Practice Exam Questions

Salesforce Certified Identity and Access Management Architect

EXAMKILLER

Help Pass Your Exam At First Try

Salesforce

Exam Identity-and-Access-Management-Architect

Salesforce Certified Identity and Access Management Architect (SP23)

Version: 16.0

[Total Questions: 244]

Question No : 1

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 certfor 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 forsalesforce and a trusted CA-signed cert for the external system

Answer: C,D

Question No : 2

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.

Answer: A,C

Question No : 3

Northern Trail Outfitters (NTO) has an off-boarding process where a terminated employee is firstdisabled in the Lightweight Directory Act Protocol (LDAP) directory, then requests are sent to the various application support teams to finish user deactivations. A terminated employee recently was able to login to NTO's Salesforce instance 24 hours aftertermination, even though the user was disabled in the corporate LDAP directory.

What should an identity architect recommend to prevent this from happening in the future?

A. Create a Just-in-Time provisioning registration handler to ensure users are deactivated in Salesforce as they are disabled in LDAP.
B. Configure an authentication provider to delegate authentication to the LDAP directory.
C. use a login flow to make a callout to the LDAP directory before authenticating the user to Salesforce.
D. Setup anidentity provider (IdP) to authenticate users using LDAP, set up single sign-on to Salesforce and disable Login Form authentication.

Answer: B

Question No : 4

Universal Containers (UC) has an e-commerce website where customers can buy products, make payments and manage their accounts. UC decides to build a Customer Community on Salesforce and wants to allow the customers to access the community from their accounts without logging in again. UC decides to implement an SP-initiated SSO using a SAML-compliant Idp. In this scenario where Salesforce is the Service Provider, which two activities must be performed in Salesforce to make SP-initiated SSO work?
Choose 2answers

A. Configure SAML SSO settings.
B. Create a Connected App.
C. Configure Delegated Authentication.
D. Set up My Domain.

Answer: A,D

Question No : 5

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.

Answer: A,C,D

Question No : 6

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

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

Answer: B

Question No : 7

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 Facebookor 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 theIdPs and SPs.

Answer: B

Question No : 8

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 BearerAssertion Flow

Answer: A

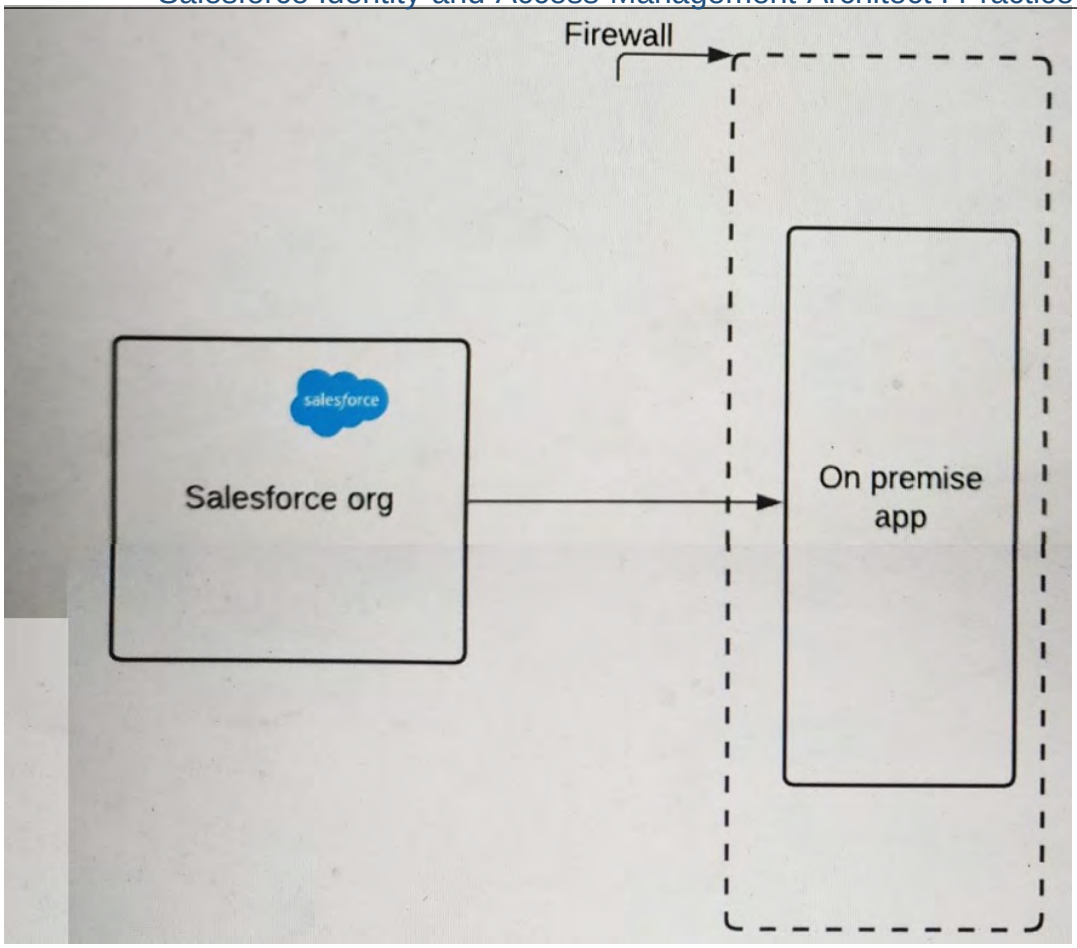
Question No : 9

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

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

Answer: C,D

Question No : 10



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 Certificateand 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 athird-party certificate from Salesforce into the on-premise server.

Answer: B

Question No : 11

Universal containers wants salesforceinbound Oauth-enabled integration clients to use SAML-BASED single Sign-on for authentication. What Oauth flow would be recommended in this scenario?

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

Answer: B

Question No : 12

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 Certificatefrom the Identity Provider expired two weeks ago.
D. The default language for the Identity Provider and Salesforce are Different.

Answer: B,C

Question No : 13

Northern Trail Outfitters (NTO) has a number of employees who do NOT need access Salesforce objects. Trie employees should sign in to a custom Benefits web app using their Salesforce credentials.

Which license should the identity architect recommend to fulfill this requirement?

A. Identity Only License
B. External Identity License
C. Identity Verification Credits Add-on License
D. Identity Connect License

Answer: A

Question No : 14

An identity architect is implementing a mobile-first Consumer Identity Access Management

(CIAM) for externalusers. User authentication is the only requirement. The users email or mobile phone number should be supported as a username.

Which two licenses are needed to meet this requirement?

Choose 2 answers

A. External Identity Licenses
B. Identity Connect Licenses
C. Email Verification Credits
D. SMS verification Credits

Answer: A,D

Question No : 15

Universal Containers wants to secure its Salesforce APIs by using an existing Security Assertion Markup Language (SAML) configuration supports the company's single sign-onprocess to Salesforce,

Which Salesforce OAuth authorization flow should be used?

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

Answer: B

Question No : 16

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

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

Answer: D

Question No : 17

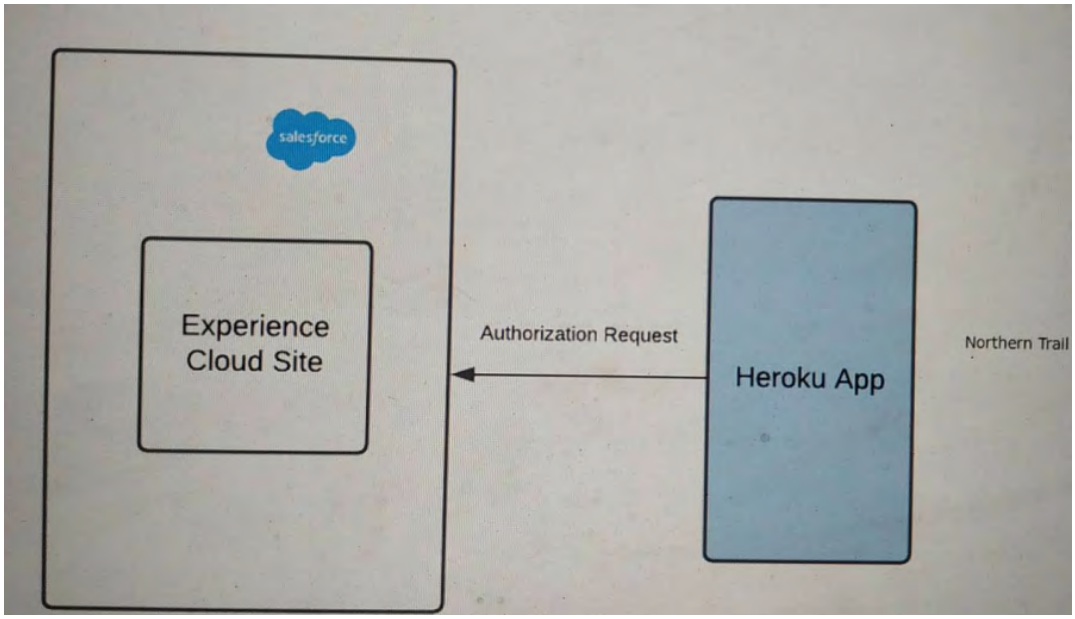
When designing a multi-branded Customer Identity and Access Management solution on the Salesforce Platform, how should an identity architect ensure a specific brand experience in Salesforce is presented?

A. The Experience ID, which can be included in OAuth/Open ID flows and Security Assertion Markup Language (SAML) flows as a URL parameter.
B. Provide a brand picker that the end user can use to select its sub-brand when they arrive on salesforce.
C. Add a custom parameter to the service provider's OAuth/SAML call and implement logic on its login page to apply branding based on the parameters value.
D. The Audience ID, which can be set in a shared cookie.

Answer: A

Question No : 18

Refer to the exhibit.



Outfitters (NTO) is using Experience Cloud as an Identity for its applicationon 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 aboverequirements?

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 routeto different login screens.
C. Authorize third-party service by sending authorization requests to the community-url/services/oauth2/authorize/cookie_value.
D. Authorize third-party service by sending authorization requests to the community-url/services/oauth2/authonze/expid_value.

Answer: D

Question No : 19

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

Answer: B

Question No : 20

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

Answer: D

Question No : 21

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

1. User Authenticates and Authorizes Access

2. Request an Access Token

3. Salesforce Grants an Access Token

4. Request an Authorization Code

5. Salesforce Grants Authorization Code

What is the correct sequence for the authorization flow?

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

Answer: D

Question No : 22

An identity architect is setting up an integration between Salesforce and a third-party system. The third-party system needs to authenticate to Salesforce and then make API calls against the REST API.

One of the requirements is that the solution needs to ensure the third party service providers connected app in Salesforce mini need for end user interaction and maximizes security.

Which OAuth flow should be used to fulfill the requirement?

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

Answer: A

Question No : 23

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 (SAMLJIT) on incoming SAML assertions.
C. Run registration handler on incoming OAuth responses.
D. Call OpenID Connect (OIDC)-userinfo endpoint with a valid access token.

Answer: C

Question No : 24

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 userwill need to do the following:

1. Enter a phone number and/or email address

2. Enter a verification code that is to be sent via email or text.

What is the recommended approach to fulfill this requirement?

A. Create a Login Discovery page and provide a Login Discovery Handler Apex class.
B. Create a custom login page with an Apex controller. The controller has logic to send and verify the identity.
C. Create an Authentication provider and implement a self-registration handler class.
D. Create a custom loginflow that uses an Apex controller to verify the phone numbers with the company's verification service.

Answer: A

Question No : 25

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 bewilling 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 AuthenticationProvider for LinkedIn Social Media Accounts.
C. Create a Custom Apex Registration Handler to handle new and existing users.
D. Configure SSO Settings For Facebook to serve as a SAML Identity Provider.

Answer: B,C

Question No : 26

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

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

Answer: A,B,E

Question No : 27

Northern Trail Outfitters would like to automatically create new employee users in Salesforce with an appropriate profile that maps to its Active Directory Department.

How should an identity architectimplement this requirement?

A. Use the createUser method in the Just-in-Time (JIT) provisioning registration handler to assign the appropriate profile.
B. Use the updateUser method in the Just-in-Time (JIT) provisioning registration handler to assign theappropriate profile.
C. Use a login flow to collect Security Assertion Markup Language attributes and assign the appropriate profile during Just-In-Time

(JIT) provisioning.
D. Make a callout during the login flow to query department from Active Directory to assign the appropriate profile.

Answer: B

Question No : 28

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 thecommerce 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.

Answer: D

Question No : 29

Universal Containers is budding a web application that will connect with the Salesforce API using JWT OAuth Flow.

Which two settings need to be configured in the connect app to support this requirement?

Choose 2 answers

A. The Use DigitalSignature option in the connected app.
B. The "web" OAuth scope in the connected app,
C. The "api" OAuth scope in the connected app.
D. The "edair_api" OAuth scope m the connected app.

Answer: A,C