A Fully Updated 2023 Sharing-and-Visibility-Architect Exam Dumps - PDF Questions and Testing Engine [Q33-Q49

A Fully Updated 2023 Sharing-and-Visibility-Architect Exam Dumps - PDF Questions and Testing Engine Easy Success Salesforce Sharing-and-Visibility-Architect Exam in First Try

Salesforce Certified Sharing and Visibility Architect is a prestigious certification that validates an individual's expertise in designing and implementing sharing and visibility solutions in Salesforce. It is a highly specialized certification that requires a deep understanding of Salesforce security and sharing models, as well as the ability to design and implement complex sharing rules, permission sets, and role hierarchies. Salesforce Certified Sharing and Visibility Architect certification exam is intended for experienced Salesforce architects, developers, and administrators who have a thorough understanding of Salesforce security and sharing features.

Salesforce Sharing-and-Visibility-Architect is one of the most advanced and specialized certification programs offered by the Salesforce platform. It is designed to validate the knowledge and expertise of Salesforce professionals in designing and implementing complex sharing and visibility solutions. Salesforce Certified Sharing and Visibility Architect certification program is intended for experienced Salesforce architects who understand the ins and outs of the platform's sharing model and can use it to solve real-world business problems.

Q33. Which two are potential vulnerabilities in the following code snippet? <apex:page> <apex:form> <apex:outputText value=&#8221;Enter Name&#8221;/> <apex:inputText value=&#8221;{!name}&#8221; /> <apex:commandButton value=&#8221;Query&#8221; action=&#8221;{!query}&#8221; /> </apex:form> </apex:page> public class SOQLController { public String name { get { return name;} set {name=value;} } public PageReference query() { String qryString=&#8217;SELECT Id FROM Contact WHERE &#8216;+ &#8216;(IsDeleted = false and Name like &#8216;%&#8217; + name + &#8216;%&#8217;}&#8217;; queryResult = Database.query(qryString); retunr null; } } Choose 2 answers
* FLS check
* SOQL Injection
* Data Access Control
* Arbitrary Redirects

Q34. When writing test methods, what functionality is verified by the system method&#8221;runAs()&#8221;?
* Enforcement of a user&#8217;s record sharing.
* Enforcement of user permissions.
* Enforcement of a user&#8217;s field-level security.
* Enforcement of user&#8217;s public group assignments.
Explanation

Enforcement of a user&#8217;s record sharing is the functionality that is verified by the system method &#8220;runAs()&#8221;.

This method allows test methods to run in the context of a specific user and verify whether that user has access to the records based on the sharing settings. The other options are not verified by the runAs() method.

Q35. Universal Containers has set Partners users who will see records owned by partner users in roles below them in the hierarchy of which roles?
* Executive, Manager, and User

Q36. Universal Containers (UC) has a mostly private organization-wide default (OWD), as it is a core principle of UC to respect client data privacy. UC has implemented complex processes for granting access to Opportunity dat a. A few key members of the Sales Reporting team need to always be able to see, but not change, Opportunity data for all Opportunities.

What should an architect recommend as an approach to meet these requirements?
* Create a Permission Set that grants &#8220;View All Data&#8221; Permission.
* Make Opportunity OWD read-only.
* Give &#8220;View All Data&#8221; Permission to the Sales Reporting Profile.
* Create a Permission Set that grants &#8220;View All&#8221; permission for Opportunity.

Q37. Universal Containers (UC) wants to reduce the amount of redundant leads entered into the system. UC also only edited/reassigned by the lead owner.

What organization-wide default (OWD) approach should be recommended to help UC implement these requirements?
* Implement a Public Read Only OWD on Lead.
* Implement a Public Read Only/Transfer OWD on Lead
* Implement a private OWD on Lead.
* Implement a Public Read/Write OWD on Lead.
Explanation

To reduce redundant leads and restrict their editing and reassignment, a Salesforce Architect should recommend implementing a private OWD on Lead. A private OWD means that only the owner of the lead record and users above them in the role hierarchy can view, edit, or transfer the lead. This will prevent duplicate leads from being created by other users, and also ensure that only the lead owner can modify or reassign the lead. Implementing a public read only OWD on Lead will not work, as it will allow other users to view the lead records, which may lead to duplication. Implementing a public read only/transfer OWD on Lead will not work, as it will allow other users to transfer the lead records to themselves or others. Implementing a public read/write OWD on Lead will not work, as it will allow other users to edit or reassign the lead records.

Q38. By Viewer Access you can see the data in a report or dashboard, but you can&#8217;t make any changes, except by cloning it into a new report or dashboard.
* True
* False
Explanation

The statement is true. By Viewer Access, you can see the data in a report or dashboard, but you can&#8217;t make any changes, except by cloning it into a new report or dashboard1. Viewer Access is one of the three types of folder access levels in Salesforce, along with Editor Access and Manage Access1.

Q39. Universal Containers has the following Sharing Settings for their Org:

Account = Private

Contact = Controlled by Parent

Opportunity = Private

Case = Private

They have enabled &#8220;Default Account Teams&#8221; and have trained users to set up their Default Team. Which three access levels can be set on the Account Team Member?

Choose 3 answers
* Opportunity Access
* Case Access
* Contact Access
* Contract Access
* Account Access
Explanation

The access levels that can be set on the Account Team Member are Account Access, Opportunity Access, and Case Access2. Contact Access and Contract Access are not available options for Account Team Members.

Q40. Universal Containers (UC) operates worldwide, with offices in more than 100 regions in 10 different countries, and has established a very complex Role Hierarchy to control data visibility. In the new fiscal year, UC is planning to reorganize the roles and reassign account owners.

Which feature should an architect recommend to avoid problems with this operation?
* Skinny table
* Partition data using Divisions
* So Deferred Sharing Recalculation

Q41. Universal Containers (UC)has implemented customer community with customer community licenses for their customers. UC requested that any record owned by its customers should be accessible by UC users in the customer support role.

How can an Architect configure the system to support the requirements?
* Sharing Set
* Share Group
* Apex Sharing
* Sharing Rule
Explanation

The architect can configure the system to support the requirements by using a sharing rule. A sharing rule is a declarative way of extending record access to users or groups of users based on criteria such as ownership, role, or field values3. In this case, the architect can create a sharing rule that grants read or read/write access to all records owned by customer community users to UC users in the customer support role. A sharing set is used to grant access to community users based on a common account or contact, not to internal users. A share group is used to share records with groups of community users who have Customer Community Plus or Partner Community licenses, not with internal users. Apex sharing is used to programmatically share records when declarative sharing cannot fulfill complex requirements, but it is not necessary in this case.

Q42. Universal Containers has developed an AppExchange managed package for their distribution partners, which required a private key to be generated for each partner and used by the code. Universal Containers support representatives must be able to access the private key value to debug connection issues, but it must not be possible for the partner to access the value.

How can the Architect best support this requirement?
* Store the value in a text field on a protected custom setting in the package.
* Store the value in a static variable in a class included in the managed package.
* Store the value in the text field on a list custom setting in the managed package.
* Store the value in an encrypted field on a custom object in the package.
The correct answer is D. Store the value in an encrypted field on a custom object in the package.

By storing the private key value in an encrypted field on a custom object in the package, the architect can ensure that the value is protected and cannot be accessed by the partner. This meets the requirement of allowing Universal Containers support representatives to access the value for debugging purposes while preventing the partner from accessing it.

Options A and C involve using custom settings to store the value, but these settings do not provide the necessary encryption to protect the private key value.

Option B suggests storing the value in a static variable in a class included in the managed package. However, static variables can be accessed by other classes within the package, including classes belonging to the partner. Therefore, this option does not adequately address the requirement of preventing the partner from accessing the private key value.

Therefore, the best option is D. Store the value in an encrypted field on a custom object in the package.

Q43. Universal Containers (UC) has recently changed its internal policy to follow market regulations and create an internal team to manage the collection process. Only this team should have access to Invoke records. currently, invoke is a child in a Master-Detail relationship to Account. Although related lists have been removed from the page layouts, some profiles stills have access to the invoice object.

Which approach should an architect recommend to fix this problem?
* Create a new Profile with no access to the Invoice object and assign it to all unauthorized users.
* Create a Permission Set with No Access to the Invoice object and assign it to unauthorized users.

* Replace Account and Invoke Master Detail Relationship by a Lookup and remove Invoice Access from the unauthorized profiles,
* Change the Invoke organization-wide default from Controlled by Parent to Private and remove invoke access from the unauthorized

Q44. A sales coach at Universal Containers wants to create and share @ report folder with other sales coaches, Which two permissions are required to accomplish this?
* Manage Reports in Public Folders and edit My Reports.
* Create and customize Reports and Report Folders.
* Create Report Folders and manage Reports in Public Folders.

Q45. Universal Containers has a custom object to maintain Job information with a private sharing model. The Delivery group is distributed through the Role Hierarchy based on geography. As the Delivery group often collaborates on Jobs, all users in the Delivery profile required View access to all Job records. In special case, the Delivery user who owns a job must be able to grant a Product Development user access to a Job record. Which two platform features can be used to support these requirements?

Choose 2 answers
* Criteria-based Sharing Rules
* &#8220;View All&#8221; Profile settings
* Owner-based Sharing Rules
* Manual Sharing

Q46. To grant Universal Containers sales manager access to shipment records properly, it was necessary to leverage Apex managed sharing. The IT team is worried about improper access to records.

Which two features and best practices should a Salesforce architect recommend to mitigate this risk?
* Use runAs system method in test classes to test using different users and profiles.
* Use with Sharing keyword in Apex classes to assure record visibility will be followed.
* Use is Shareable in Apex classes to assure record visibility will be followed.
* Use is Accessible keyword in Apex classes to assure record visibility will be followed
Explanation

To mitigate the risk of improper access to records when using Apex managed sharing, the Salesforce architect should recommend using runAs system method in test classes and with Sharing keyword in Apex classes. The runAs system method allows testing the code as different users with different profiles and permissions, which can help verify that the sharing logic is working as expected2. The with Sharing keyword enforces the record visibility rules for the current user context, which can help prevent unauthorized access to records that are not shared with the user

Q47. Universal Containers, a global corporation of 50,000 users, has a 24&#215;7 call center operated by 20,000 users that includes employees and contractors. Their sales organization is 10,000 strong and they started processing about 100,000 updates to opportunity custom fields called Priority and NextStep. They also started processing 20,000 updates to a highly nested territory hierarchy. There was a third mass update on a Next Step field on the Action Plan custom object that has Case as a lookup field. Users started seeing a Group membership lock error in the system. What is a probable cause for this error?
* Lock contention due to system-initiated sharing rule recalculation
* Lock contention on Case records because of Action Plan custom object updates.
* Lock contention on Territory object because of Territory object updates.
* Lock contention on Account records because of Opportunity object updates.

Q48. UniversalContainers(UC)hasimplementedcustomercommunitywithcustomercommunitylicenses for their customers. UCrequested thatanyrecord owned by its customers should be accessible byUC users in the customer support role.

How can an Architect configure the system to support the requirements?
* Sharing Set
* Share Group
* Apex Sharing
* Sharing Rule

Q49. A user posts a file to the Chatter feed for a record of an object that has a Private organization-wide default.

Which statement accurately describes who can view the file by default?
* The user who posted the file and users with a shared chatter post link to the file
* The user who posted the file and users with access to the record
* Only the user who posted the file

Sharing-and-Visibility-Architect Study Material, Preparation Guide and PDF Download:
https://www.validexam.com/Sharing-and-Visibility-Architect-latest-dumps.html]