Certified Identity and Access Management Designer.VCEplus.premium.exam.60q

Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Certified Identity and Access Management Designer

Version 1.0

Exam A

QUESTION 1
Universal Containers (UC) has decided to build a new, highly sensitive application on the Lightning platform. The security team at UC has decided that they want users to provide a fingerprint in addition to username/password to authenticate to this application.

How can an Architect support fingerprints as a form of identification for Salesforce authentication?

A. Use Custom Login Flows with callouts to a third-party fingerprint scanning application.
B. Use Salesforce Two-factor Authentication with callouts to a third-party fingerprint scanning application.
C. Use Delegated Authentication with callouts to a third-party fingerprint scanning application.
D. Use an AppExchange product that does fingerprint scanning with native Salesforce Identity Confirmation.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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 RESTful and written in .Net.

Which two considerations should the UC Architect provide to the new CIO? (Choose two.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
How should an Architect force users to authenticate with Two-factor Authentication (2FA) for Salesforce only when **NOT** connected to an internal company network?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4 What is a role of an Identity Provider in a Single Sign-on setup using SAML?

A. Consume assertion
B. Revoke assertion

C. Validate assertion
D. Create assertion

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
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. Set up a proxy service for the login service in the DMZ.
D. Include Client Id and Client Secret in the login header callout.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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 three.)

A. Public Group Assignment
B. Role Assignment
C. Custom Permissions Assignment
D. Granting Report Folder Access
E. Permission Sets Assignment

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
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 enlisted 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 two.)

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
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. SAML Identity Location
B. Identity Provider Login URL
C. Entity Id
D. Issuer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
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 Refresh Token OAuth Flow.
B. Create a Connected App that supports the JWT Bearer Token OAuth Flow.
C. Create a Connected App that supports the User-Agent OAuth Flow.
D. Create a Connected App that supports the Web Server OAuth Flow.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Customer Service Representatives at Universal Containers (UC) are complaining that whenever they click on links to case records and are asked to log in 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 users have the correct Federation ID within Salesforce.
C. The Salesforce SSO settings are using HTTP POST.
D. The Identity Provider is correctly preserving the RelayState.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Universal Containers 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 ProfileID in each assertion.
B. Implement Delegated Authentication that will update the user profiles as necessary.
C. Create an Apex scheduled job in one org that will synchronize the other org's profiles.
D. Implement an OAuth JWT flow to pass the profile credentials between systems.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
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 flow is this?

A. IdP-Initiated
B. IdP-Initiated with Deep Linking
C. SP-Initiated
D. Web Server Flow

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13 What item should an Architect consider when designing a Delegated Authentication implementation?

A. The web service should be secured with TLS using Salesforce trusted certificates.
B. The web service should be able to accept one to four input method parameters.
C. The web service should use the Salesforce Federation ID to identify the user.
D. The web service should implement a custom password decryption method.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14 Universal Containers has built a custom token-based Two-Factor Authentication 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 an Architect should consider?

A. Replace the custom 2FA system with an AppExchange App that supports on-premise applications and Salesforce.
B. Use the custom 2FA system for on-premise applications and native 2FA for Salesforce.
C. Replace the custom 2FA system with Salesforce 2FA for on-premise applications and Salesforce.

D. Use Custom Login Flows to connect to the existing custom 2FA system for use in Salesforce.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Universal Containers (UC) is looking to purchase a third-party application as an Identity Provider. UC is looking to develop a business case for the purchase in general and has enlisted an Architect for advice. Which two capabilities of an Identity Provider should the Architect detail to help strengthen the business case? (Choose two.)

A. The Identity Provider can authenticate multiple applications.
B. The Identity Provider can authenticate multiple social media accounts.
C. The Identity Provider can store credentials for multiple applications.
D. The Identity Provider can centralize enterprise password policy.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Universal Containers (UC) wants to implement Delegated Authentication for a certain subset of Salesforce users.

Which three items should UC take into consideration when building the web service to handle the Delegated Authentication request? (Choose three.)

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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17 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 setup? (Choose two.)

A. Salesforce is the Service Provider.
B. Salesforce is the Identity Provider.
C. Google is the Identity Provider.
D. Google is the Service Provider.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
An Architect has successfully configured SAML-based SSO for Universal Containers. SSO has been working for 3 months when Universal Containers manually adds a batch of new users to Salesforce. The new users receive an error from Salesforce when trying to use SSO. Existing users are still able to successfully use SSO to access Salesforce.

What is the likely cause of this behavior?

A. The new users do **NOT** have the SSO permission enabled on their profiles.
B. The Federation ID field on the new User records is **NOT** correctly set.
C. The administrator forgot to reset the new user's Salesforce password.
D. The My Domain capability is **NOT** enabled on the new user's profile.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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 CA-Signed Certificate from the Certificate and Key Management menu.
C. The default Client Certificate from the Develop --> API Menu.
D. The default Client Certificate or a Certificate from Certificate and Key Management menu.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
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. Remove the Login Page from the list of Authentication Services on the My Domain configuration.
B. Set the Identity Provider as default and enable the Redirect to the Identity Provider setting on the SAML Configuration.
C. Use Visualforce as the landing page for My Domain to redirect users to the Identity Provider login page.
D. Enable the Redirect to the Identity Provider setting under Authentication Services on the My Domain Configuration.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Universal Containers (UC) has a custom, internal-only, mobile billing application for users who are commonly out of the office. The app is configured as a Connected App in Salesforce. Due to the nature of this app, UC would like to take the appropriate measures to properly secure access to the app.

Which two solutions should be recommended? (Choose two.)

A. Use Google Authenticator as an additional part of the login process.

B. Require High Assurance sessions in order to use the Connected App.
C. Disallow the use of Single Sign-on for any users of the mobile app.
D. Set Login IP Ranges to the internal network for all of the app users' Profiles.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Universal Containers (UC) wants to integrate a web application with Salesforce. The UC team has implemented the OAuth Web-Server Authentication Flow for authentication purposes. Which

two considerations should an Architect point out to UC? (Choose two.)

A. The flow will **NOT** provide an OAuth Refresh Token back to the server.
B. The web application should be hosted on a secure server.
C. The flow involves passing the user credentials back and forth.
D. The web server must be able to protect consumer secret.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
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 probable cause of this issue?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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 recommended Salesforce license type for all of the UC employees?

A. Salesforce Platform license
B. External Identity license
C. Identity license
D. Salesforce license

Correct Answer: A

Section: (none)
Explanation
Explanation/Reference:

QUESTION 25
Universal Containers wants to build a custom mobile app connecting to Salesforce using OAuth, and would like to restrict the types of resources mobile users can access.

What OAuth feature of Salesforce should be used to achieve the goal?

A. Refresh Tokens
B. Scopes
C. Access Tokens
D. Mobile PINs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Universal Containers (UC) is building an integration between Salesforce and a legacy web application using the Canvas framework. The security team 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 two.)

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
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? (Choose two.)

A. Configure SSO settings for Facebook to serve as a SAML Identity Provider.
B. Configure an Authentication Provider for LinkedIn social media accounts.
C. Create a custom Apex Registration Handler to handle new and existing users.
D. Use Delegated Authentication to call the Twitter login API to authenticate users.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Universal Containers (UC) 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. IdP-initiated SSO will **NOT** work.
B. Either SP- or IdP-initiated SSO will work.
C. SP-initiated SSO will **NOT** work.
D. Neither SP- nor IdP-initiated SSO will work.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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. api
C. Visualforce
D. full

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
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 probable reason for this behavior?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
The security team at Universal Containers 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 with a Login Flow to dynamically add or remove a Permission Set that grants the Export Reports permission.
D. Use SAML Federated Authentication and block access to reports when accessed through a Standard Assurance session.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32 Which three capabilities does SAML-based Federated authentication provide? (Choose three.)

A. Centralized federation provides single point of access, control and auditing.
B. Access tokens are used to access resources on the server once the user is authenticated.
C. Web applications with no passwords are more secure and stronger against hacks.
D. Trust relationships between Identity Provider and Service Provider are required.
E. SAML tokens can be in XML or JSON format and can be used interchangeably.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Universal Containers 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 process will create a Person Account record.
C. The self-registration page will create a new Account record.
D. The self-registration page will ask users to select an Account.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
After a recent audit, Universal Containers (UC) 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 two.)

A. Require users to use a biometric reader as well as their password.
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 provide their RSA token along with their credentials.

Correct Answer: AD

Section: (none)
Explanation

Explanation/Reference:
QUESTION 35
Universal Containers (UC) has a mobile application for its employees that uses data from Salesforce as well as uses Salesforce for authentication purposes. UC wants its mobile users to only enter their credentials the first time they run the app. The application has been live for a little over 6 months, and all of the users who were a part of the initial launch are complaining that they have to re-authenticate. UC has also recently changed the URI Scheme associated with the mobile app.

What should the Architect at UC first investigate?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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 two.)

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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Universal Containers (UC) wants to build a mobile application that will be making calls to the Salesforce REST API. UC's Salesforce implementation relies heavily on custom objects and custom Apex code. UC does not want its users to have to enter credentials every time they use the app.

Which two scope values should an Architect recommend to UC? (Choose two.)

A. full B.
api
C. refresh_token
D. custom_permissions

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
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 this scenario? (Choose two.)

A. Google is the Service Provider and Facebook is the Identity Provider.
B. Facebook is the Service Provider and Salesforce is the Identity Provider.
C. Salesforce is the Service Provider and Google is the Identity Provider.
D. Salesforce is the Service Provider and Facebook is the Identity Provider.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Universal Containers (UC) has Active Directory (AD) as their enterprise identity store and would like to use it for Salesforce user authentication. UC expects to synchronize user data between Salesforce and AD and assign the appropriate Profile and Permission Sets based on AD group membership.

What would be the recommended way to implement SSO?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40 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? (Choose three.)

A. Add each Connected App to the App Launcher with a Start URL.
B. Create a Connected App 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. Set up an Auth Provider for each external application.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
Universal Containers (UC) has implemented an SP-initiated SAML flow between an external IdP and Salesforce. A user at UC is attempting to log in to Salesforce mobile app 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 **NOT** been selected in the My Domain configuration.
B. The "Redirect to Identity Provider" option has **NOT** been selected on the SAML configuration.
C. The user has **NOT** been granted the “Enable Single Sign-on” permission.
D. The user has **NOT** configured the Salesforce mobile app to use My Domain for login.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which two security risks can be mitigated by enabling Two-Factor Authentication in Salesforce? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
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. IdP-Initiated
B. SP-Initiated
C. User-Agent
D. Web Server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
An Architect needs to set up a Facebook Authentication provider as a login option for a Salesforce Customer Community.

What portion of the authentication provider setup associates a Facebook user with a Salesforce user?

A. Apex Registration Handler
B. Federation ID
C. Consumer Key and Consumer Secret
D. User Info Endpoint URL

Correct Answer: A
Section: (none)

Explanation
Explanation/Reference:

QUESTION 45 Universal Containers (UC) employees have Salesforce access from restricted IP ranges only, to protect against unauthorized access. UC wants to roll out the Salesforce mobile app and make it accessible from any location. Which two options should an Architect recommend? (Choose two.)

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
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. Service-Provider-initiated SSO
B. Web Server OAuth SSO flow
C. Identity-Provider-initiated SSO
D. StartURL on Identity Provider

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
In a typical SSL setup involving a trusted party and a trusting party, what consideration should an Architect take into account when using digital certificates?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48 Which three are features of federated Single Sign-on solutions?
(Choose three.)

A. It federates credentials control to authorized applications.
B. It improves affiliated applications adoption rates.
C. It enables quick and easy provisioning and deactivating of users.

D. It establishes trust between Identity Store and Service Provider.
E. It solves all identity and access management problems.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49 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. Develop a scheduled job that calls out to Facebook on a nightly basis.
B. Use the updateUser() method on the Registration Handler class.
C. Use SAML Just-In-Time Provisioning between Facebook and Salesforce.
D. Use information in the Signed Request that is received from Facebook.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
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 licenses and adding dirty data. Which

two actions should UC take to prevent unauthorized form submissions during the self-registration process? (Choose two.)

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
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. Username and Password Flow
C. User Agent Flow
D. Web Server Authentication Flow

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52

Universal Containers (UC) has implemented a multi-org architecture in their company. Many users have licenses across multiple orgs, and they are complaining about remembering which org and credentials are tied to which business process.

Which two recommendations should the Architect make to address the complaints? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53

Universal Containers (UC) uses an internal system for recruiting and would like to have the candidates' info available in 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 two.)

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54

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 recommended ways can the IT team provision users and allow Single Sign-on between Salesforce and Google Apps? (Choose two.)

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55

Universal Containers (UC) uses a legacy Employee portal for employees to collaborate and post 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 portal's IP address to the Login IP range on the user profile.
B. Use a dedicated profile for the user the Employee portal uses.
C. Use a digital certificate signed by the Employee portal server.
D. Add the Employee portal's IP address to the Trusted IP range for the Connected App.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Universal Containers (UC) uses Salesforce to allow customers to keep track of the order status. The customers can log in to Salesforce using external authentication providers, such as Facebook and Google. UC is also leveraging the App Launcher to let customers access an off-platform application for generating shipping labels. The label generator application uses OAuth to provide users access.

What license type should an Architect recommend for the customers?

A. External Identity license
B. Identity license
C. Customer Community license
D. Customer Community Plus license

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
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 Salesforce APIs to create users on the fly.
B. Use Just-in-Time provisioning.
C. Use On-the-Fly provisioning.
D. Use Identity Connect to sync users.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Universal Containers (UC) is building a mobile application that will make calls to the Salesforce REST API. Additionally, UC would like to provide the optimal experience for its mobile users.

Which two OAuth scopes should UC configure in the Connected App? (Choose two.)

A. api

B. web
C. full
D. refresh_token

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
Universal Containers (UC) has implemented SAML-based Single Sign-on for their Salesforce application and is planning to use the Salesforce mobile app. UC wants to ensure that Single Sign-on is used for accessing the Salesforce mobile app.

Which two recommendations should the Architect make? (Choose two.)

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Universal Containers wants to set up SSO for a selected group of users to access external applications from Salesforce through App Launcher. Which

three steps must be completed in Salesforce to accomplish the goal? (Choose three.)

A. Associate User profiles with the Connected Apps.
B. Complete My Domain and Identity Provider setup.
C. Create Connected Apps for the external applications.
D. Complete Single Sign-on Settings in Security Controls.
E. Create Named Credentials for each external system.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference: