Salesforce

Exam Questions Identity-and-Access-Management-Designer

Salesforce Certified Identity and Access Management Designer (SP19)

NEW QUESTION 1
Universal Container's (UC) is using Salesforce Experience Cloud site for its container wholesale business. The identity architect wants to an authentication provider for the new site.
Which two options should be utilized in creating an authentication provider? Choose 2 answers

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

Answer: AB

NEW QUESTION 2
universal container plans to develop a custom mobile app for the sales team that will use salesforce for authentication and access management. The mobile app access needs to be restricted to only the sales team. What would be the recommended solution to grant mobile app access to sales users?

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

Answer: B

NEW QUESTION 3
Universal containers (UC) uses a home-grown employee portal for their employees to collaborate. UC decides to use salesforce ideas to allow the employees to post ideas from the employee portal. When clicking some links in the employee portal, the users should be redirected to salesforce, authenticated, and presented with relevant pages. What scope should be requested when using the Oauth token to meet this requirement?

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

Answer: A

NEW QUESTION 4
Universal Containers (UC) has a desktop application to collect leads for marketing campaigns. UC wants to extend this application to integrate with Salesforce to create leads. Integration between the desktop application and Salesforce should be seamless. What Authorization flow should the Architect recommend?

A. JWT Bearer Token Flow
B. Web Server Authentication Flow
C. User Agent Flow
D. Username and Password Flow

Answer: C

NEW QUESTION 5
Northern Trail Outfitters (NTO) is planning to roll out a partner portal for its distributors using Experience Cloud. NTO would like to use an external identity provider (idP) and for partners to register for access to the portal. Each partner should be allowed to register only once to avoid duplicate accounts with Salesforce.
What should a identity architect recommend to create partners?

A. On successful creation of Partners using Self Registration page in Experience Cloud, create identity in Ping.
B. Create a custom page m Experience Cloud to self register partner with Experience Cloud and Ping identity store.
C. Create a custom web page in the Portal and create users in the IdP and Experience Cloud using published APIs.
D. Allow partners to register through the IdP and create partner users in Salesforce through an API.

Answer: B

NEW QUESTION 6
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.

Answer: A

NEW QUESTION 7
Universal containers (UC) is setting up Delegated Authentication to allow employees to log in using their corporate credentials. UC's security team is concerned about the risk of exposing the corporate login service on the Internet and has asked that a reliable trust mechanism be put in place between the login service and salesforce. What mechanism should an architect put in place to enable a trusted connection between the login services and salesforce?

A. Include client ID and client secret in the login header callout.
B. Set up a proxy server for the login service in the DMZ.
C. Require the use of Salesforce security Tokens on password.
D. Enforce mutual Authentication between systems using SSL.

Answer: C

NEW QUESTION 8
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

Answer: C

NEW QUESTION 9
An Architect needs to advise the team that manages the Identity Provider how to differentiate Salesforce from other Service Providers. What SAML SSO setting in Salesforce provides this capability?

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

Answer: C

NEW QUESTION 10
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.

Answer: A

NEW QUESTION 10
Universal Containers (UC) rolling out a new Customer Identity and Access Management Solution will be built on top of their existing Salesforce instance.
Several service providers have been setup and integrated with Salesforce using OpenID Connect to allow for a seamless single sign-on experience. UC has a requirement to limit user access to only a subset of service providers per customer type.
Which two steps should be done on the platform to satisfy the requirement? Choose 2 answers

A. Manage which connected apps a user has access to by assigning authentication providers to the users profile.
B. Assign the connected app to the customer community, and enable the users profile in the Community settings.
C. Use Profiles and Permission Sets to assign user access to Admin Pre-Approved Connected Apps.
D. Set each of the Connected App access settings to Admin Pre-Approved.

Answer: CD

NEW QUESTION 12
Northern Trail Outfitters is implementing a busmess-to-business (B2B) collaboration site using Salesforce Experience Cloud. The partners will authenticate with an existing identity provider and the solution will utilize Security Assertion Markup Language (SAML) to provide single sign-on to Salesforce. Delegated administration will be used in the Expenence Cloud site to allow the partners to administer their users' access.
How should a partner identity be provisioned in Salesforce for this solution?

A. Create only a contact.
B. Create a contactless user.
C. Create a user and a related contact.
D. Create a person account.

Answer: C

NEW QUESTION 15
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.

Answer: AD

NEW QUESTION 18
An architect needs to advise the team that manages the identity provider how to differentiate salesforce from other service providers. What SAML SSO setting in salesforce provides this capability?

A. Entity id
B. Issuer
C. Identity provider login URL
D. SAML identity location

Answer: A

NEW QUESTION 21
Northern Trail Outfitters (NTO) wants to give customers the ability to submit and manage issues with their purchases. It is important for NTO to give its customers the ability to login with their Amazon credentials.
What should an identity architect recommend to meet these requirements?

A. Configure a predefined authentication provider for Amazon.
B. Create a custom external authentication provider for Amazon.
C. Configure an OpenID Connect Authentication Provider for Amazon.
D. Configure Amazon as a connected app.

Answer: C

NEW QUESTION 25
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

Answer: CD

NEW QUESTION 26
Universal containers (UC) would like to enable self - registration for their salesforce partner community users. UC wants to capture some custom data elements from the partner user, and based on these data elements, wants to assign the appropriate profile and account values. Which two actions should the architect recommend to UC? Choose 2 answers

A. Modify the communitiesselfregcontroller to assign the profile and account.
B. Modify the selfregistration trigger to assign profile and account.
C. Configure registration for communities to use a custom visualforce page.
D. Configure registration for communities to use a custom apex controller.

Answer: AC

NEW QUESTION 28
Universal containers wants to implement single Sign-on for a salesforce org using an external identity provider and corporate identity store. What type of Authentication flow is required to support deep linking?

A. Web server Oauth SSO flow.
B. Identity-provider-initiated SSO
C. Service-provider-initiated SSO
D. Start URL on identity provider

Answer: C

NEW QUESTION 31
A global company's Salesforce Identity Architect is reviewing its Salesforce production org login history and is seeing some intermittent Security Assertion Markup Language (SAML SSO) 'Replay Detected and Assertion Invalid' login errors.
Which two issues would cause these errors? Choose 2 answers

A. The subject element is missing from the assertion sent to salesforce.
B. The certificate loaded into SSO configuration does not match the certificate used by the IdP.
C. The current time setting of the company's identity provider (IdP) and Salesforce platform is out of sync by more than eight minutes.
D. The assertion sent to 5alesforce contains an assertion ID previously used.

Answer: AD

NEW QUESTION 32
Which two things should be done to ensure end users can only use single sign-on (SSO) to login in to Salesforce?
Choose 2 answers

A. Enable My Domain and select "Prevent login from https://login.salesforce.com".
B. Request Salesforce Support to enable delegated authentication.
C. Once SSO is enabled, users are only able to login using Salesforce credentials.
D. Assign user "is Single Sign-on Enabled" permission via profile or permission set.

Answer: AD

NEW QUESTION 36
Universal containers (UC) employees have salesforce access from restricted ip ranges only, to protect against unauthorised access. UC wants to rollout the salesforce1 mobile app and make it accessible from any location. Which two options should an architect recommend? Choose 2 answers

A. Relax the ip restriction in the connect app settings for the salesforce1 mobile app
B. Use login flow to bypass ip range restriction for the mobile app.
C. Relax the ip restriction with a second factor in the connect app settings for salesforce1 mobile app
D. Remove existing restrictions on ip ranges for all types of user access.

Answer: AB

NEW QUESTION 37
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 synced between Salesforce and the third party system. However, UC quickly notices that changes to user roles in Salesforce are not getting synched to the third-party system. What is the most likely reason for this behaviour?

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

Answer: A

NEW QUESTION 41
Users logging into Salesforce are frequently prompted to verify their identity.
The identity architect is required to provide recommendations so that frequency of prompt verification can be reduced.
What should the identity architect recommend to meet the requirement?

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

Answer: B

NEW QUESTION 46
Universal Containers (UC) is building a custom Innovation platform on their Salesforce instance. The Innovation platform will be written completely in Apex and Visualforce and will use custom objects to store the Data. UC would like all users to be able to access the system without having to log in with Salesforce credentials. UC will utilize a third-party idp using SAML SSO. What is the optimal Salesforce licence type for all of the UC employees?

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

Answer: D

NEW QUESTION 50
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.

Answer: D

NEW QUESTION 55
Ttie executive sponsor for an organization has asked if Salesforce supports the ability to embed a login widget into its service providers in order to create a more seamless user experience.
What should be used and considered before recommending it as a solution on the Salesforce Platform?

A. OpenID Connect Web Server Flo
B. Determine if the service provider is secure enough to store the client secret on.
C. Embedded Logi
D. Identify what level of UI customization will be required to make it match the service providers look and feel.
E. Salesforce REST api

F. Ensure that Secure Sockets Layer (SSL) connection for the integration is used.
G. Embedded Logi
H. Consider whether or not it relies on third party cookies which can cause browser compatibility issues.

Answer: C

NEW QUESTION 58

Universal containers wants to set up SSO for a selected group of users to access external applications from salesforce through App launcher. Which three steps must be completed in salesforce to accomplish the goal?

A. Associate user profiles with the connected Apps.
B. Complete my domain and Identity provider setup.
C. Create connected apps for the external applications.
D. Complete single Sign-on settings in security controls.
E. Create named credentials for each external system.

Answer: ABC

NEW QUESTION 59

An identity architect wants to secure Salesforce APIs using Security Assertion Markup Language (SAML). For secunty purposes, administrators will need to authorize the applications that will be consuming the APIs.
Which Salesforce OAuth authorization flow should be used7

A. OAuth 2-0 SAML Bearer Assertion Flow
B. OAuth 2.0 JWT Bearer Flow
C. SAML Assertion Flow
D. OAuth 2.0 User-Agent Flow

Answer: C

NEW QUESTION 60

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.

Answer: D

NEW QUESTION 64

A global fitness equipment manufacturer uses Salesforce to manage its sales cycle. The manufacturer has a custom order fulfillment app that needs to request order data from Salesforce. The order fulfillment app needs to integrate with the Salesforce API using OAuth 2.0 protocol.
What should an identity architect use to fulfill this requirement?

A. Canvas App Integration
B. OAuth Tokens
C. Authentication Providers
D. Connected App and OAuth scopes

Answer: D

NEW QUESTION 67

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

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

Answer: C

NEW QUESTION 71

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 most likely to cause of the issue?

A. The use of high assurance sections are required for the connected App.
B. The users do not have the correct permission set assigned to them.
C. The connected App setting "All users may self-authorize" is enabled.
D. The salesforce administrators gave revoked the Oauth authorization.

Answer: B

NEW QUESTION 74

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

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

Answer: C

NEW QUESTION 79
Which two security risks can be mitigated by enabling Two-Factor Authentication (2FA) in Salesforce? Choose 2 answers

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

Answer: BC

NEW QUESTION 82
which three are features of federated Single Sign-on solutions? Choose 3 answers

A. It federates credentials control to authorized applications.
B. It establishes trust between Identity store and service provider.
C. It solves all identity and access management problems.
D. It improves affiliated applications adoption rates.
E. It enables quick and easy provisioning and deactivating of users.

Answer: BCE

NEW QUESTION 83
Universal containers (UC) is setting up their customer Community self-registration process. They are uncomfortable with the idea of assigning new users to a default account record. What will happen when customers self-register in the community?

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

Answer: A

NEW QUESTION 86
An Identity architect works for a multinational, multi-brand organization. As they work with the organization to understand their Customer Identity and Access Management requirements, the identity architect learns that the brand experience is different for each of the customer's sub-brands and each of these branded experiences must be carried through the login experience depending on which sub-brand the user is logging into.
Which solution should the architect recommend to support scalability and reduce maintenance costs, if the organization has more than 150 sub-brands?

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

Answer: A

NEW QUESTION 88
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

Answer: B

NEW QUESTION 93
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.

Answer: A

NEW QUESTION 96
Northern Trail Outfitters (NTO) has an existing custom business-to-consumer (B2C) website that does NOT support single sign-on standards, such as Security Assertion Markup Language (SAMi) or OAuth. NTO wants to use Salesforce Identity to register and authenticate new customers on the website.
Which two Salesforce features should an identity architect use in order to provide username/password authentication for the website?
Choose 2 answers

A. Identity Connect
B. Delegated Authentication
C. Connected Apps
D. Embedded Login

Answer: BD

NEW QUESTION 98
What are three capabilities of Delegated Authentication? Choose 3 answers

A. It can be assigned by Custom Permissions.
B. It can connect to SOAP services.
C. It can be assigned by Permission Sets.
D. It can be assigned by Profiles.
E. It can connect to REST services.

Answer: BCE

NEW QUESTION 101
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

Answer: B

NEW QUESTION 104
Northern Trail Outfitters (NTO) leverages Microsoft Active Directory (AD) for management of employee usernames, passwords, permissions, and asset access. NTO also owns a third-party single sign-on (SSO) solution. The third-party party SSO solution is used for all corporate applications, including Salesforce.
NTO has asked an architect to explore Salesforce Identity Connect for automatic provisioning and deprovisiorung of users in Salesforce.
What role does identity Connect play in the outlined requirements?

A. Service Provider
B. Single Sign-On
C. Identity Provider
D. User Management

Answer: D

NEW QUESTION 105
Universal containers (UC) would like to enable SAML-BASED SSO for a salesforce partner community. UC has an existing ldap identity store and a third-party portal. They would like to use the existing portal as the primary site these users access, but also want to allow seamless access to the partner community. What SSO flow should an architect recommend?

A. User-Agent
B. IDP-initiated
C. Sp-Initiated
D. Web server

Answer: B

NEW QUESTION 106
Universal Containers (UC) has a Customer Community that uses Facebook for of authentication. UC would like to ensure that changes in the Facebook profile are
65. reflected on the appropriate Customer Community user. How can this requirement be met?

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

Answer: D

NEW QUESTION 108

Northern Trail Outfitters (NTO) is setting up Salesforce to authenticate users with an external identity provider. The NTO Salesforce Administrator is having trouble getting things setup.
What should an identity architect use to show which part of the login assertion is fading?

A. SAML Metadata file importer
B. Identity Provider Metadata download
C. Connected App Manager
D. Security Assertion Markup Language Validator

Answer: D

NEW QUESTION 110
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 againstSalesforce 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.

Answer: AC

NEW QUESTION 115
Universal containers (UC) has implemented SAML SSO to enable seamless access across multiple applications. UC has regional salesforce orgs and wants it's users to be able to access them from their main Salesforce org seamless. Which action should an architect recommend?

A. Configure the main salesforce org as an Authentication provider.
B. Configure the main salesforce org as the Identity provider.
C. Configure the regional salesforce orgs as Identity Providers.
D. Configure the main Salesforce org as a service provider.

Answer: B

NEW QUESTION 120
The security team at Universal containers(UC) has identified exporting reports as a high-risk action and would like to require users to be logged into salesforce with their active directory (AD) credentials when doing so. For all other uses of Salesforce, Users should be allowed to use AD credentials or salesforce credentials. What solution should be recommended to prevent exporting reports except when logged in using AD credentials while maintaining the ability to view reports when logged in with salesforce credentials?

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

Answer: C

NEW QUESTION 124
Containers (UC) has decided to implement a federated single Sign-on solution using a third-party Idp. In reviewing the third-party products, they would like to ensure the product supports the automated provisioning and deprovisioning of users. What are the underlining mechanisms that the UC Architect must ensure are part of the product?

A. SOAP API for provisioning; Just-in-Time (JIT) for Deprovisioning.
B. Just-In-time (JIT) for Provisioning; SOAP API for Deprovisioning.
C. Provisioning API for both Provisioning and Deprovisioning.
D. Just-in-Time (JIT) for both Provisioning and Deprovisioning.

Answer: D

NEW QUESTION 125
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

Answer: ABE

NEW QUESTION 128
Universal Containers (UC) has Active Directory (AD) as their enterprise identity store and would like to use it for Salesforce user authentication. UC expects to synchronize user data between Salesforce and AD and Assign the appropriate Profile and Permission Sets based on AD group membership. What would be the optimal way to implement SSO?

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

Answer: D

NEW QUESTION 130
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

Answer: ACD

NEW QUESTION 131
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.

Answer: BD

NEW QUESTION 134
The CIO of universal containers(UC) wants to start taking advantage of the refresh token capability for the UC applications that utilize Oauth 2.0. UC has listed an architect to analyze all of the applications that use Oauth flows to. See where refresh Tokens can be applied. Which two OAuth flows should the architect consider in their evaluation? Choose 2 answers

A. Web server
B. Jwt bearer token
C. User-Agent
D. Username-password

Answer: AC

NEW QUESTION 135
Universal Containers (UC) has an existing web application that it would like to access from Salesforce without requiring users to re-authenticate. The web application is owned UC and the UC team that is responsible for it is willing to add new javascript code and/or libraries to the application. What implementation should an Architect recommend to UC?

A. Create a Canvas app and use Signed Requests to authenticate the users.
B. Rewrite the web application as a set of Visualforce pages and Apex code.
C. Configure the web application as an item in the Salesforce App Launcher.
D. Add the web application as a ConnectedApp using OAuth User-Agent flow.

Answer: A

NEW QUESTION 137
Universal Containers (UC) has an existing Salesforce org configured for SP-Initiated SAML SSO with their Idp. A second Salesforce org is being introduced into the environment and the IT team would like to ensure they can use the same Idp for new org. What action should the IT team take while implementing the second org?

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

Answer: B

NEW QUESTION 141
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.

Answer: C

NEW QUESTION 145
Universal containers (UC) wants users to authenticate into their salesforce org using credentials stored in a custom identity store. UC does not want to purchase or use a third-party Identity provider. Additionally, UC is extremely wary of social media and does not consider it to be trust worthy. Which two options should an architect recommend to UC? Choose 2 answers

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

Answer: CD

NEW QUESTION 146
How should an Architect automatically redirect users to the login page of the external Identity provider when using an SP-Initiated SAML flow with Salesforce as a Service Provider?

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

Answer: C

NEW QUESTION 149
Universal Containers (UC) is using a custom application that will act as the Identity Provider and will generate SAML assertions used to log in to Salesforce. UC is considering including custom parameters in the SAML assertion. These attributes contain sensitive data and are needed to authenticate the users. The assertions are submitted to salesforce via a browser form post. The majority of the users will only be able to access Salesforce via UC's corporate network, but a subset of admins and executives would be allowed access from outside the corporate network on their mobile devices. Which two methods should an Architect consider to ensure that the sensitive data cannot be tampered with, nor accessible to anyone while in transit?

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

Answer: AC

NEW QUESTION 153
A web service is developed that allows secure access to customer order status on the Salesforce Platform, The service connects to Salesforce through a connected app with the web server flow. The following are the required actions for the authorization flow:
* 1. User Authenticates and Authorizes Access
* 2. Request an Access Token
* 3. Salesforce Grants an Access Token
* 4. Request an Authorization Code
* 5. Salesforce Grants Authorization Code
What is the correct sequence for the authorization flow?

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

Answer: D

NEW QUESTION 158
Universal containers (UC) has a custom, internal-only, mobile billing application for users who are commonly out of the office. The app is configured as a connected App in salesforce. Due to the nature of this app, UC would like to take the appropriate measures to properly secure access to the app. Which two are recommendations to make the UC? Choose 2 answers

A. Disallow the use of single Sign-on for any users of the mobile app.
B. Require high assurance sessions in order to use the connected App
C. Use Google Authenticator as an additional part of the logical processes.
D. Set login IP ranges to the internal network for all of the app users profiles.

Answer: BC

NEW QUESTION 162
Which two considerations should be made when implementing Delegated Authentication? Choose 2 answers

A. The authentication web service can include custom attributes.
B. It can be used to authenticate API clients and mobile apps.
C. It requires trusted IP ranges at the User Profile level.
D. Salesforce servers receive but do not validate a user's credentials.
E. Just-in-time Provisioning can be configured for new users.

Answer: BE

NEW QUESTION 163
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:
* 1. The development team has decided to use a Canvas app to expose the pricing application to agents.
* 2. 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

A. Select "Enable as a Canvas Personal App" in the connected app settings.
B. Enable OAuth settings in the connected app with required OAuth scopes for the pricing application.
C. Configure the Canvas app as a connected app and set Admin-approved users as pre-authorized.
D. Enable SAML in the connected app and Security Assertion Markup Language (SAML) Initiation Method as Service Provider Initiated.

Answer: CD

NEW QUESTION 166
Universal containers (UC) has a classified information system that it's call centre team uses only when they are working on a case with a record type of "classified". They are only allowed to access the system when they own an open "classified" case, and their access to the system is removed at all other times. They would like to implement SAML SSO with salesforce as the IDP, and automatically allow or deny the staff's access to the classified information system based on whether they currently own an open "classified" case record when they try to access the system using SSO. What is the recommended solution for automatically allowing or denying access to the classified information system based on the open "classified" case record criteria?

A. Use a custom connected App handler using apex to dynamically allow access to the system based on whether the staff owns any open "classified" cases.
B. Use apex trigger on case to dynamically assign permission sets that grant access when a user is assigned with an open "classified" case, and remove it when the case is closed.
C. Use custom SAML jit provisioning to dynamically query the user's open "classified" cases whenattempting to access the classified information system
D. Use salesforce reports to identify users that currently owns open "classified" cases and should be granted access to the classified information system.

Answer: A

NEW QUESTION 167
Universal Containers (UC) built an integration for their employees to post, view, and vote for ideas in Salesforce from an internal Company portal. When ideas are posted in Salesforce, links to the ideas are created in the company portal pages as part of the integration process. The Company portal connects to Salesforce using OAuth. Everything is working fine, except when users click on links to existing ideas, they are always taken to the Ideas home page rather than the specific idea, after authorization. Which OAuth URL parameter can be used to retain the original requested page so that a user can be redirected correctly after OAuth authorization?

A. Redirect_uri
B. State
C. Scope
D. Callback_uri

Answer: A

NEW QUESTION 172
Universal Containers (UC) has a Customer Community that uses Facebook for Authentication. UC would like to ensure that Changes in the Facebook profile are reflected on the appropriate Customer Community user: How can this requirement be met?

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

Answer: A

NEW QUESTION 174
Universal containers (UC) has implemented SAML -based single Sign-on for their salesforce application. UC is using pingfederate as the Identity provider. To access salesforce, Users usually navigate to a bookmarked link to my domain URL. What type of single Sign-on is this?

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

Answer: A

NEW QUESTION 177
Northern Trail Outfitters (NTO) wants its customers to use phone numbers to log in to their new digital portal, which was designed and built using Salesforce Experience Cloud. In order to access the portal, the user will need to do the following:
* 1. Enter a phone number and/or email address
* 2. Enter a verification code that is to be sent via email or text.
What is the recommended approach to fulfill this requirement?

A. Create a Login Discovery page and provide a Login Discovery Handler Apex class.
B. Create a custom login page with an Apex controlle

C. The controller has logic to send and verify the identity.
D. Create an Authentication provider and implement a self-registration handler class.
E. Create a custom login flow that uses an Apex controller to verify the phone numbers with the company's verification service.

Answer: D

NEW QUESTION 180
Universal Containers (UC) has decided to replace the homegrown customer portal with Salesforce Experience Cloud. UC will continue to use its third-party single sign-on (SSO) solution that stores all of its customer and partner credentials.
The first time a customer logs in to the Experience Cloud site through SSO, a user record needs to be created automatically.
Which solution should an identity architect recommend in order to automatically provision users in Salesforce upon login?

A. Just-in-Time (JIT) provisioning
B. Custom middleware and web services
C. Custom login flow and Apex handler
D. Third-party AppExchange solution

Answer: A

NEW QUESTION 184
customer service representatives at Universal containers (UC) are complaining that whenever they click on links to case records and are asked to login with SAML SSO, they are being redirected to the salesforce home tab and not the specific case record. What item should an architect advise the identity team at UC to investigate first?

A. My domain is configured and active within salesforce.
B. The salesforce SSO settings are using http post
C. The identity provider is correctly preserving the Relay state
D. The users have the correct Federation ID within salesforce.

Answer: C

NEW QUESTION 186
Universal containers (UC) has implemented a multi-org strategy and would like to centralize the management of their salesforce user profiles. What should the architect recommend to allow salesforce profiles to be managed from a central system of record?

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

Answer: A

NEW QUESTION 188
Universal Containers (UC) has five Salesforce orgs (UC1, UC2, UC3, UC4, UC5). of Every user that is in UC2, UC3, UC4, and UC5 is also in UC1, however not all users 65* have access to every org. Universal Containers would like to simplify the authentication process such that all Salesforce users need to remember one set of credentials. UC would like to achieve this with the least impact to cost and maintenance. What approach should an Architect recommend to UC?

A. Purchase a third-party Identity Provider for all five Salesforce orgs to use and set up JIT user provisioning on all other orgs.
B. Purchase a third-party Identity Provider for all five Salesforce orgs to use, but don't set up JIT user provisioning for other orgs.
C. Configure UC1 as the Identity Provider to the other four Salesforce orgs and set up JIT user provisioning on all other orgs.
D. Configure UC1 as the Identity Provider to the other four Salesforce orgs, but don't set up JIT user provisioning for other orgs.

Answer: B

NEW QUESTION 190
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

Answer: C

NEW QUESTION 192
Universal containers uses an Employee portal for their employees to collaborate. employees access the portal from their company's internal website via SSO. It is set up to work with Active Directory. What is the role of Active Directory in this scenario?

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

Answer: C

NEW QUESTION 194
Universal Containers (UC) employees have Salesforce access from restricted IP ranges only, to protect against unauthorised access. UC wants to roll out the Salesforce1 mobile app and make it accessible from any location. Which two options should an Architect recommend? Choose 2 answers

A. Relax the IP restriction with a second factor in the Connect App settings for Salesforce1 mobile app.
B. Remove existing restrictions on IP ranges for all types of user access.
C. Relax the IP restrictions in the Connect App settings for the Salesforce1 mobile app.
D. Use Login Flow to bypass IP range restriction for the mobile app.

Answer: AC

NEW QUESTION 197
A group of users try to access one of Universal Containers' Connected Apps and receive the following error message: " Failed: Not approved for access." What is the most likely cause of this issue?

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

Answer: C

NEW QUESTION 200
Universal Containers (UC) would like its community users to be able to register and log in with Linkedin or Facebook Credentials. UC wants users to clearly see Facebook &Linkedin Icons when they register and login. What are the two recommended actions UC can take to achieve this Functionality? Choose 2 answers

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

Answer: AB

NEW QUESTION 205
A company's external application is protected by Salesforce through OAuth. The identity architect for the project needs to limit the level of access to the data of the protected resource in a flexible way.
What should be done to improve security?

A. Select "Admin approved users are pre-authonzed" and assign specific profiles.
B. Create custom scopes and assign to the connected app.
C. Define a permission set that grants access to the app and assign to authorized users.
D. Leverage external objects and data classification policies.

Answer: B

NEW QUESTION 210
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.

Answer: AD

NEW QUESTION 215
An Architect has configured a SAML-based SSO integration between Salesforce and an external Identity provider and is ready to test it. When the Architect attempts to log in to Salesforce using SSO, the Architect receives a SAML error. Which two optimal actions should the Architect take to troubleshoot the issue?

A. Ensure the Callback URL is correctly set in the Connected Apps settings.
B. Use a browser that has an add-on/extension that can inspect SAML.
C. Paste the SAML Assertion Validator in Salesforce.
D. Use the browser's Development tools to view the Salesforce page's markup.

Answer: BC

NEW QUESTION 217
Northern Trail Outfitters (NTO) is planning to build a new customer service portal and wants to use passwordless login, allowing customers to login with a one-time passcode sent to them via email or SMS.
How should the quantity of required Identity Verification Credits be estimated?

A. Each community comes with 10,000 Identity Verification Credits per month and only customers with more than 10,000 logins a month should estimate additional SMS verifications needed.
B. Identity Verification Credits are consumed with each SMS (text message) sent and should be estimated based on the number of login verification challenges for SMS verification users.

C. Identity Verification Credits are consumed with each verification sent and should be estimated based on the number of logins that will incur a verification challenge.

D. Identity Verification Credits are a direct add-on license based on the number of existing member-based or login-based Community licenses.

Answer: B

NEW QUESTION 221
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

Identity-and-Access-Management-Designer Practice Exam Features:

* Identity-and-Access-Management-Designer Questions and Answers Updated Frequently

* Identity-and-Access-Management-Designer Practice Questions Verified by Expert Senior Certified Staff

* Identity-and-Access-Management-Designer Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* Identity-and-Access-Management-Designer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The Identity-and-Access-Management-Designer Practice Test Here