Exam : **Sharing-and-Visibility-Architect**

Title : Salesforce Certified Sharing and Visibility Architect

Vendor : Salesforce

Version : DEMO

NO.1 Users at Universal Containers are complaining that a field has disappeared from the Account page after last weekend's deployment. The page layout did not change with this deployment.
How should the admin troubleshoot this issue?

A. Run a Who Sees What report, filtering on Account.

B. Leg in as 3 user and check several accounts to isolate the problem records.

C. View Field Accessibility in the Object Manager.

Answer: C

Explanation:
If a field disappears from the Account page, the likely cause is that its visibility has been restricted through Field-Level Security (FLS) or a related profile/permission set update. Using Field Accessibility in Object Manager allows the admin to review and troubleshoot field permissions across profiles.
* Option A: A "Who Sees What" report is used for record visibility, not field visibility.
* Option B: Logging in as a user might help confirm the issue but doesn't provide insights into why the field is missing.
* Option C (Correct): Field Accessibility offers a comprehensive view of field-level security for troubleshooting.
:
Field Accessibility

NO.2 Universal Containers (UC) wants to reduce the amount of redundant leads entered into the system. UC also wants to ensure that leads are only edited/reassigned by the lead owner.
Which organization-wide default (OWD) approach should be recommended to help UC implement these requirements?

A. Implement a Public Read Only/Transfer OWD on Lead.

B. Implement 2 Public Read-Only OWD on Lead.

C. Implement a Private OWD on Lead.

Answer: C

Explanation:
To ensure that only lead owners can edit or reassign their leads, the OWD for Lead should be set to Private. In a Private model:
* Only the owner (and users above the owner in the Role Hierarchy) can access and edit the record by default.
* Redundant lead entries can be minimized by enforcing validation rules or duplicate management logic.
* Option A: A Public Read Only/Transfer OWD does not restrict edit access to the lead owner, as anyone with appropriate permissions could edit or transfer the leads.
* Option B: Public Read-Only OWD does not align with the requirement to ensure only lead owners can edit or reassign leads.
* Option C (Correct): Private OWD ensures that only the lead owner has edit access, adhering to UC's requirements.
:
Organization-Wide Default Settings

NO.3 Universal Containers (UC) has 200 distributors that use Partner Community licenses. Partners cannot see each other's data, but UC is also trying to give more visibility to data for certain individuals

at a distributor.
Which scalable option give users in the partner manager role access to all case and container records for partner users at the same distributor?

A. Create an ownership based sharing rule.

B. Give Super User permission to the individual partner manager users.

C. Create sharing sets.

Answer: B
Explanation:
* Super User Permission: In Salesforce, the "Super User" permission allows partner community users in specific roles (such as Partner Managers) to access records owned by or shared with users within their partner account. This is an effective and scalable solution for giving partner manager users access to all case and container records for users at the same distributor.
* Why Option B is Correct: Granting Super User permissions is straightforward, scalable, and avoids complex configurations such as ownership-based sharing rules or sharing sets.
* Why Others Are Incorrect:
* Option A: Ownership-based sharing rules are not ideal because they do not accommodate scalability and flexibility across multiple distributors.
* Option C: Sharing sets provide access based on the account relationship, but they are limited in scope compared to the flexibility provided by Super User permissions.
For detailed information on Super User permissions, refer to the Salesforce documentation on Partner Communities: https://help.salesforce.com/

NO.4 Universal Containers implemented Sales Cloud and requested that only certain branch staff trained to sell high-risk products can create opportunities for high-risk products.
How should an architect allow only specific branch staff to sell high-risk products?

A. Set the price book OWD to View Only and share the (High Risk) price book with the trained staff via manual sharing.

B. Set the price book OWD to View Only and share the (High Risk) price book with the trained staff via a sharing rule.

C. Set the price book organization-wide default (OWD) to View Only and share the price book (High Risk) with the trained staff.

Answer: B
Explanation:
To ensure only specific branch staff can create opportunities for high-risk products, set the Price Book OWD to View Only to limit access. Then, use a sharing rule to share the high-risk price book with the trained staff.
This approach ensures:
* Untrained users cannot see or use the price book.
* Trained staff have explicit access through the sharing rule.
* Option A: Manual sharing is inefficient for a large group and less manageable than sharing rules.
* Option C: While technically correct, sharing rule implementation is clearer and more scalable for this use case.
:
Price Book Sharing Model

NO.5 A sales rep at Universal Containers was added to an opportunity team with Read/Write permissions.
Which action is she allowed to perform in the opportunity?
A. Update opportunity stage.
B. Replace opportunity owner.
C. Add/remove members in the opportunity team.
Answer: A
Explanation:
The Opportunity Team feature allows collaboration by granting specific permissions (Read, Read/Write, or access defined by roles) to users added to an opportunity. In this scenario, the sales rep has Read/Write permissions, which means they can:
* View and update the opportunity, including editing fields like the opportunity stage.
* They cannot perform administrative tasks like transferring ownership or managing the opportunity team unless explicitly granted "Full Access" or assigned additional roles that permit these actions.
* Option A (Correct): Updating the opportunity stage is allowed as part of Read/Write access.
* Option B: Replacing the opportunity owner requires administrative privileges, which are not included in standard Read/Write permissions.
* Option C: Adding or removing members in the opportunity team requires "Full Access," which exceeds Read/Write permissions.
:
Opportunity Team Management
Salesforce Sharing and Permissions Documentation

NO.6 Universal Containers (UC) service reps are assigned to a profile which has View All on the Case object. The organization-wide default (OWD) for the Account and Case objects is Private.
To make sure service reps have access to all relevant information (Accounts and Contacts) to attend to customer requests, which detail should an architect consider?
A. Service reps will NOT be able to access the relevant Accounts if their OWD is Private.
B. Service reps will NOT be able to access the relevant Contacts if their OWD is Controlled by Parent.
C. Service reps will be able to access the relevant Contacts if their OWD is Controlled by Parent.
Answer: C
Explanation:
* OWD Settings and Access Control:
* When the OWD for Contacts is "Controlled by Parent," access to the Contact is determined by access to the related Account.
* Why Option C is Correct:
* Service reps have "View All" permission on Cases, granting them access to related Accounts. Since Contacts are controlled by the parent Account, service reps also gain access to relevant Contacts.
* Why Others Are Incorrect:
* Option A: Service reps can access Accounts related to Cases they can view, even if the OWD is Private.
* Option B: Contacts controlled by the parent are accessible as long as the parent Account is accessible.
For detailed guidance, see Salesforce documentation on OWD and Controlled by Parent: https://help.

salesforce.com/

NO.7 Universal Containers (UC) delivers training in 500 different regions. The UC operations users team manages course setup, scheduling, and trainer setup. The team members work at a regional level and report to an operations manager. The operations manager requested access to edit ALL scheduled courses owned by the operation users team.
How should this be achieved?

A. The operations manager will get access to the scheduled courses by creating an ownership-based sharing rule and share the scheduled courses with the operations manager.

B. The operations manager will get access to the scheduled courses owned by the operations users team defined in the Role Hierarchy.

C. The operations manager will get access to the scheduled courses by creating a public group, and add the operations manager and the operations users team to the public group.

Answer: B
Explanation:
In Salesforce, the Role Hierarchy grants record access to users higher in the hierarchy. If the operations users are below the operations manager in the Role Hierarchy and the object's organization-wide default (OWD) is not "Private," the manager will inherit access to records owned by their subordinates. This approach is automatic and does not require additional sharing rules or groups.
* Option A: Ownership-based sharing rules are unnecessary if the Role Hierarchy provides the required access.
* Option C: Using a Public Group is an unnecessary workaround for this scenario when Role Hierarchy fulfills the requirement.
:
Role Hierarchy Overview

NO.8 Sales reps at Universal Containers (UC) complain about the manual activities they need to perform in order to grant access to supporting internal users (legal, engineering, finance, etc.) for customer records when they need help. In general, the sales reps involved in the deals will not change.
How should an architect help UC improve sales reps' productivity?

A. Create a criteria based sharing rule to grant access to other users.

B. Leverage default Account team.

C. Create a permission set with View All Data and assign to supporting users.

Answer: B
Explanation:
Default Account Teams allow users to predefine a set of supporting internal users (e.g., legal, engineering, finance) who need access to customer records. The team members are automatically granted the specified access whenever an Account is created or updated, reducing the manual effort required by sales reps.
* Option A: A criteria-based sharing rule might grant access to a larger group but does not provide the flexibility and precision of Account Teams.
* Option C: Assigning View All Data via a permission set gives overly broad access and violates the principle of least privilege.

:
Account Teams Overview