system with an app exchange app that supports on-premise applications and salesforce.
- D. Use custom login flows to connect to the existing custom 2fa system for use in salesforce.

Answer: D

NEW QUESTION 98

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 100

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 104

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 106

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 107

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

NEW QUESTION 109

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 114

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

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

Answer: C

NEW QUESTION 116

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

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

Answer: D

NEW QUESTION 118

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

NEW QUESTION 120

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

NEW QUESTION 125

Universal Containers is budding a web application that will connect with the Salesforce API using JWT OAuth Flow. Which two settings need to be configured in the connect app to support this requirement? Choose 2 answers

- A. The Use Digital Signature option in the connected app.
- B. The "web" OAuth scope in the connected app,
- C. The "api" OAuth scope in the connected app.
- D. The "edair_api" OAuth scope in the connected app.

Answer: AC

NEW QUESTION 130

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 131

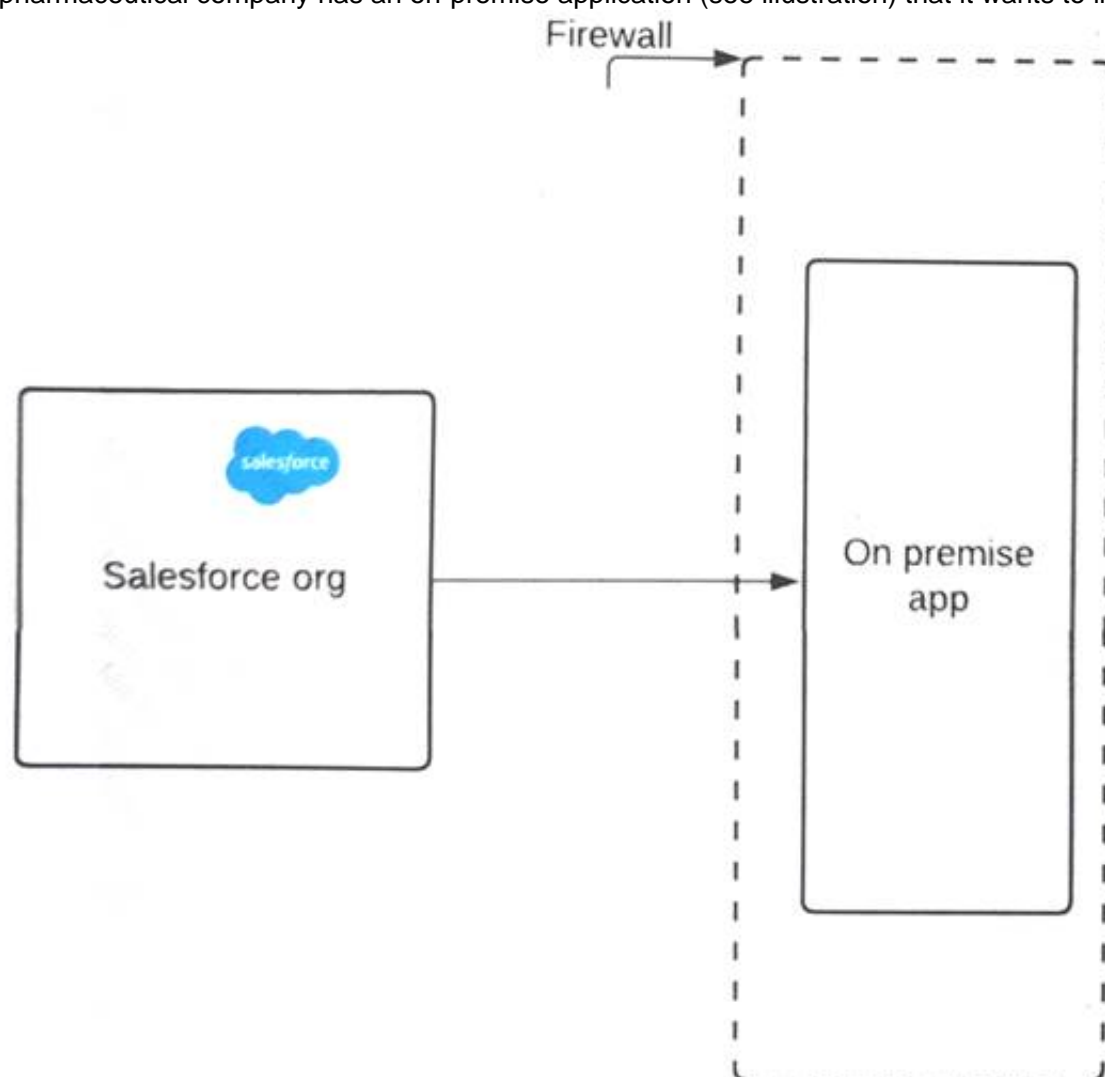
Containers (UC) uses a legacy Employee portal for their employees to collaborate. Employees access the portal from their company's internal website via SSO. It is set up to work with SiteMinder and Active Directory. The Employee portal has features to support posing ideas. UC decides to use Salesforce 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

NEW QUESTION 135

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: B

NEW QUESTION 136

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 137

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 138

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 139

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 141

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 146

Universal containers (UC) has implemented ansp-Initiated SAML flow between an external IDP and salesforce. A user at UC is attempting to login to salesforce1 for the first time and is being prompted for salesforce credentials instead of being shown the IDP login page. What is the likely cause of the issue?

- A. The "Redirect to Identity Provider" option has been selected in the my domain configuration.
- B. The user has not configured the salesforce1 mobile app to use my domain for login
- C. The "Redirect to identity provider" option has not been selected the SAML configuration.
- D. The user has not been granted the "Enable single Sign-on" permission

Answer: B

NEW QUESTION 148

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 add 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 150

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 domain Configuration.
- 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: C

NEW QUESTION 154

Universal Containers (UC) is using a custom application that will act as the Identity Provider and will generate SAML assertions used to log in to Salesforce. UC is considering including custom parameters in the SAML assertion. These attributes contain sensitive data and are needed to authenticate the users. The assertions are submitted to Salesforce via a browser form post. The majority of the users will only be able to access Salesforce via UC's corporate network, but a subset of admins and executives would be allowed access from outside the corporate network on their mobile devices. Which two methods should an Architect consider to ensure that the sensitive data cannot be tampered with, nor accessible to anyone while in transit?

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

Answer: AC

NEW QUESTION 156

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 159

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

NEW QUESTION 160

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 163

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

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

Answer: AC

NEW QUESTION 168

Universal Containers (UC) has a classified information system that its 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 own open "classified" cases and should be granted access to the classified information system.

Answer: A

NEW QUESTION 169

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 173

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. Develop a scheduled job that calls out to Facebook on a nightly basis.
- C. Use information in the signed Request that is received from Facebook.
- D. Use SAML Just-In-Time Provisioning between Facebook and Salesforce.

Answer: A

NEW QUESTION 176

Universal Containers uses Salesforce as an identity provider and Concur as the Employee Expense management system. The HR director wants to ensure Concur accounts for employees are created only after the appropriate approval in the Salesforce org. Which three steps should the identity architect use to implement this requirement? Choose 3 answers

- A. Create an approval process for a custom object associated with the provisioning flow.
- B. Create a connected app for Concur in Salesforce.
- C. Enable User Provisioning for the connected app.
- D. Create an approval process for user object associated with the provisioning flow.
- E. Create an approval process for UserProvisioningRequest object associated with the provisioning flow.

Answer: BCE

NEW QUESTION 179

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 182

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

- A. My domain is configured and active within Salesforce.
- B. The Salesforce SSO settings are using http post

- C. The identity provider is correctly preserving the Relay state
- D. The users have the correct Federation ID within salesforce.

Answer: C

NEW QUESTION 187

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

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

Answer: BD

NEW QUESTION 192

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

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

Answer: C

NEW QUESTION 195

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 196

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 199

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

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

Answer: AB

NEW QUESTION 203

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 207

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

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

Answer: AC

NEW QUESTION 211

Northern Trail Outfitters (NTO) is planning to build a new customer service portal and wants to use passwordless login, allowing customers to login with a one-time passcode sent to them via email or SMS.

How should the quantity of required Identity Verification Credits be estimated?

- A. Each community comes with 10,000 Identity Verification Credits per month and only customers with more than 10,000 logins a month should estimate additional SMS verifications needed.
- B. Identity Verification Credits are consumed with each SMS (text message) sent and should be estimated based on the number of login verification challenges for SMS verification users.
- C. Identity Verification Credits are consumed with each verification sent and should be estimated based on the number of logins that will incur a verification challenge.
- D. Identity Verification Credits are a direct add-on license based on the number of existing member-based or login-based Community licenses.

Answer: B

NEW QUESTION 216

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 220

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 224

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

<https://www.2passeasy.com/dumps/Identity-and-Access-Management-Designer/>

Money Back Guarantee

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