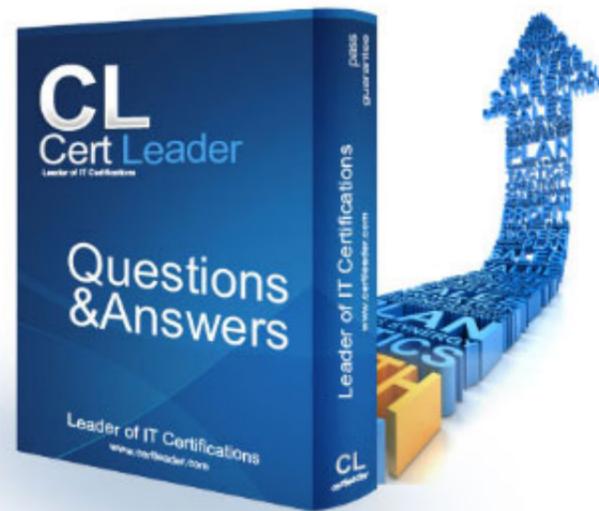


## Identity-and-Access-Management-Designer Dumps

### Salesforce Certified Identity and Access Management Designer (SP19)

<https://www.certleader.com/Identity-and-Access-Management-Designer-dumps.html>



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

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

**Answer:** BD

**NEW QUESTION 4**

Universal containers (UC) uses a home-grown employee portal for their employees to collaborate. UC decides to use salesforce ideas to allow the employees to post ideas from the employee portal. When clicking some links in the employee portal, the users should be redirected to salesforce, authenticated, and presented with relevant pages. What scope should be requested when using the Oauth token to meet this requirement?

- A. Web
- B. Full
- C. API
- D. Visualforce

**Answer:** A

**NEW QUESTION 5**

A leading fitness tracker company is getting ready to launch a customer community. The company wants its customers to login to the community and connect their fitness device to their profile. Customers should be able to obtain exercise details and fitness recommendation In the community. Which should be used to satisfy this requirement?

- A. Named Credentials
- B. Login Flows
- C. OAuth Device Flow
- D. Single Sign-On Settings

**Answer:** C

**NEW QUESTION 6**

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 7**

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 8**

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 9**

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 10**

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 10**

Universal Containers (UC) has decided to use Identity Connect as its identity provider. UC uses Active Directory (AD) and has a team that is very familiar and comfortable with managing AD groups. UC would like to use AD groups to help configure Salesforce users. Which three actions can AD groups control through Identity Connect? Choose 3 answers

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

**Answer: ACE**

**NEW QUESTION 11**

A global company's Salesforce Identity Architect is reviewing its Salesforce production org login history and is seeing some intermittent Security Assertion Markup Language (SAML SSO) 'Replay Detected and Assertion Invalid' login errors.

Which two issues would cause these errors? Choose 2 answers

- A. The subject element is missing from the assertion sent to Salesforce.
- B. The certificate loaded into SSO configuration does not match the certificate used by the IdP.
- C. The current time setting of the company's identity provider (IdP) and Salesforce platform is out of sync by more than eight minutes.
- D. The assertion sent to Salesforce contains an assertion ID previously used.

**Answer: AD**

**NEW QUESTION 15**

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 17**

Users logging into Salesforce are frequently prompted to verify their identity.

The identity architect is required to provide recommendations so that frequency of prompt verification can be reduced.

What should the identity architect recommend to meet the requirement?

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

**Answer: B**

#### **NEW QUESTION 20**

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 23**

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

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

**Answer: A**

#### **NEW QUESTION 27**

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

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

**Answer: CD**

#### **NEW QUESTION 32**

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

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

**Answer: C**

#### **NEW QUESTION 37**

Universal Containers (UC) has a strict requirement to authenticate users to Salesforce using their mainframe credentials. The mainframe user store cannot be accessed from a SAML provider. UC would also like to have users in Salesforce created on the fly if they provide accurate mainframe credentials.

How can the Architect meet these requirements?

- A. Use a Salesforce Login Flow to call out to a web service and create the user on the fly.
- B. Use the SOAP API to create the user when created on the mainframe; implement Delegated Authentication.
- C. Implement Just-In-Time Provisioning on the mainframe to create the user on the fly.
- D. Implement OAuth User-Agent Flow on the mainframe; use a Registration Handler to create the user on the fly.

**Answer: C**

**NEW QUESTION 40**

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 44**

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 48**

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 50**

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

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

**Answer:** A

**NEW QUESTION 52**

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 55**

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 56**

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 58**

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

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

**Answer: A**

**NEW QUESTION 62**

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 66**

An identity architect has been asked to recommend a solution that allows administrators to configure personalized alert messages to users before they land on the Experience Cloud site (formerly known as Community) homepage.

What is recommended to fulfill this requirement with the least amount of customization?

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

**Answer: B**

**NEW QUESTION 69**

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

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

**Answer: BC**

**NEW QUESTION 72**

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 76**

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 80**

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 83**

Refer to the exhibit.

Outfitters (NTO) is using Experience Cloud as an Identity for its application on Heroku. The application on Heroku should be able to handle two brands, Northern Trail Shoes and Northern Trail Shirts.

A user should select either of the two brands in Heroku before logging into the community. The app then performs Authorization using OAuth2.0 with the Salesforce Experience Cloud site.

NTO wants to make sure it renders login page images dynamically based on the user's brand preference selected in Heroku before Authorization. what should an identity architect do to fulfill the above requirements?

- A. For each brand create different communities and redirect users to the appropriate community using a custom Login controller written in Apex.
- B. Create multiple login screens using Experience Builder and use Login Flows at runtime to route to different login screens.
- C. Authorize third-party service by sending authorization requests to the community-url/services/oauth2/authorize/cookie\_value.
- D. Authorize third-party service by sending authorization requests to thecommunity-url/services/oauth2/authorize/expid\_value.

**Answer:** D

#### **NEW QUESTION 86**

The security team at Universal containers(UC) has identified exporting reports as a high-risk action and would like to require users to be logged into salesforce with their active directory (AD) credentials when doing so. For all other uses of Salesforce, Users should be allowed to use AD credentials or salesforce credentials.

What solution should be recommended to prevent exporting reports except when logged in using AD credentials while maintaining the ability to view reports when logged in with salesforce credentials?

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

**Answer:** C

#### **NEW QUESTION 89**

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 94**

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 98**

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 101**

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 106**

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 110**

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 112**

Uwversal Containers (UC) is building a custom employee hut) application on Amazon Web Services (AWS) and would like to store their users' credentials there. Users will also need access to Salesforce for internal operations. UC has tasked an identity architect with evaluating Afferent solutions for authentication and authorization between AWS and Salesforce. How should an identity architect configure AWS to authenticate and authorize Salesforce users?

- A. Configure the custom employee app as a connected app.
- B. Configure AWS as an OpenID Connect Provider.
- C. Create a custom external authentication provider.
- D. Develop a custom Auth server in AWS.

**Answer:** B

**NEW QUESTION 117**

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 118**

Universal containers (UC) wants to implement a partner community. As part of their implementation, UC would like to modify both the Forgot password and change password experience with custom branding for their partner community users. Which 2 actions should an architect recommend to UC? Choose 2 answers

- A. Build a community builder page for the change password experience and Custom Visualforce page for the Forgot password experience.
- B. Build a custom visualforce page for both the change password and Forgot password experiences.
- C. Build a custom visualforce page for the change password experience and a community builder page for the Forgot password experience.
- D. Build a community builder page for both the change password and Forgot password experiences.

**Answer: BC**

**NEW QUESTION 119**

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

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

**Answer: B**

**NEW QUESTION 121**

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

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

**Answer: CD**

**NEW QUESTION 123**

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 127**

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

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

What is the correct sequence for the authorization flow?

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

**Answer: D**

**NEW QUESTION 128**

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 130

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 134

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 139

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

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

**Answer:** AD

#### NEW QUESTION 142

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

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

**Answer:** A

#### NEW QUESTION 143

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 146

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 148**

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 151**

Universal containers (UC) has implemented a multi-org strategy and would like to centralize the management of their salesforce user profiles. What should the architect recommend to allow salesforce profiles to be managed from a central system of record?

- A. Implement jit provisioning on the SAML IDP that will pass the profile id in each assertion.
- B. Create an apex scheduled job in one org that will synchronize the other orgs profile.
- C. Implement Delegated Authentication that will update the user profiles as necessary.
- D. Implement an Oauthjwt flow to pass the profile credentials between systems.

**Answer:** A

**NEW QUESTION 152**

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 153**

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

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

**Answer:** BC

**NEW QUESTION 157**

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 159**

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 161**

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 162**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

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

\* One year free update

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

\* Trusted by Millions

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

\* Shop Securely

All transactions are protected by VeriSign!

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

<https://www.certleader.com/Identity-and-Access-Management-Designer-dumps.html>