Marvelous Salesforce - Integration-Architect - Reliable Salesforce Certified Integration Architect Test Tutorial

BONUS!!! Download part of PracticeMaterial Integration-Architect dumps for free: https://drive.google.com/open?id=1lvC5Lv_SwTWmuC-FkTt84po6Fw08Xoj_

These Salesforce Integration-Architect exam questions give you an idea about the final Salesforce Integration-Architect exam questions formats, exam question structures, and best possible answers, and you will also enhance your exam time management skills. Finally, at the end of Integration-Architect Exam Practice test you will be ready to pass the final Integration-Architect exam easily. Best of luck in Salesforce Certified Integration Architect (Integration-Architect) exam and professional career!!!

Salesforce Integration-Architect Certification Exam is designed to test an individual's knowledge and skills in the area of integrating Salesforce with other external systems. Salesforce Certified Integration Architect certification is intended for professionals who have experience in designing and implementing complex integrations between Salesforce and other systems, and who are looking to demonstrate their expertise in this area. Integration-Architect Exam focuses on a range of topics, including data integration, security and access control, messaging, APIs, and more.

>> Reliable Integration-Architect Test Tutorial <<

Integration-Architect Certification Training and Integration-Architect Test Torrent - Salesforce Certified Integration Architect Guide Torrent - PracticeMaterial

Three versions are available for Integration-Architect study materials, and you can choose the most suitable one according to your own needs. Integration-Architect PDF version is printable, and you can print them and take some notes on them if you want. Integration-Architect Soft test engine can be used in more than 200 personal computers, and they support MS operating system. Integration-Architect Online Test engine is convenient and easy to learn, and it supports all web browsers. You can have a general review of what you have learned. Just have a try, and there is always a version for you.

Achieving the Salesforce Integration-Architect Certification will enable you to demonstrate your expertise in designing and implementing complex integrations. Salesforce Certified Integration Architect certification will also enhance your career prospects by making you more attractive to potential employers. Additionally, the certification will give you access to a network of certified professionals who can provide you with support and guidance throughout your career.

Salesforce Certified Integration Architect Sample Questions (Q76-Q81):

NEW QUESTION # 76
What is the first thing an Integration Architect should validate if a callout from a LightningWeb Component to an external endpoint is failing?

- A. The endpoint URL has been added to Remote Site Settings.
- B. The endpoint domain has been added to Cross-Origin Resource Sharing.
- C. The endpoint URL has been added to Content Security Policies.

- D. The endpoint URL has added been to an outbound firewall rule.

Answer: A

Explanation:
Explanation
The first thing an integration architect should validate if a callout from a Lightning Web Component to an external endpoint is failing is the endpoint domain has been added to Cross-Origin Resource Sharing (CORS).
CORS is a mechanism that allows web browsers to make requests to servers on different origins, such as different domains, protocols, or ports. CORS requires the server to send back a special header that indicates whether the browser is allowed to access the resource or not. If the endpoint domain is not added to the CORS whitelist in Salesforce, the browser will block the callout and throw an error. Option B is not correct because Content Security Policies (CSP) are used to control what resources can be loaded on a Visualforce or Lightning page, such as scripts, stylesheets, images, etc. CSP does not affect the callout from a Lightning Web Component to an external endpoint. Option C is not correct because outbound firewall rules are used to restrict the network traffic from Salesforce to external systems. Firewall rules are configured at the network level, not at the Salesforce level. Option D is not correct because Remote Site Settings are used to specify the domains that are allowed for callouts from Apex code, not from Lightning Web Components. References:
Working with CORS and CSP to Call APIs from LWC
[Cross-Origin Resource Sharing (CORS)]

NEW QUESTION # 77
Northern Trail Outfitters requires an integration to be set up between one of its Salesforce orgs and an External Data Source using Salesforce Connect. The External Data Source supports Open Data Protocol.
Which configuration should an integration architect recommend be implemented in order to secure requests coming from Salesforce?

- A. Configure CSRF Protection for OData connection.
- B. Configure Special Compatibility for OData connection.
- C. Configure Identity Type for OData connection.

Answer: C

Explanation:
In the context of Salesforce Connect, securing the integration depends heavily on how the platform authenticates with the external system. The Identity Type configuration is the fundamental security setting for an External Data Source.
The architect must choose between two Identity Types:
* Named Principal: Salesforce uses the same set of credentials for all users to access the external system. This is simple to manage but does not allow the external system to distinguish between individual Salesforce users for auditing or permission purposes.
* Per User: Each Salesforce user must have their own credentials for the external system. This is the most secure option as it ensures that the data visible in Salesforce respects the specific permissions the user has in the source system.
By correctly configuring the Identity Type, the architect ensures that the requests coming from Salesforce are properly authorized at the target system. Option B (CSRF Protection) is a security measure to prevent cross- site request forgery but is not the primary mechanism for authenticating the Salesforce service itself. Option A is a technical compatibility setting for non-standard OData implementations and does not directly relate to security. Therefore, recommending the appropriate Identity Type-typically "Per User" for sensitive data-is the key step in securing the OData connection.

NEW QUESTION # 78
Northern Trail Outfitters (NTO) is looking to integrate three external systems that run nightly data enrichment processes in Salesforce. NTO has both of the following security and strict auditing requirements:
1. The external systems must follow the principle of least privilege, and
2. The activities of the eternal systems must be available for audit.
What should an Integration Architect recommend as a solution for these integrations?

- A. A shared integration user for the three external system integrations.
- B. A shared Connected App for the three external system integrations.
- C. A unique integration user for each external system integration.
- D. A Connected App for each external system integration.

Answer: D

Explanation:
Explanation
Using a Connected App for each external system integration is a good solution because it can provide security, auditing, and monitoring features for each integration. A Connected App is an application that can connect to Salesforce using APIs and OAuth as an authentication protocol. A Connected App can also enforce policies such as IP restrictions, login hours, and session timeout for each integration. Using a shared integration user for the three external system integrations is not a good solution because it violates the principle of least privilege, as well as makes it difficult to audit the activities of each system. Using a shared Connected App for the three external system integrations is also not a good solution because it does not allow for granular control and visibility of each integration. Using a unique integration user for each external system integration is not enough to meet the security and auditing requirements, as it does not provide any mechanism for authentication, authorization, or encryption. Reference: Salesforce Integration Architecture Designer Resource Guide, page 20-21

NEW QUESTION # 79
Universal Containers (UC) uses Salesforce to track the following customer data:
1. Leads,
2. Contacts
3. Accounts
4. Cases
Salesforce is considered to be the system of record for the customer. In addition to Salesforce, customer data exists in anEnterprise Resource Planning (ERP) system, ticketing system, and enterprise data lake. Each of these additional systems have their own unique identifier. UC plans on using middleware to integrate Salesforce with the external systems.
UC has a requirementto update the proper external system with record changes in Salesforce and vice versa.
Which two solutions should an Integration Architect recommend to handle this requirement?
Choose 2answers

- A. Design an MDM solution that maps external ID's to the Salesforce record ID.
- B. Locally cache external ID'S at the middleware layer and design business logic to map updates between systems.
- C. Use Change Data Capture to update downstream systems accordingly when a recordchanges.
- D. Store unique identifiers in an External ID field in Salesforce and use this to update the proper records across systems.

Answer: A,C

Explanation:
Using Change Data Capture (CDC) to update downstream systems accordingly when a record changes is a solution that can handle this requirement by capturingdata changes in Salesforce and sending them to external systems via a publish-subscribe model. This way, the external systems can receive near real-time updates from Salesforce and synchronize their data accordingly. Designing an MDM solution that maps external ID's to the Salesforce record ID is a solution that can handle this requirement by creating a master data hub that stores and manages the unique identifiers of each system and their relationships. This way, the MDM solution can ensuredata quality,consistency, and accuracy across systems. Locally caching external ID's at the middleware layer and designing business logic to map updates between systems is not a good solution because it can introduce performance and scalability issues, as well as increase the complexity and maintenance cost of the middleware layer. Storing unique identifiers in an External ID field in Salesforce and using this to update the proper records across systems is not enough to handle this requirement, as it does not address how to update Salesforce with record changes from external systems. Reference: Salesforce Integration Architecture Designer Resource Guide, page 27-28

NEW QUESTION # 80
An Architect is asked to build a solution that allows a service to access Salesforce through the API. What is the first thing the Architect should do?

- A. Authenticate the integration using existing Single Sign-On.
- B. Authenticate the integration using existing Network-BasedSecurity.
- C. Create a new user with SystemAdministrator profile.
- D. Create a special user solely for the integration purposes.

Answer: D

Explanation:
Create a special user solely for the integration purposes. This is the first thing that the Architect should do when building a solution that allows a service to access Salesforcethrough the API. Creating a special user for the integration purposes can help to ensure

security, accountability, and traceability of the API calls. The special user should have a unique username, password, security token, and profile that grants only thenecessary permissions and access for the integration. The special user should also be assigned to an API- only user license type that prevents logging in to the Salesforce UI. References: Certification - Integration Architect - Trailhead, [User Licenses], [API User Permission]

NEW QUESTION # 81

.....