IDENTITY-AND-ACCESS-MANAGEMENT-DESIGNER Q&As

Salesforce Certified Identity and Access Management Designer

Pass Salesforce IDENTITY-AND-ACCESS-MANAGEMENT-DESIGNER Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/identity-and-access-management-designer.html

100% Passing Guarantee
100% Money Back Assurance

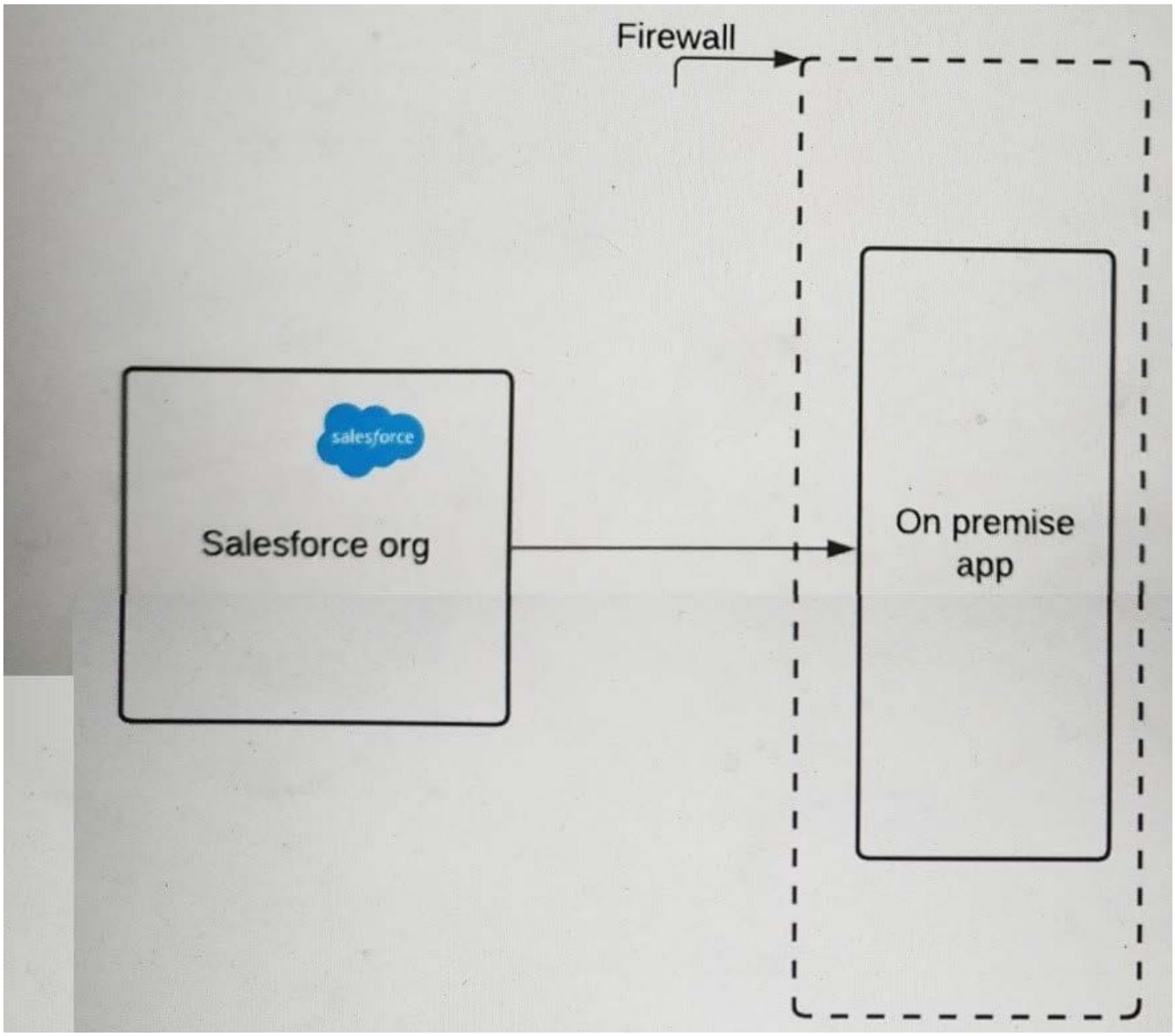
Following Questions and Answers are all new published by Salesforce Official Exam Center

QUESTION 1

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

QUESTION 2

A financial enterprise is planning to set up a user authentication mechanism to login to the Salesforce system. Due to regulatory requirements, the CIO of the company wants user administration, including passwords and authentication requests, to be managed by an external system that is only accessible via a SOAP webservice.

Which authentication mechanism should an identity architect recommend to meet the requirements?

A. OAuth Web-Server Flow

B. Identity Connect

C. Delegated Authentication

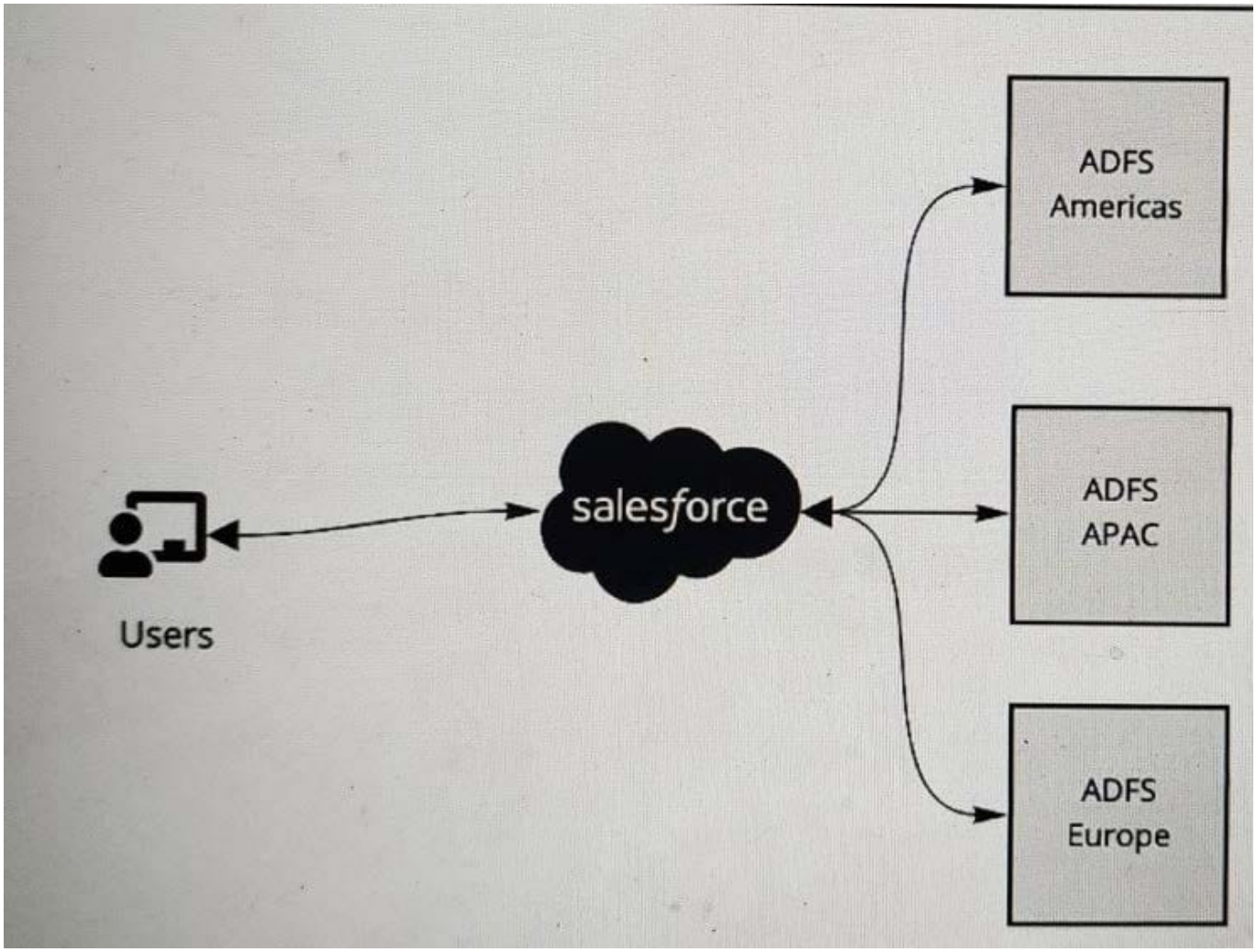
D. Just-in-Time Provisioning

Correct Answer: C

QUESTION 3

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

QUESTION 4

An identity architect has built a native mobile application and plans to integrate it with a Salesforce Identity solution. The following are the requirements for the solution:

1.

Users should not have to login every time they use the app.

2.

The app should be able to make calls to the Salesforce REST API.

3.

End users should NOT see the OAuth approval page.

How should the identity architect configure the Salesforce connected app to meet the requirements?

A. Enable the API Scope and Offline Access Scope, upload a certificate so JWT Bearer Flow can be used and then set the connected app access settings to "Admin Pre- Approved".

B. Enable the API Scope and Offline Access Scope on the connected app, and then set the connected app to access settings to \\'Admin Pre-Approved".

C. Enable the Full Access Scope and then set the connected app access settings to "Admin Pre-Approved".

D. Enable the API Scope and Offline Access Scope on the connected app, and then set the Connected App access settings to "User may self authorize".

Correct Answer: A

QUESTION 5

Universal Containers allows employees to use a mobile device to access Salesforce for daily operations using a hybrid mobile app. This app uses Mobile software development kits (SDK), leverages refresh token to regenerate access token when required and is distributed as a private app.

The chief security officer is rolling out an org wide compliance policy to enforce re- venfication of devices if an employee has not logged in from that device in the last week.

Which connected app setting should be leveraged to comply with this policy change?

A. Scope - Deny refresh_token scope for this connected app.

B. Refresh Token Policy - Expire the refresh token if it has not been used for 7 days.

C. Session Policy - Set timeout value of the connected app to 7 days.

D. Permitted User - Ask admins to maintain a list of users who are permitted based on last login date.

Correct Answer: B