Salesforce.Identity and Access Management Architect.by.Herry.121q

Number: Identity and Access Management Architect
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: Identity and Access Management Architect
Exam Name: Salesforce Certified Identity and Access Management Architect

Exam A

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

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

Correct Answer: B, D
Section:

QUESTION 2
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

Correct Answer: A
Section:

QUESTION 3
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

Correct Answer: B
Section:

QUESTION 4
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 appliction to authenticate itself against Salesforce as the Idp.
C. Utilize Canvas OAuth flow to allow the third-party appliction to authenticate itself against Salesforce as the Idp.
D. Create a registration handler Apex class to allow the third-party appliction to authenticate itself against Salesforce as the Idp.

Correct Answer: A, C
Section:

QUESTION 5
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.

Correct Answer: C
Section:

QUESTION 6
An architect needs to set up a Facebook Authentication provider as login option for a salesforce customer Community. What portion of the authentication provider setup associates a Facebook user with a salesforce user?

A. Consumer key and consumer secret
B. Federation ID
C. User info endpoint URL
D. Apex registration handler

Correct Answer: D
Section:

QUESTION 7
Which three different attributes can be used to identify the user in a SAML 65> assertion when Salesforce is acting as a Service Provider? Choose 3 answers

A. Federation ID
B. Salesforce User ID
C. User Full Name
D. User Email Address
E. Salesforce Username

Correct Answer: A, C, D
Section:

QUESTION 8
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.

Correct Answer: C
Section:

QUESTION 9
Universal Containers (UC) uses Active Directory (AD) as their identity store for employees and must continue to do so for network access. UC is undergoing a major transformation program and moving all of their enterprise applications to cloud platforms including Salesforct, Workday, and SAP HAN A. UC needs to implement an SSO solution for accessing all of the third-party cloud applications and the CIO is inclined to use Salesforce for all of their identity and access management needs.
Which two Salesforce license types does UC need for its employees'
Choose 2 answers

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

Correct Answer: B, D
Section:

QUESTION 10
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:

QUESTION 11
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.

Correct Answer: C
Section:

QUESTION 12
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.

Correct Answer: D
Section:

QUESTION 13
Under which scenario Web Server flow will be used?

A. Used for web applications when server-side code needs to interact with APIS.
B. Used for server-side components when page needs to be rendered.
C. Used for mobile applications and testing legacy Integrations.
D. Used for verifying Access protected resources.

Correct Answer: A
Section:

QUESTION 14
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.

Correct Answer: B, C
Section:

QUESTION 15
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

Correct Answer: C
Section:

QUESTION 16

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.

Correct Answer: C
Section:

QUESTION 17
Universal Containers (UC) wants its closed Won opportunities to be synced to a Data Warehouse in near real time. UC has implemented Outbound Message to enable near real-time data sync. UC wants to ensure that communication between Salesforce and Target System is Secure. What Certificate is sent along with the Outbound Message?

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

Correct Answer: B
Section:

QUESTION 18
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.

Correct Answer: A, D, E
Section:

QUESTION 19
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 ecommerce 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.

Correct Answer: A
Section:

QUESTION 20
Containers (UC) has an existing Customer Community. UC wants to expand the self-registration capabilities such that customers receive a different community experience based on the data they provide during the registration process. What is the recommended approach an Architect Should recommend to UC?

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

Correct Answer: C
Section:

QUESTION 21
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.

Correct Answer: A
Section:

QUESTION 22
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.

Correct Answer: B, C, E
Section:

QUESTION 23
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 resourse after authentication?

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

Correct Answer: B
Section:

QUESTION 24
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.

Correct Answer: C
Section:

QUESTION 25
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.

Correct Answer: C
Section:

QUESTION 26
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.

Correct Answer: A, B
Section:

QUESTION 27
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.

Correct Answer: D
Section:

QUESTION 28
Which two statements are capable of Identity Connect? Choose 2 answers

A. Synchronization of Salesforce Permission Set Licence Assignments.
B. Supports both Identity-Provider-Initiated and Service-Provider-Initiated SSO.
C. Support multiple orgs connecting to multiple Active Directory servers.
D. Automated user synchronization and de-activation.

Correct Answer: B, D
Section:

QUESTION 29
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.

Correct Answer: A, C
Section:

QUESTION 30
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.

Correct Answer: B, D
Section:

QUESTION 31
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.

Correct Answer: B, C

Section:

QUESTION 32
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.

Correct Answer: B, C
Section:

QUESTION 33
Universal Containers (UC) has implemented SAML-based SSO solution for use with their multi-org Salesforce implementation, utilizing one of the the orgs as the Identity Provider. One user is reporting that they can log in to the Identity Provider org but get a generic SAML error message when accessing the other orgs. Which two considerations should the architect review to troubleshoot the issue? Choose 2 answers

A. The Federation ID must be a valid Salesforce Username
B. The Federation ID must is case sensitive
C. The Federation ID must be in the form of an email address.
D. The Federation ID must be populated on the user record.

Correct Answer: B, D
Section:

QUESTION 34
Universal Containers (UC) wants to integrate a third-party Reward Calculation system with Salesforce to calculate Rewards. Rewards will be calculated on a schedule basis and update back into Salesforce.
The integration between Salesforce and the Reward Calculation System needs to be secure. Which are two recommended practices for using OAuth flow in this scenario. choose 2 answers

A. OAuth Refresh Token FLow
B. OAuth Username-Password Flow
C. OAuth SAML Bearer Assertion FLow
D. OAuth JWT Bearer Token FLow

Correct Answer: C, D
Section:

QUESTION 35
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

Correct Answer: C, D

Section:

QUESTION 36

Sales users at Universal containers use salesforce for Opportunity management. Marketing uses a third-party application called Nest for Lead nurturing that is accessed using username/password. The VP of sales wants to open up access to nest for all sales uses to provide them access to lead history and would like SSO for better adoption. Salesforce is already setup for SSO and uses Delegated Authentication. Nest can accept username/Password or SAML-based Authentication. IT teams have received multiple password-related issues for nest and have decided to set up SSO access for Nest for Marketing users as well. The CIO does not want to invest in a new IDP solution and is considering using Salesforce for this purpose. Which are appropriate license type choices for sales and marketing users, giving 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.

Correct Answer: A, D
Section:

QUESTION 37

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

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

Correct Answer: D
Section:

QUESTION 38

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 2 answers

A. Refresh token
B. API
C. full
D. Web

Correct Answer: A, B
Section:

QUESTION 39

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.

Correct Answer: B
Section:

QUESTION 40
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.

Correct Answer: A, C
Section:

QUESTION 41
The security team at Universal Containers (UC) has identified exporting reports as a high-risk action and would like to require users to be logged into Salesforce with their Active Directory (AD) credentials when doing so. For all other users of Salesforce, users should be allowed to use AD Credentials or Salesforce credentials. What solution should be recommended to prevent exporting reports except when logged in using AD credentials while maintaining the ability to view reports when logged in with Salesforce credentials?

A. Use SAML Federated Authentication and block access to reports when accessed through a Standard Assurance session.

B. Use SAML Federated Authentication and Custom SAML JIT Provisioning to dynamically and or remove a permission set that grants the Export Reports Permission.

C. Use SAML federated Authentication, treat SAML Sessions as High Assurance, and raise the session level required for exporting reports.

D. Use SAML federated Authentication with a Login Flow to dynamically add or remove a Permission Set that grants the Export Reports Permission.

Correct Answer: C
Section:

QUESTION 42
Universal Containers (UC) wants its users to access Salesforce and other SSO-enabled applications from a custom web page that UC magnets. UC wants its users to use the same set of credentials to access each of the applications. what SAML SSO flow should an Architect recommend for UC?

A. SP-Initiated with Deep Linking

B. SP-Initiated

C. IdP-Initiated

D. User-Agent

Correct Answer: C
Section:

QUESTION 43
Universal Containers (UC) uses a home-grown Employee portal for their employees to collaborate.
UC decides to use Salesforce Ideas to allow employees to post Ideas from the Employee portal.
When users click on some of the links in the Employee portal, the users should be redirected to Salesforce, authenticated, and presented with the relevant pages. What OAuth flow is best suited for this scenario?

A. Web Application flow
B. SAML Bearer Assertion flow
C. User-Agent flow
D. Web Server flow

Correct Answer: D
Section:

QUESTION 44
Universal Containers (UC) has a mobile application for its employees that uses data from Salesforce as well as uses Salesforce for Authentication purposes. UC wants its mobile users to only enter their credentials the first time they run the app. The application has been live for a little over 6 months, and all of the users who were part of the initial launch are complaining that they have to reauthenticate.
UC has also recently changed the URI Scheme associated with the mobile app. What should the Architect at UC first investigate?Universal Containers (UC) has a mobile application for its employees that uses data from Salesforce as well as uses Salesforce for Authentication purposes. UC wants its mobile users to only enter their credentials the first time they run the app. The application has been live for a little over 6 months, and all of the users who were part of the initial launch are complaining that they have to re-authenticate. UC has also recently changed the URI Scheme associated with the mobile app. What should the Architect at UC first investigate?

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

Correct Answer: A
Section:

QUESTION 45
Universal Containers (UC) wants to build a mobile application that twill 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 2 answers.

A. Custom_permissions
B. Api
C. Refresh_token
D. Full

Correct Answer: B, C
Section:

QUESTION 46
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 2 answers

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: A, D
Section:

QUESTION 47
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.

Correct Answer: A, B
Section:

QUESTION 48
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

Correct Answer: A, C
Section:

QUESTION 49
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.

Correct Answer: B, C
Section:

QUESTION 50
How should an Architect force users to authenticate with Two-factor Authentication (2FA) for Salesforce only when not connected to an internal company network?

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

Correct Answer: A
Section:

QUESTION 51
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

Correct Answer: B
Section:

QUESTION 52
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.

Correct Answer: B, C
Section:

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.

Correct Answer: A
Section:

QUESTION 54
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

Correct Answer: A, C
Section:

QUESTION 55
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.

Correct Answer: C
Section:

QUESTION 56
Universal containers (UC) is successfully using Delegated Authentication for their salesforce users.
The service supporting Delegated Authentication is written in Jav a. 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.

Correct Answer: C, D
Section:

QUESTION 57
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

Correct Answer: A, D
Section:

QUESTION 58
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

Correct Answer: A, C
Section:

QUESTION 59
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.

Correct Answer: A, C
Section:

QUESTION 60
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.

Correct Answer: A
Section:

QUESTION 61
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

Correct Answer: B, D
Section:

QUESTION 62
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

Correct Answer: B
Section:

QUESTION 63
Universal containers(UC) has decided to build a new, highly sensitive application on Force.com platform. The security team at UC has decided that they want users to provide a fingerprint in addition to username/Password to authenticate to this application. How can an architect support fingerprints as a form of identification for salesforce Authentication?

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

Correct Answer: D
Section:

QUESTION 64
Universal Containers built a custom mobile app for their field reps to create orders in Salesforce.
OAuth is used for authenticating mobile users. The app is built in such a way that when a user session expires after Initial login, a new access token is obtained automatically without forcing the user to log in again. While that improved the field reps' productivity, UC realized that they need a "logout" feature.
What should the logout function perform in this scenario, where user sessions are refreshed automatically?

A. Invoke the revocation URL and pass the refresh token.
B. Clear out the client Id to stop auto session refresh.
C. Invoke the revocation URL and pass the access token.
D. Clear out all the tokens to stop auto session refresh.

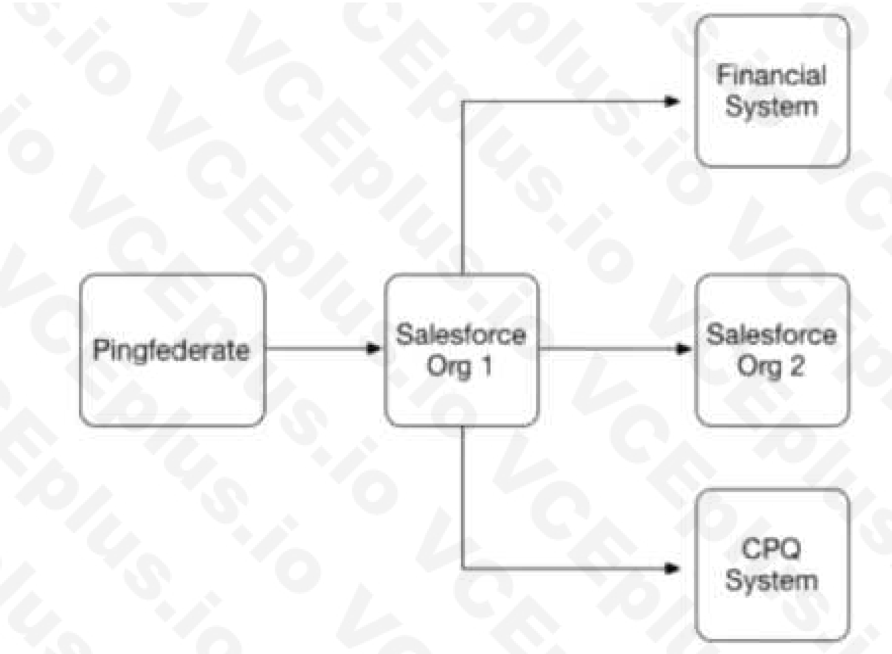
Correct Answer: A
Section:

QUESTION 65
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 UC1
Choose 2 answers

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

Correct Answer: A, C
Section:

QUESTION 66
Universal Containers (UC) has implemented SAML-based Single Sign-On to provide seamless access to its Salesforce Orgs, financial system, and CPQ system. Below is the SSO implementation landscape.



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

A. Financial System and CPQ System are the only Service Providers.

B. Salesforce Org1 and Salesforce Org2 are the only Service Providers.

C. Salesforce Org1 and Salesforce Org2 are acting as Identity Providers.

D. Salesforce Org1 and PingFederate are acting as Identity Providers.

Correct Answer: D
Section:

QUESTION 67
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.

Correct Answer: B, E
Section:

QUESTION 68
Universal Containers wants to implement Single Sign-on for a Salesforce org using an external Identity Provider and corporate identity store.
What type of authentication flow is required to support deep linking'

A. Web Server OAuth SSO flow

B. Service-Provider-Initiated SSO

C. Identity-Provider-initiated SSO

D. StartURL on Identity Provider

Correct Answer: B
Section:

QUESTION 69

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.

Correct Answer: A
Section:

QUESTION 70

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

Correct Answer: B
Section:

QUESTION 71

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 ato successful Customer 360 Truth project.
What are two are 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.

Correct Answer: B, C
Section:

QUESTION 72

A client is planning to rollout multi-factor authentication (MFA) to its internal employees and wants to understand which authentication and verification methods meet the Salesforce criteria for secure authentication.
Which three functions meet the Salesforce criteria for secure mfa?
Choose 3 answers

A. username and password + SMS passcode

B. Username and password + secunty key

C. Third-party single sign-on with Mobile Authenticator app

D. Certificate-based Authentication

E. Lightning Login

Correct Answer: B, C, E
Section:

QUESTION 73
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 appropnate 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 UserProvisionlngRequest object associated with the provisioning flow.

Correct Answer: B, C, E
Section:

QUESTION 74
Universal Containers has multiple Salesforce instances where users receive emails from different instances. Users should be logged into the correct Salesforce instance authenticated by their IdP when clicking on an email link to a Salesforce record.
What should be enabled in Salesforce as a prerequisite?

A. My Domain

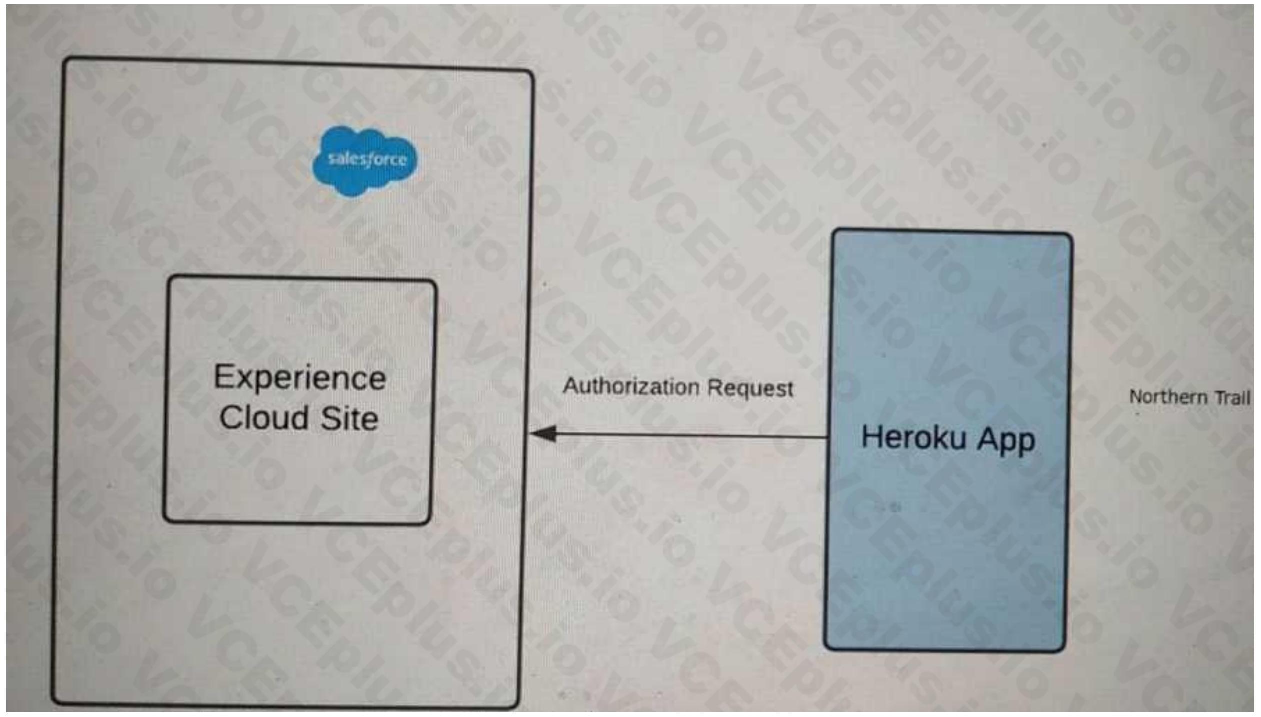
B. External Identity

C. Identity Provider

D. Multi-Factor Authentication

Correct Answer: A
Section:

QUESTION 75
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 communityurl/ services/oauth2/authorize/cookie_value.
D. Authorize third-party service by sending authorization requests to the communityurl/ services/oauth2/authonze/expid_value.

Correct Answer: D
Section:

QUESTION 76
Universal Containers (UC) uses Salesforce for its customer service agents. UC has a proprietary system for order tracking which supports Security Assertion Markup Language (SAML) based single sign-on. The VP of customer service wants to ensure only active Salesforce users should be able to access the order tracking system which is only visible within Salesforce.
What should be done to fulfill the requirement?
Choose 2 answers

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

Correct Answer: A, B
Section:

QUESTION 77
A division of a Northern Trail Outfitters (NTO) purchased Salesforce. NTO uses a third party identity provider (IdP) to validate user credentials against Its corporate Lightweight Directory Access Protocol (LDAP) directory. NTO wants to help employees remember as passwords as possible.
What should an identity architect recommend?

A. Setup Salesforce as a Service Provider to the existing IdP.
B. Setup Salesforce as an IdP to authenticate against the LDAP directory.
C. Use Salesforce connect to synchronize LDAP passwords to Salesforce.
D. Setup Salesforce as an Authentication Provider to the existing IdP.

Correct Answer: A
Section:

QUESTION 78
Universal Containers is using OpenID Connect to enable a connection from their new mobile app to its production Salesforce org.
What should be done to enable the retrieval of the access token status for the OpenID Connect connection?

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

Correct Answer: B
Section:

QUESTION 79
An Identity and Access Management (IAM) architect is tasked with unifying multiple B2C Commerce sites and an Experience Cloud community with a single identity. The solution needs to support more than 1,000 logins per minute.
What should the IAM do to fulfill this requirement?

A. Configure both the community and the commerce sites as OAuth2 RPs (relying party) with an external identity provider.
B. Configure community as a Security Assertion Markup Language (SAML) identity provider and enable Just-in-Time Provisioning to B2C Commerce.
C. Create a default account for capturing all ecommerce contacts registered on the community because personAccount is not supported for this case.
D. Confirm performance considerations with Salesforce Customer Support due to high peaks.

Correct Answer: D
Section:

QUESTION 80
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.

Correct Answer: C
Section:

QUESTION 81

Universal Containers is creating a mobile application that will be secured by Salesforce Identity using the OAuth 2.0 user-agent flow (this flow uses the OAuth 2.0 implicit grant type).
Which three OAuth concepts apply to this flow?
Choose 3 answers

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

Correct Answer: A, B, E
Section:

QUESTION 82
A technology enterprise is planning to implement single sign-on login for users. When users log in to the Salesforce User object custom field, data should be populated for new and existing users.
Which two steps should an identity architect recommend?
Choose 2 answers

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

Correct Answer: A, B
Section:

QUESTION 83
A farming enterprise offers smart farming technology to its farmer customers, which includes a variety of sensors for livestock tracking, pest monitoring, climate monitoring etc. They plan to store all the data in Salesforce.
They would also like to ensure timely maintenance of the Installed sensors.
They have engaged a salesforce Architect to propose an appropriate way to generate sensor Information In Salesforce.
Which OAuth flow should the architect recommend?

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

Correct Answer: A
Section:

QUESTION 84
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.

Correct Answer: A
Section:

QUESTION 85
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.

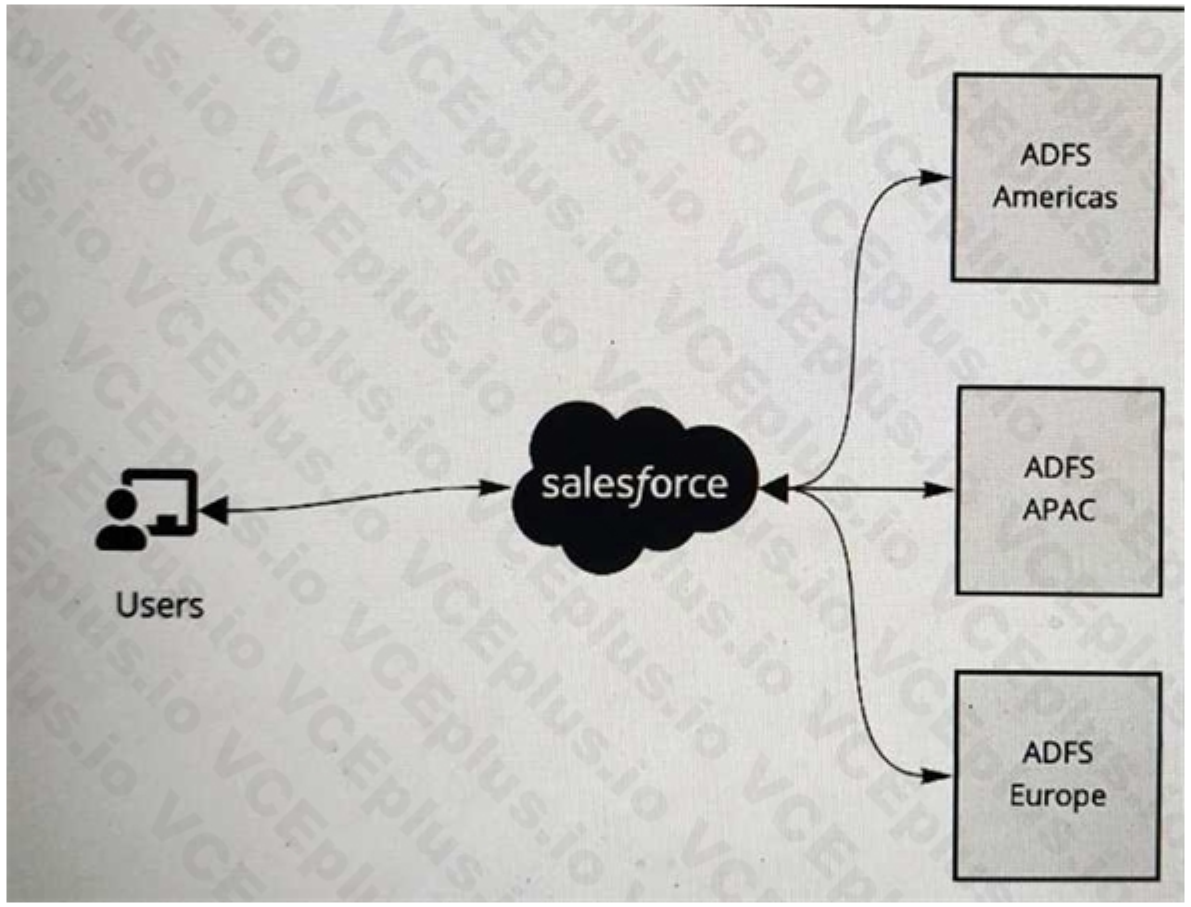
Correct Answer: B
Section:

QUESTION 86
Universal Containers is implementing Salesforce Identity to broker authentication from its enterprise single sign-on (SSO) solution through Salesforce to third party applications using SAML.
What rote does Salesforce Identity play in its relationship with the enterprise SSO system?

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

Correct Answer: C
Section:

QUESTION 87
Refer to the exhibit.



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

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

Correct Answer: B
Section:

QUESTION 88
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:

A. Enter a phone number and/or email address
B. Enter a verification code that is to be sent via email or text.
What is the recommended approach to fulfill this requirement?
C. Create a Login Discovery page and provide a Login Discovery Handler Apex class.
D. Create a custom login page with an Apex controller. The controller has logic to send and verify the identity.
E. Create an Authentication provider and implement a self-registration handler class.
F. Create a custom login flow that uses an Apex controller to verify the phone numbers with the company's verification service.

Correct Answer: A

Section:

QUESTION 89

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.

Correct Answer: B
Section:

QUESTION 90

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.

Correct Answer: B
Section:

QUESTION 91

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 signon (SSO).
Which feature of Identity Connect is applicable for this scenano?

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 licence 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.

Correct Answer: A
Section:

QUESTION 92

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.

Correct Answer: B
Section:

QUESTION 93
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.

Correct Answer: A
Section:

QUESTION 94
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.

Correct Answer: B, D
Section:

QUESTION 95
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.

Correct Answer: C
Section:

QUESTION 96
Universal Containers (UC) uses Salesforce as a CRM and identity provider (IdP) for their Sales Team to seamlessly login to intemaJ portals. The IT team at UC is now evaluating Salesforce to act as an IdP for its remaining employees.
Which Salesforce license is required to fulfill this requirement?

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

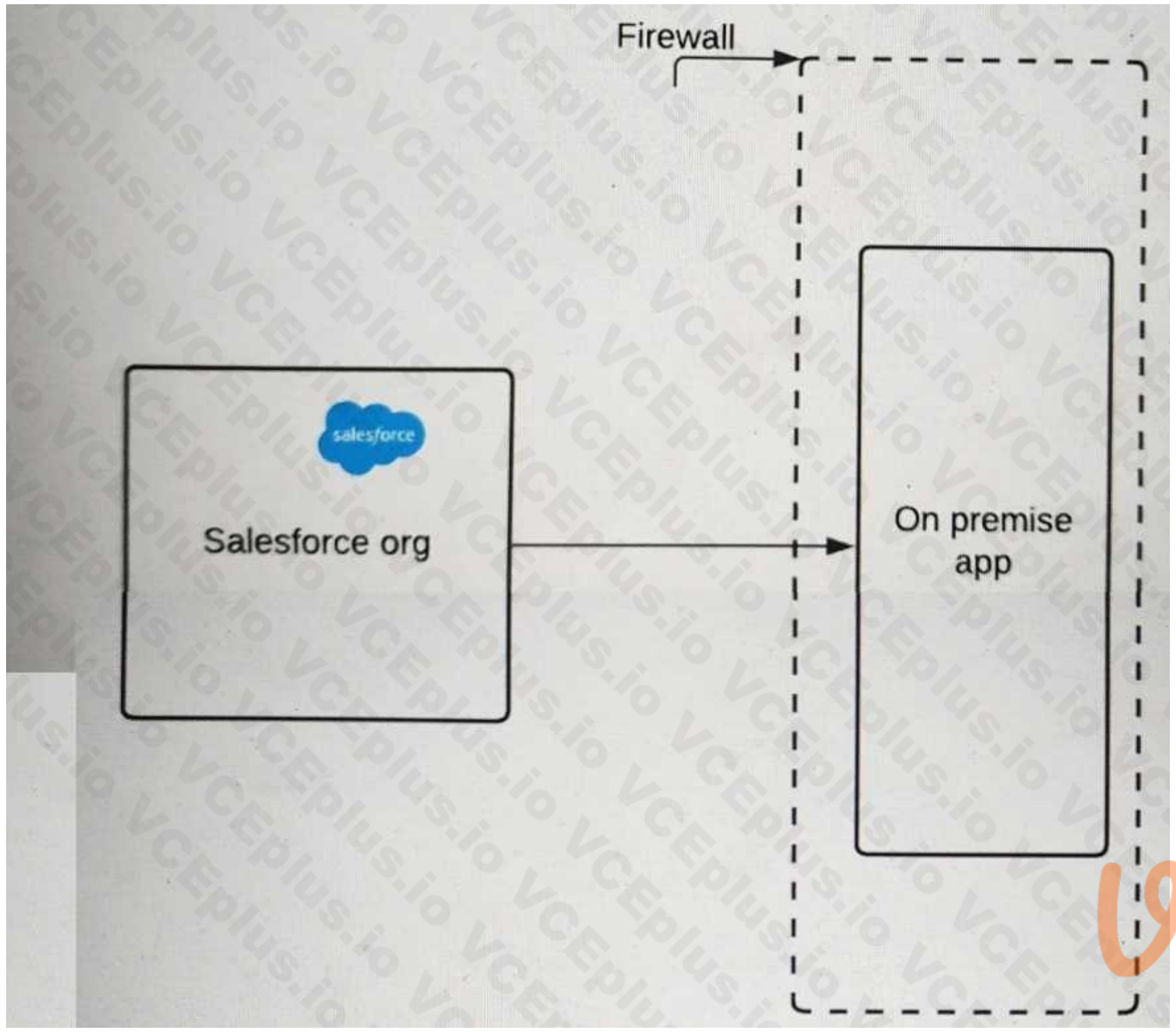
Correct Answer: D
Section:

QUESTION 97
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 ail 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.

Correct Answer: A
Section:

QUESTION 98
Refer to the exhibit.



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.

Correct Answer: B
Section:

QUESTION 99
A Salesforce customer is implementing Sales Cloud and a custom pricing application for its call center agents. An Enterprise single sign-on solution is used to authenticate and sign-in users to all applications. The customer has the following requirements:

A. The development team has decided to use a Canvas app to expose the pricing application to agents.
B. Agents should be able to access the Canvas app without needing to log in to the pricing application.
Which two options should the identity architect consider to provide support for the Canvas app to initiate login for users?
Choose 2 answers
C. Select "Enable as a Canvas Personal App" in the connected app settings.

D. Enable OAuth settings in the connected app with required OAuth scopes for the pricing application.

E. Configure the Canvas app as a connected app and set Admin-approved users as pre-authorized.

F. Enable SAML in the connected app and Security Assertion Markup Language (SAML) Initiation Method as Service Provider Initiated.

Correct Answer: C, D
Section:

QUESTION 100
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.

Correct Answer: D
Section:

QUESTION 101
Universal Containers would like its customers to register and log in to a portal built on Salesforce Experience Cloud. Customers should be able to use their Facebook or Linkedln credentials for ease of use.
Which three steps should an identity architect take to implement social sign-on?
Choose 3 answers

A. Register both Facebook and Linkedln as connected apps.

B. Create authentication providers for both Facebook and Linkedln.

C. Check "Facebook" and "Linkedln" under Login Page Setup.

D. Enable "Federated Single Sign-On Using SAML".

E. Update the default registration handlers to create and update users.

Correct Answer: B, C, E
Section:

QUESTION 102
Universal Containers (UC) operates in Asia, Europe and North America regions. There is one Salesforce org for each region. UC is implementing Customer 360 in Salesforce and has procured External Identity and Customer Community licenses in all orgs.
Customers of UC use Community to track orders and create inquiries. Customers also tend to move across regions frequently.
What should an identity architect recommend to optimize license usage and reduce maintenance overhead?

A. Merge three orgs into one instance of Salesforce. This will no longer require maintaining three separate copies of the same customer.

B. Delete contact/ account records and deactivate user if user moves from a specific region; Sync will no longer be required.

C. Contacts are required since Community access needs to be enabled. Maintenance is a necessary overhead that must be handled via data integration.

D. Enable Contactless User in all orgs and downgrade users from Experience Cloud license to External Identity license once users have moved out of that region.

Correct Answer: C
Section:

QUESTION 103
Northern Trail Outfitters recently acquired a company. Each company will retain its Identity Provider (IdP). Both companies rely extensively on Salesforce processes that send emails to users to take specific actions in Salesforce.
How should the combined companys' employees collaborate in a single Salesforce org, yet authenticate to the appropriate IdP?

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

Correct Answer: D
Section:

QUESTION 104
A consumer products company uses Salesforce to maintain consumer information, including orders.
The company implemented a portal solution using Salesforce Experience Cloud for its consumers where the consumers can log in using their credentials. The company is considering allowing users to login with their Facebook or Linkedln credentials.
Once enabled, what role will Salesforce play?

A. Facebook and Linkedln will be the SPs.
B. Salesforce will be the service provider (SP).
C. Salesforce will be the identity provider (IdP).
D. Facebook and Linkedln will act as the IdPs and SPs.

Correct Answer: B
Section:

QUESTION 105
A service provider (SP) supports both Security Assertion Markup Language (SAML) and OpenID Connect (OIDC).
When integrating this SP with Salesforce, which use case is the determining factor when choosing OIDC or SAML?

A. OIDC is more secure than SAML and therefore is the obvious choice.
B. The SP needs to perform API calls back to Salesforce on behalf of the user after the user logs in to the service provider.
C. If the user has a session on Salesforce, you do not want them to be prompted for a username and password when they login to the SP.
D. They are equivalent protocols and there is no real reason to choose one over the other.

Correct Answer: B
Section:

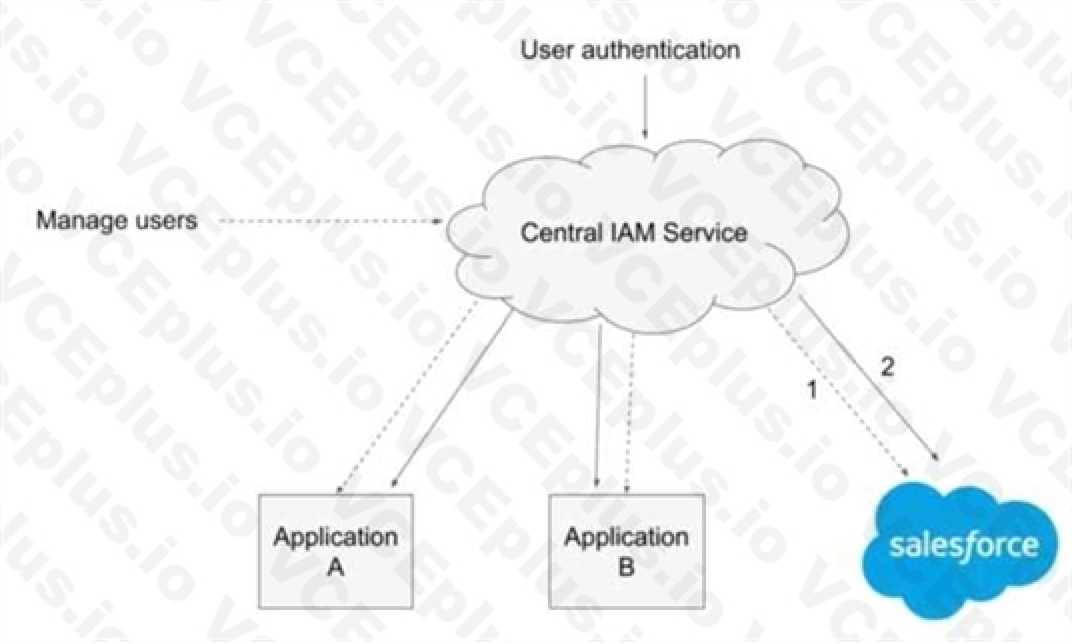
QUESTION 106
Northern Trail Outfitters (NTO) is launching a new sportswear brand on its existing consumer portal built on Salesforce Experience Cloud. As part of the launch, emails with promotional links will be sent to existing customers to log in and claim a discount. The marketing manager would like the portal dynamically branded so that users will be directed to the brand link they clicked on; otherwise, users will view a recognizable NTO-branded page.
The campaign is launching quickly, so there is no time to procure any additional licenses. However, the development team is available to apply any required changes to the portal.
Which approach should the identity architect recommend?

A. Create a full sandbox to replicate the portal site and update the branding accordingly.
B. Implement Experience ID in the code and extend the URLs and endpomts, as required.

C. Use Heroku to build the new brand site and embedded login to reuse identities.
D. Configure an additional community site on the same org that is dedicated for the new brand.

Correct Answer: B
Section:

QUESTION 107
Refer to the exhibit.



An organization has a central cloud-based Identity and Access Management (IAM) Service for authentication and user management, which must be utilized by all applications as follows:
1 - Change of a user status in the central IAM Service triggers provisioning or deprovisioining in the integrated cloud applications.
2 - Security Assertion Markup Language single sign-on (SSO) is used to facilitate access for users authenticated at identity provider (Central IAM Service).
Which approach should an IAM architect implement on Salesforce Sales Cloud to meet the requirements?

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

Correct Answer: A
Section:

QUESTION 108
Which tool should be used to track login data, such as the average number of logins, who logged in more than the average number of times and who logged in during non-business hours?

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

Correct Answer: D
Section:

QUESTION 109

Northern Trail Outfitters want to allow its consumer to self-register on it business-to-consumer (B2C) portal that is built on Experience Cloud. The identity architect has recommended to use Person Accounts.
Which three steps need to be configured to enable self-registration using person accounts?
Choose 3 answers

A. Enable access to person and business account record types under Public Access Settings.

B. Contact Salesforce Support to enable business accounts.

C. Under Login and Registration settings, ensure that the default account field is empty.

D. Contact Salesforce Support to enable person accounts.

E. Set organization-wide default sharing for Contact to Public Read Only.

Correct Answer: A, C, D
Section:

QUESTION 110

Universal Containers (UC) is using Active Directory as its corporate identity provider and Salesforce as its CRM for customer care agents, who use SAML based sign sign-on to login to Salesforce. The default agent profile does not include the Manage User permission. UC wants to dynamically update the agent role and permission sets.
Which two mechanisms are used to provision agents with the appropriate permissions?
Choose 2 answers

A. Use Login Flow in User Context to update role and permission sets.

B. Use Login Flow in System Context to update role and permission sets.

C. Use SAML Just-m-Time (JIT) Handler class run as current user to update role and permission sets.

D. Use SAML Just-in-Time (JIT) handler class run as an admin user to update role and permission sets.

Correct Answer: B, D
Section:

QUESTION 111

Northern Trail Outfitters wants to implement a partner community. Active community users will need to review and accept the community rules, and update key contact information for each community member before their annual partner event.
Which approach will meet this requirement?

A. Create tasks for users who need to update their data or accept the new community rules.

B. Create a custom landing page and email campaign asking all community members to login and verify their data.

C. Create a login flow that conditionally prompts users who have not accepted the new community rules and who have missing or outdated information.

D. Add a banner to the community Home page asking users to update their profile and accept the new community rules.

Correct Answer: C
Section:

QUESTION 112

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

A. Identity Verification

B. Identity Connect

C. Identity Only

D. External Identity

Correct Answer: C
Section:

QUESTION 113
Universal Containers is creating a mobile application that will be secured by Salesforce Identity using the OAuth 2.0 user-agent flow. Application users will authenticate using username and password.
They should not be forced to approve API access in the mobile app or reauthenticate for 3 months.
Which two connected app options need to be configured to fulfill this use case?
Choose 2 answers

A. Set Permitted Users to "Admin approved users are pre-authorized".

B. Set Permitted Users to "All users may self-authorize".

C. Set the Session Timeout value to 3 months.

D. Set the Refresh Token Policy to expire refresh token after 3 months.

Correct Answer: B, D
Section:

QUESTION 114
Universal containers(UC) wants to integrate a third-party reward calculation system with salesforce to calculate rewards. Rewards will be calculated on a schedule basis and update back into salesforce.
The integration between Salesforce and the reward calculation system needs to be secure. Which are the recommended best practices for using Oauth flows in this scenario? Choose 2 answers

A. Oauth refresh token flow

B. Oauth SAML bearer assertion flow

C. Oauthjwt bearer token flow

D. Oauth Username-password flow

Correct Answer: B, C
Section:

QUESTION 115
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.

Correct Answer: A, C
Section:

QUESTION 116
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.

Correct Answer: B
Section:

QUESTION 117
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.

Correct Answer: A, C, E
Section:

QUESTION 118
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.

Correct Answer: B, C
Section:

QUESTION 119
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.

Correct Answer: A
Section:

QUESTION 120

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

Correct Answer: C, D
Section:

QUESTION 121
Universal Containers (UC) wants to provide single sign-on (SSO) for a business-to-consumer (B2C) application using Salesforce Identity.
Which Salesforce license should UC utilize to implement this use case?

A. Identity Only
B. Salesforce Platform
C. External Identity
D. Partner Community

Correct Answer: C
Section: