Salesforce Administrator ADM-201 Exam Questions

Total Questions: 200+
Demo Questions: 30
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit: ADM-201 Exam Dumps by Cert Empire

Question: 1

The administrator at Ursa Major Solar has created a custom report type and built a report for the sales operations team. However, none of the users are able to access the report. Which two options could cause this issue? (Choose 2 answers)

A: The user's profile is missing View access.

B: The report is saved in a private folder.

C: The custom report type is in development.

D: The org has reached its limit for custom report types.

Correct Answer:

B, C

Explanation:

User access to a report depends on multiple factors, including the report's storage location and the status of its underlying components.

1. Report Folder (B): A report saved in a user's private folder (e.g., "My Personal Custom Reports") is, by default, not accessible to any other user. For the sales operations team to access the report, the administrator must save it in a shared, public, or other accessible folder and grant the team the necessary permissions.

2. Custom Report Type Status (C): When a custom report type is created, its default deployment status is "In Development." While in this state, only users with the "Manage Custom Report Types" permission (typically administrators) can create or run reports based on it. The administrator must change the status to "Deployed" for it to be available to other users.

Why Incorrect Options are Wrong:

A: The user's profile is missing View access. This is imprecise. If it refers to the "Run Reports" permission, its absence would prevent access to all reports, not just this specific one. Options B and C are more directly tied to the admin's recent actions.

D: The org has reached its limit for custom report types. This limit would have prevented the administrator from creating the custom report type initially. It does not affect user access to a report that has already been successfully built.

References:

1. Report Folders: Salesforce Help, "Share a Report or Dashboard Folder in Lightning Experience." This document explains that to share reports, they must be in a user-created folder with appropriate sharing settings, not a private folder.

2. Custom Report Type Status: Salesforce Help, "Manage Custom Report Types." This guide states, "To let users create and run reports from your custom report type, set its status to 'Deployed.'... Report types with a status of 'In Development' are not visible to users (except for users with the 'Manage Custom Report Types' permission)."

3. General Report Access: Salesforce Trailhead, "Reports & Dashboards for Lightning Experience," Unit: "Share Reports and Dashboards." This module emphasizes that report access is controlled primarily by folder permissions. It states, "To give your colleagues access to the report... you have to save it to a shared folder."

Question: 2

An administrator has been asked to change the data type of an auto number to a text field. What should the administrator be aware of before changing the field?

A: Existing field values will be deleted.

B: Existing field values will remain unchanged.

C: Existing field values will be converted.

D: Existing Auto Number field to Text is prevented.

Correct Answer:

B

Explanation:

When changing the data type of a custom field from Auto-Number to Text, Salesforce preserves the existing values. The field will no longer automatically generate a number for new records, but the data in existing records will remain as it was, now stored as a text string. This is a non-destructive change to the existing data.

Why Incorrect Options are Wrong:

A: Existing field values will be deleted. This is incorrect. Salesforce does not delete the data during this specific conversion; the values are preserved.

C: Existing field values will be converted. This is imprecise. The values are already stored as strings (e.g., "A-0001"); they are simply retained as static text. "Unchanged" is the more accurate description.

D: Existing Auto Number field to Text is prevented. This is incorrect. The Salesforce platform allows an administrator to change an auto-number field to a text field.

References:

1. Salesforce Help, Article ID: 000333733, "Considerations for Changing Custom Field Types": This official documentation explicitly states the outcome of various field type changes. For the change from Auto-Number to Text, it confirms that existing data is preserved. The table within this document details that "Data is preserved" for this specific conversion.

2. Salesforce Platform App Builder Certification Guide (Official Study Guide): The section on "Data Modeling and Management" covers field types and the implications of changing them,

reinforcing that changing from an auto-number to a text field retains the existing record values.

Question: 3

Cloud Kicks is working on a better way to track its product shipments utilizing Salesforce. Which field type should an administrator use to capture coordinates?

A: Geolocation

B: External lookup

C: Custom address

D: Geofence

Correct Answer:

A

Explanation:

The Geolocation custom field type is specifically designed to store location data by capturing latitude and longitude coordinates. This allows for the precise tracking of locations, such as product shipments, and enables distance calculations within Salesforce. It is a compound field that includes separate values for latitude and longitude, making it the most accurate and direct solution for the stated requirement.

Why Incorrect Options are Wrong:

B: External lookup: This field type is used to create a relationship between a Salesforce object and an external object, not for storing coordinate data directly on a record.

C: Custom address: The Address field type is a compound field for storing structured mailing address components (street, city, state, etc.), not for capturing raw coordinate data.

D: Geofence: Geofencing is a feature or concept used to define a virtual geographic boundary, often to trigger events. It is not a standard Salesforce field type for data storage.

References:

1. Salesforce Help, "Geolocation Custom Field": "You can add a geolocation custom field to an object to store location data. Geolocation is a compound field that’s made up of and stores the following: Latitude and Longitude."

2. Salesforce Object Reference Guide, "Field Types": This guide details the various field types available in Salesforce. The "Geolocation" type is defined for storing latitude and longitude. In contrast, "External Lookup Relationship" is defined for linking to external

objects, and "Address" is a compound type for physical addresses. (Refer to the sections on Geolocation and other field types).

3. Salesforce Developer Documentation, "Compound Fields": "Address and Geolocation fields are compound fields. A compound field is a special field that groups together multiple elements of a specific data type." This source distinguishes between Address and Geolocation as separate compound field types with different purposes.

Question: 4

Universal Containers requires that when an opportunity is closed won, all other open opportunities on the same account must be marked as closed lost. Which automation solution should an administrator use to implement this request?

A: Workflow Rule

B: Flow Builder

C: Outbound Message

D: Quick Action

Correct Answer:

B

Explanation:

This business requirement involves a record-triggered action that must find and update multiple related records (i.e., sibling records). When an opportunity is updated to 'Closed Won', the system needs to query for all other open opportunities under the same account and update their status. Flow Builder is the designated Salesforce automation tool for such complex logic. A record-triggered flow can be initiated on the opportunity update, use a Get Records element to find the related open opportunities, and an Update Records element to change their stage to 'Closed Lost'.

Why Incorrect Options are Wrong:

A: Workflow Rule: Workflow Rules are deprecated and cannot perform this action. They are limited to updating the triggering record or its direct parent, and cannot query for and update sibling records.

C: Outbound Message: An Outbound Message is an action used to send data to an external system. It does not update records within the Salesforce environment.

D: Quick Action: A Quick Action requires manual user interaction to be initiated. The requirement specifies an automatic process that occurs upon saving a record, not a manual one.

References:

1. Salesforce Help, "Which Automation Tool Should I Use?": This official guide compares automation tools. It states, "Flow Builder can launch a complex business process that works

with multiple records... For all behind-the-scenes automation, we recommend that you use Flow Builder." This confirms Flow is the correct choice for multi-record updates.

2. Salesforce Help, "Flow Element: Get Records": "Find Salesforce records that meet filter conditions... After you’ve found the records, you can store their values in variables to use later in the flow, such as to update one of the found records..." This describes the exact functionality needed to find the other open opportunities.

3. Salesforce Help, "Flow Element: Update Records": "Find Salesforce records that meet filter conditions and update the values in those records." This describes the action required to change the status of the found opportunities to 'Closed Lost'.

Question: 5

Cloud Kicks has the organization-wide defaults for Opportunity set to Private. Which two features should the administrator use to open up access to opportunity records for sales users working on collaborative deals? (Choose 2 answers)

A: Role hierarchy

B: Sharing set

C: Profiles

D: Sharing rules

Correct Answer:

A, D

Explanation:

When an object's Organization-Wide Default (OWD) is set to Private, access to records is initially restricted to the record owner. To grant broader access, Salesforce uses a layered sharing model. The role hierarchy is a fundamental layer that provides vertical access, allowing users in higher roles to automatically view and edit records owned by users in roles directly below them. For collaborative scenarios that require horizontal or criteria-based access (e.g., sharing between peers or across teams), sharing rules are used. They create automatic exceptions to the OWD, granting specified users access to records based on criteria like record ownership or field values.

Why Incorrect Options are Wrong:

B: Sharing set: This feature is used to grant Experience Cloud (community/portal) users access to records, not for internal sales users as specified in the scenario.

C: Profiles: Profiles control object-level and field-level security (e.g., if a user can see the Opportunity object at all), but they do not grant access to specific records.

References:

1. Salesforce Help, Control Access to Records: "The role hierarchy enables users above another user in the hierarchy to have the same level of access to records owned by or shared with the users below them." This confirms the role of the hierarchy in granting vertical access.

2. Salesforce Help, Sharing Rules: "Sharing rules are automatic exceptions to your organization-wide defaults... Use sharing rules to extend sharing access to users in public groups, roles, or territories." This confirms their use for extending access beyond the OWD.

3. Salesforce Security Guide, Page 13: "Regardless of the org-wide default settings, a manager can always view and edit the same records as his or her employees. To restrict a manager’s access to records from their employees, you must remove the manager’s object permissions." This reinforces the function of the role hierarchy.

4. Salesforce Security Guide, Page 23: "Use a sharing set to grant site users access to any record associated with an account or contact that matches the user’s account or contact." This explicitly defines sharing sets for external site users.

5. Salesforce Help, Control Access to Objects: "After you set object permissions for a particular type of user in their profile... you can then lock down access to records using the sharing settings." This distinguishes the function of profiles (object-level) from sharing settings (record-level).

Question: 6

Users at Cloud Kicks are reporting different options when updating a custom picklist on the Opportunity object based on the kind of opportunity. Where should an administrator update the option in the picklist?

A: Record type

B: Picklist value sets

C: Fields and relationships

D: Related lookup filters

Correct Answer:

A

Explanation:

Record types in Salesforce are used to offer different business processes, page layouts, and picklist values to different users. When users see varying picklist options based on the "kind of opportunity," it indicates that different record types are in use. The administrator must edit the picklist values available for the specific record type associated with that kind of opportunity to make the necessary updates. This allows for tailored user experiences and data entry processes for distinct categories of records within the same object.

Why Incorrect Options are Wrong:

B: Picklist value sets: These define a master set of values that can be shared across multiple fields, but they do not control which values are available for a specific record type.

C: Fields and relationships: This is where the picklist field and its master list of all possible values are created, but record types control the specific values presented to users.

D: Related lookup filters: These are used to restrict records in a lookup relationship field, which is not applicable to a standard picklist field as described in the scenario.

References:

1. Salesforce Help, "Record Types": "Record types determine the business processes, page layouts, and picklist values users have access to." This directly links record types to the control of available picklist values.

2. Salesforce Help, "Edit Picklists for Record Types and Business Processes": "After you create a record type, you can specify the values that are included in the picklists for that record type... For each record type, you can include a different set of values from a master picklist." This outlines the exact procedure for the administrator's task.

3. Salesforce Help, "Picklist Value Sets": "A picklist value set is a set of values that you can use for more than one picklist field." This clarifies their role as a reusable master list, distinct from the record-type-specific display.

Question: 7

Universal Containers created a new job posting on the first of the month. It triggered a process scheduled action that will send a Chatter post to the department VP in 30 days if the position is still open and the status is not equal to Interviewing. On the 10th of the month, an applicant interviews, and the job posting status is updated to Interviewing. What will happen to the Chatter post in this situation?

A: The pending Chatter post will be canceled.

B: The pending Chatter post will be sent in 30 days.

C: The pending Chatter post will be paused.

D: The pending Chatter post will be sent on the 10th of the month.

Correct Answer:

A

Explanation:

In Salesforce Process Builder, the criteria for a scheduled action are evaluated twice: once when the record initially triggers the process, and again immediately before the scheduled action is set to execute. In this scenario, the process scheduled the Chatter post on day 1. However, on day 10, the record was updated so that it no longer meets the action's criteria (status is not equal to Interviewing). When the 30-day mark arrives, Salesforce will re-evaluate the criteria, find that they are no longer met, and will not execute the action. This is functionally a cancellation of the pending action.

Why Incorrect Options are Wrong:

B: This is incorrect. The Chatter post will not be sent because the criteria for the scheduled action are no longer met at the time of execution.

C: This is incorrect. Scheduled actions in the automation queue do not have a "paused" state; they are either pending execution or are removed/canceled.

D: This is incorrect. The action was explicitly scheduled for 30 days after the initial trigger, not for the date of a subsequent record update.

References:

1. Salesforce Help, "Considerations for Processes": Under the "Actions" section, the documentation states, "Salesforce evaluates the criteria for a scheduled action just before

the action is executed." This confirms that the criteria are re-checked at the scheduled time, and if they are no longer met, the action will not run.

2. Salesforce Help, "Monitor Your Process-Scheduled Actions": This document explains how scheduled actions are placed in a queue. It notes, "An action is executed only if the associated criteria node still evaluates to true." This directly supports the conclusion that the action is canceled if the criteria become false before the execution time.

3. Salesforce Help, "Time-Based Actions and Transactions": While this document is for Workflow Rules, the underlying engine and principles are the same for Process Builder's scheduled actions. It states, "Salesforce re-evaluates the workflow rule criteria when the time-dependent action is due. If the record no longer meets the criteria, Salesforce doesn't execute the action."

Question: 8

Sales reps at Ursa Major Solar are having difficulty managing deals. The leadership team has asked the administrator to help sales reps prioritize and close more deals. What should the administrator configure to help with these issues?

A: Einstein Opportunity Scoring

B: Einstein Search Personalization

C: Einstein Lead Scoring

D: Einstein Activity Capture

Correct Answer:

A

Explanation:

The core requirement is to help sales representatives prioritize and manage deals. In the Salesforce ecosystem, "deals" are represented by the Opportunity object. Einstein Opportunity Scoring is specifically designed to address this need by using artificial intelligence to analyze past opportunities and assign a score (from 1 to 99) to each open opportunity. This score indicates the likelihood of the deal being won, enabling sales reps to focus their time and effort on the opportunities with the highest probability of closing, thereby improving prioritization and close rates.

Why Incorrect Options are Wrong:

B: Einstein Search Personalization: This feature tailors search results to a user's activity. It improves the efficiency of finding records but does not directly assist in prioritizing or managing the deal pipeline.

C: Einstein Lead Scoring: This feature scores Leads based on their likelihood to convert into an Opportunity. The scenario is about managing existing deals (Opportunities), not qualifying new leads.

D: Einstein Activity Capture: This tool automates the logging of emails and events to related records. While it provides a more complete view of customer interactions, it does not offer a direct prioritization mechanism like scoring.

References:

1. Salesforce Help, Einstein Opportunity Scoring: "Einstein Opportunity Scoring gives each opportunity a score from 1 to 99, which is available on opportunity records... The score tells you the likelihood that an opportunity will be won. By focusing on opportunities with higher scores, sales reps can work more efficiently and close more deals." (Salesforce Help, Article: "Einstein Opportunity Scoring")

2. Salesforce Help, Einstein Lead Scoring: "Einstein Lead Scoring helps your sales team prioritize leads so they can focus on the ones that are most likely to convert." (Salesforce Help, Article: "How Einstein Lead Scoring Works")

3. Salesforce Help, Einstein Activity Capture: "Einstein Activity Capture helps keep data between Salesforce and your email and calendar applications up to date." (Salesforce Help, Article: "Einstein Activity Capture")

4. Salesforce Help, Einstein Search Personalization: "Einstein Search Personalization gets you to the records you want faster. When you search for a term, Einstein Search looks at your recent activity and location to rank your search results." (Salesforce Help, Article: "Einstein Search Personalization")

Question: 9

The administrator at Northern Trail Outfitters has been using a spreadsheet to track assigned licenses and permission sets. What feature can be used to track this in Salesforce?

A: Login History

B: Permission Set Groups

C: Lightning Usage App

D: User Report

Correct Answer:

D

Explanation:

A User Report is the most direct and appropriate tool for tracking assigned licenses and permission sets. Administrators can create a standard report on the User object and add the 'User License' field as a column to view license assignments for all users. To track permission set assignments, a custom report type can be created that links the User object with the Permission Set Assignment object. This provides a comprehensive, reportable view that directly replaces a manual spreadsheet.

Why Incorrect Options are Wrong:

A: Login History: This feature is used for auditing user login attempts, IP addresses, and login methods, not for tracking license or permission set assignments.

B: Permission Set Groups: This feature is for bundling and assigning permission sets to users to simplify administration, not for reporting on or tracking existing assignments.

C: Lightning Usage App: This app provides metrics on user adoption and performance within Lightning Experience, not administrative details like license types or permission sets.

References:

1. User Reports: Salesforce Help, "Standard Report Types," describes the "Users" report type, which allows reporting on user records, including fields like Profile and User License.

2. Reporting on Permission Sets: Salesforce Help, "Create a Custom Report Type," explains the process for creating custom report types. To report on permission set

assignments, an administrator would create a report type with "Users" as the primary object and "Permission Set Assignments" as the related object.

3. Lightning Usage App: Salesforce Help, "Monitor Adoption with the Lightning Usage App," states, "The Lightning Usage App lets you monitor adoption metrics like daily and monthly active users... and the most visited pages." This confirms its purpose is adoption monitoring, not license tracking.

4. Permission Set Groups: Salesforce Help, "Permission Set Groups," details their function: "A permission set group bundles permission sets together... You can include a permission set in more than one permission set group." This highlights its role in assignment, not reporting.

Question: 10

Northern Trail Outfitters has two different sales processes: one for business opportunities with four stages and one for partner opportunities with eight stages. Both processes will vary in page layouts and picklist value options. What should an administrator configure to meet these requirements?

A: Validation rules that ensure that users are entering accurate sales stage information.

B: Public groups to limit record types and sales processes for opportunities.

C: Different page layouts that control the picklist values for the opportunity types.

D: Separate record types and sales processes for the different types of opportunities.

Correct Answer:

D

Explanation:

To support distinct business workflows with different stages, page layouts, and picklist values, the standard Salesforce solution is to use Record Types in conjunction with Sales Processes. A Sales Process defines the specific stages an opportunity moves through. A Record Type then links a specific Sales Process, a unique Page Layout, and a set of available picklist values to a particular type of record (e.g., 'Business' vs. 'Partner'). This combination allows an administrator to present a tailored user experience and enforce a specific process based on the type of opportunity being created, directly meeting all stated requirements.

Why Incorrect Options are Wrong:

A: Validation rules are used to enforce data quality and integrity standards after a user enters data, not to define the underlying business process, stages, or page layout.

B: Public groups are used for sharing records and managing access permissions, not for defining business processes or user interface elements like page layouts and picklist values.

C: While different page layouts are part of the solution, they alone cannot control the available sales stages in the sales path or filter the picklist values for the Stage field.

References:

1. Salesforce Help, "Create a Sales Process": "Sales processes let you create different sales cycles to be used for different types of opportunities... After you create a sales process, assign it to one or more opportunity record types." This confirms that Sales Processes control the stages and are linked via Record Types.

2. Salesforce Help, "Create Record Types": "Record types let you offer different business processes, picklist values, and page layouts to different users... For example, you can create a record type for your sales opportunities and another for your business development opportunities, with different picklist values for the Stage field." This directly supports using record types for different processes, layouts, and picklists.

3. Salesforce Help, "Guidelines for Creating and Updating Record Types": "Before you create a record type, include all the possible picklist values that your various user groups will need. Then, when you create the record type, you can associate a subset of the picklist values with it." This explains how record types control picklist values.

Question: 11

Where can a system administrator go if they are trying to determine why a user cannot log in to Salesforce? (Choose all that apply.)

A: The Login History related list on the user's record

B: The user's profile

C: Manage Users I Login History

D: Call salesforce.com Support

Correct Answer:

A, C

Explanation:

To determine why a user cannot log in, a system administrator has two primary tools within Salesforce Setup. The most direct method for a specific user is to navigate to that user's detail record and view the "Login History" related list, which shows their 20 most recent login attempts and the status. For a more comprehensive view or if the attempt is older, the administrator can use the org-wide "Login History" page (found under Setup), which stores up to 20,000 records for the last six months and can be filtered by user and other criteria to find the specific failed attempt and its reason.

Why Incorrect Options are Wrong:

B: The user's profile contains settings like IP restrictions or login hours that cause login failures, but it does not provide a log of why a specific attempt failed.

D: Contacting Salesforce Support is an escalation path for complex issues, not the standard first step for troubleshooting a common user login problem that can be diagnosed with internal tools.

References:

1. Salesforce Help Documentation, "Monitor Login History": This document details the org-wide Login History page. It states, "As an administrator, you can monitor all login attempts for your organization... The Login History page displays up to 20,000 records of user logins for the past 6 months." This directly supports option C.

2. Salesforce Help Documentation, "User Fields": In the description of standard user record components, the "Login History" related list is specified. It notes, "This related list on a

user’s detail page shows the user’s 20 most recent login attempts." This directly supports option A.

3. Salesforce Help Documentation, "What Are Profiles?": This resource explains that profiles control user access settings. "In a user profile, you can set login hours... You can also limit the IP addresses from which users can log in." This confirms a profile is for configuration, not for logging access attempts, making option B incorrect for diagnosing a failure.

Question: 12

If a user leaves your company, the system administrator should do the following to prevent future access to the Salesforce org.

A: Delete their user record

B: De-activate their user record

C: Delete any accounts or contacts owned by that user

D: None of the above

Correct Answer:

B

Explanation:

The correct and standard procedure when a user leaves a company is to deactivate their user record. Deactivation immediately revokes all access to the Salesforce organization, preventing the user from logging in. This action preserves the user's historical data and record ownership, which is crucial for auditing and maintaining data integrity. Deactivating the user also frees up the Salesforce license, allowing it to be assigned to a new user. This method ensures security is enforced without compromising historical information.

Why Incorrect Options are Wrong:

A: Delete their user record: Deleting a user is often impossible if they own records or are part of system processes. It also permanently erases their historical data, which is not a recommended practice.

C: Delete any accounts or contacts owned by that user: This action results in data loss and does not address the core requirement of revoking the user's access to the Salesforce org. Record ownership should be transferred, not deleted.

D: None of the above: This is incorrect because deactivating the user record is the officially recommended and correct procedure.

References:

1. Salesforce Help, "Deactivate Users": This document outlines the standard procedure. It states, "To prevent users from logging in to your Salesforce org without deleting them, you can deactivate their user accounts... Deactivating a user is not the same as deleting one. You can’t delete users, but you can deactivate them."

2. Salesforce Help, "Considerations for Deactivating Users": This guide details the implications of deactivation, confirming that it preserves the user's records. It notes, "When you deactivate a user, you preserve their historical activity and records."

3. Salesforce Help, "Delete Users": This article explains the very limited circumstances under which a user can be deleted and why it is generally not the correct action. It states, "You can’t delete a user that owns records... To delete the user, reassign all records they own and remove them from the items listed." This highlights why deactivation is the preferred method.

Question: 13

Which of the following is not a standard Profile?

A: System Administrator

B: Read only

C: Marketing Director

D: Partner Portal User

E: Standard Administrator

Correct Answer:

C, E

Explanation:

"Marketing Director" is not a standard profile. This title typically corresponds to a Role in the Salesforce role hierarchy, which is used to control data visibility and roll-up reporting, rather than a Profile, which controls object and field-level security.

"Standard Administrator" is also not a standard profile. The correct name for the standard profile with the highest level of permissions is "System Administrator". The name "Standard Administrator" does not exist as a default profile in Salesforce.

Therefore, both options are correct as they do not represent standard Salesforce profiles.

Why Incorrect Options are Wrong:

A: System Administrator: This is a standard profile included in all Salesforce orgs, granting the highest level of access to customize and manage the application.

B: Read Only: This is a standard profile that allows users to view data across the organization but prevents them from creating, editing, or deleting records.

D: Partner Portal User: This represents a standard external user profile, now commonly named "Partner Community User," designed for partners who access Salesforce data through an Experience Cloud site (formerly Portal).

References:

1. Salesforce Help. (n.d.). Standard Profiles. Retrieved from Salesforce Help & Training.

Reference Details: This document lists the standard profiles available in Salesforce orgs. It includes "System Administrator" and "Read Only" but does not list "Marketing Director" or "Standard Administrator."

2. Salesforce Help. (n.d.). User Roles. Retrieved from Salesforce Help & Training.

Reference Details: This article explains that roles, such as "CEO" or "Sales Director," are used to create a hierarchy that determines how users access data, confirming that a title like "Marketing Director" is a role, not a profile.

3. Salesforce Help. (n.d.). Standard Experience Cloud Site User Profiles. Retrieved from Salesforce Help & Training.

Reference Details: This document lists standard profiles for external users, including "Partner Community User," which is the modern equivalent of the "Partner Portal User" profile.

Question: 14

Which of the following are true about List Views?

A: Save list views for future use.

B: Specify which groups of users have access to the list view.

C: Print list views.

D: Follow records and view related Chatter posts.

E: Export List View data to Excel

F: All of the above

Correct Answer:

A, B, C

Explanation:

List views in Salesforce are a fundamental tool for managing records. Core functionalities include the ability to create and save custom views with specific filters and column layouts for future use (A). Administrators and users with appropriate permissions can control the visibility of these list views, sharing them with specific public groups, roles, or all users, which ensures data access is properly managed (B). Salesforce also provides a "Printable View" option, which generates a simplified, printer-friendly version of the list view, allowing users to easily print the data as displayed (C).

Why Incorrect Options are Wrong:

D: While you can add a "Follow" action to a list view, you cannot view related Chatter posts directly within the list view interface itself; this is done on the record's detail page.

E: Direct export to an Excel or CSV file is a standard feature of Salesforce Reports, not List Views. The "Printable View" can be copied, but it is not a direct file export function.

F: This option is incorrect because options D and E describe functionalities that are not standard features of List Views.

References:

1. Salesforce Help, Article ID 000385177, "Create and Customize List Views in Lightning Experience." This document confirms that users can create and save list views (A) and

manage their visibility by sharing them with specific groups of users (B). The section "Create a Custom List View" details the saving and sharing options.

2. Salesforce Help, Article ID 000385179, "Print List Views." This source explicitly states that both Salesforce Classic and Lightning Experience offer a "Printable View" option for list views, confirming the functionality described in option (C).

3. Salesforce Help, Article ID 000385178, "Work with List Views in Lightning Experience." This article details the actions available within a list view, such as inline editing and applying actions to records. It makes no mention of viewing Chatter feeds within the list view grid, supporting the exclusion of option (D).

4. Salesforce Help, Article ID 000380328, "Export Data." This documentation outlines the primary methods for exporting data from Salesforce, which are the Data Export Service, Data Loader, and Reports. It does not list "List Views" as a tool for direct data export, confirming that (E) is not a standard feature.

Question: 15

If a user has public read-only access to records [that he/she does not own], the following are true.

A: The user can view the record but not edit it

B: The user can view and delete the record, but not edit it

C: The user can change the owner of the record

D: The user can search for the record

E: The user can report on the record

Correct Answer:

A, D, E

Explanation:

When an object's Organization-Wide Default (OWD) is set to "Public Read-Only," all users are granted view access to every record of that object, regardless of ownership. This base level of access allows a user to see the record's data but explicitly prevents them from making any modifications (editing). Because the user has visibility into these records, the records will be included in search results and can be pulled into reports, provided the user has the appropriate profile permissions to run searches and reports. This access level does not grant permissions to delete or transfer ownership of records the user does not own.

Why Incorrect Options are Wrong:

B: "Read-Only" access does not grant permission to delete records. Deleting requires a higher access level, such as "Modify All" or record ownership.

C: Changing the owner of a record requires "Transfer" permission, which is a higher privilege not included in "Read-Only" access.

References:

1. Salesforce Help Documentation, "Organization-Wide Sharing Defaults." This document states for "Public Read Only": "All users can view all records but not edit them. Only the owner, and users above that role in the hierarchy, can edit the records." This directly supports option A and refutes options B and C.

2. Salesforce Security Guide, "Record-Level Access." This guide details the different levels of access. "Read" access allows users to view records. It clarifies that actions like editing, deleting, and transferring require higher levels of permission (Read/Write or Full Access) which are not granted by a "Public Read-Only" setting for non-owners.

3. Salesforce Help Documentation, "How Search Works." The documentation explains that search results are security-trimmed: "The records you see in search results are the records you have access to." This confirms that if a user can view a record (Option A), they can also find it via search (Option D).

4. Salesforce Help Documentation, "How Security Affects Reports." This source clarifies that report results are governed by the running user's access rights: "A report only displays records that the person running the report has permission to see... If a user can't access a record, that record won't be in the report." This supports option E.

Question: 16

The system administrator needs to prevent telesales teams from logging into Salesforce outside of the office. How will he/she do this?

A: There is not way to do this

B: Setup I Security Controls I Network Access and specify the team's range of IP addresses

C: Add the range of IP addresses to the team's profile(s)

D: Contact salesforce.com as this feature must be enabled

Correct Answer:

C

Explanation:

The most precise and effective method to restrict login access for a specific group of users to a designated location is by configuring Login IP Ranges on their assigned user Profile. By specifying the office's IP address range within the telesales team's profile(s), the administrator ensures that any login attempt from an IP address outside this range will be denied. This approach directly targets the specified user group without affecting other users in the organization, fulfilling the requirement accurately.

Why Incorrect Options are Wrong:

A: This is incorrect. Salesforce provides granular security controls, including the ability to restrict logins by IP address at the profile level.

B: Network Access sets org-wide trusted IP ranges. Logging in from outside this range triggers identity verification, but does not block the login, and it applies to all users.

D: This is a standard, self-service security feature available to administrators and does not require intervention from Salesforce support to be enabled.

References:

1. Salesforce Help, Control Login Access Policies: "You can set login hours and the range of IP addresses from which users can log in on a profile-by-profile basis." This directly supports using profiles for IP restrictions.

2. Salesforce Help, Restrict Login IP Ranges in the Original Profile User Interface: "You can restrict the IP addresses from which users can log in... When you define IP address

restrictions for a profile, logins from any other IP address are denied." This confirms that setting IP ranges on a profile denies access, which is the requirement.

3. Salesforce Help, Set Trusted IP Ranges for Your Organization: "When users log in to Salesforce from a recognized browser or device and an IP address within the trusted IP range, they gain access to your org without a verification challenge... Users who try to log in from an IP address outside the defined range are challenged to verify their identity." This clearly differentiates the org-wide Network Access feature (Option B) from the profile-level restriction (Option C).

Question: 17

To prevent a user from logging into the Salesforce org outside normal business hours, the System Administrator would do this in:

A: The user record

B: The user's profile record

C: Network settings

D: The role hierarchy

E: None of the above

Correct Answer:

B

Explanation:

To control when users can log in to the Salesforce organization, an administrator configures Login Hours on a user's assigned profile. This security feature allows the administrator to specify the permissible days and hours for access. If a user attempts to log in outside of these designated hours, access is denied. If a user is already logged in when their permitted hours end, their active session is terminated. This setting is applied to all users assigned to that specific profile.

Why Incorrect Options are Wrong:

A: The user record: The user record links a user to a profile but does not contain the login hour settings. You cannot set time-based restrictions directly on a user record.

C: Network settings: Network Settings (or Network Access) define trusted IP ranges for the entire organization, restricting where users can log in from, not when.

D: The role hierarchy: The role hierarchy is primarily used to control data visibility and record access, not authentication rules like login times.

E: None of the above: This is incorrect because the functionality described is a standard feature configured on the user's profile record.

References:

1. Salesforce Help, Restrict User Login Hours: "You can specify the hours when users can log in based on their profile. To set login hours, from Setup, in the Quick Find box, enter Profiles, and then select Profiles. Select a profile and click Login Hours."

2. Salesforce Help, Profiles: Under the "Settings and Permissions in Profiles" section, "Login Hours" is listed as a key setting that can be configured. It states that profiles control "The hours when users can log in."

3. Salesforce Security Guide, User Authentication: This guide details various security controls. In the section on "Identity Verification and Login Controls," it describes how profiles are used to enforce policies such as login hours and IP restrictions to secure user access. (See section: "Restrict Login Access to Certain Times and Locations").

Question: 18

Which feature effectively allows you to "lock" the converted amount on closed opportunities?

A: Locale

B: Company Profile

C: Multi-currency

D: Advanced Currency Management

E: None of the above

Correct Answer:

D

Explanation:

Advanced Currency Management is the specific feature that addresses the requirement. It allows an organization to manage dated exchange rates, which are conversion rates tied to a specific date range. When an opportunity is closed, the system uses the exchange rate that was active on the opportunity's CloseDate. This functionality effectively "locks" the converted amount to the historical rate, ensuring that financial reporting for past periods remains accurate and does not fluctuate with current exchange rate changes. Standard multi-currency, by contrast, applies the current exchange rate to all records, including closed opportunities.

Why Incorrect Options are Wrong:

A: Locale: This setting controls the display format for dates, times, numbers, and names, but does not manage currency conversion rates or locking mechanisms.

B: Company Profile: This contains foundational settings like the organization's default currency and locale but does not include features for managing dated exchange rates.

C: Multi-currency: This standard feature allows the use of multiple currencies but updates converted amounts on all opportunities (open and closed) whenever exchange rates are modified.

References:

1. Salesforce Help, "Manage Multiple Currencies": Under the section for Advanced Currency Management, the documentation states, "Advanced currency management allows you to manage dated exchange rates... For example, the exchange rate on January 1 was 1 USD to 1.39 AUD, but on February 1, it changed to 1 USD to 1.42 AUYour opportunities closed between January 1 and February 1 use the first exchange rate." This confirms the use of the CloseDate to lock the rate.

2. Salesforce Help, "Considerations for Enabling Multiple Currencies": This document clarifies the behavior difference: "When you enable advanced currency management, the converted amounts on opportunities... are based on the dated exchange rate for the opportunity Close Date." This directly supports the concept of "locking" the amount upon closing.

Question: 19

Which of the following are part of the Service Cloud offering?

A: Opportunities

B: Knowledge

C: Entitlements

D: Campaigns

E: Quotes

Correct Answer:

B, C

Explanation:

Salesforce Service Cloud is designed to manage customer support and service operations. Salesforce Knowledge is a core component, enabling the creation and management of a knowledge base that support agents and customers can use to find solutions to problems. Entitlement Management is another key feature, used to define, enforce, and track customer service levels, such as response times and support hours, based on their service agreements. These two features are fundamental to the Service Cloud offering.

Why Incorrect Options are Wrong:

A: Opportunities: This is a core object of the Sales Cloud, used to track potential sales deals and revenue.

D: Campaigns: This is a primary feature of Sales Cloud and Marketing Cloud, used to manage and track marketing initiatives.

E: Quotes: This is a standard feature within Sales Cloud, used to create and manage price proposals for products and services.

References:

1. Salesforce Help, Service Cloud: The official product documentation lists key features of Service Cloud, including "Knowledge" for creating a knowledge base and "Entitlement Management" for tracking service level agreements. (Salesforce Help, "Service Cloud", Key Capabilities section).

2. Trailhead, Service Cloud Basics Module, "Get to Know Service Cloud Features" Unit: This official training module explicitly identifies Knowledge and Entitlements as fundamental features of Service Cloud. It states, "With entitlements, you can specify the level of service each customer is entitled to." and "Knowledge lets you create and manage a knowledge base with your company's information."

3. Salesforce Help, Sales Cloud: The documentation for Sales Cloud lists "Opportunity Management," "Quote Management," and "Campaign Influence" as core features, clearly distinguishing them from the Service Cloud offering. (Salesforce Help, "Sales Cloud", Features section).

Question: 20

What should a system administrator use to disable an application for a group of users?

A: Sharing Rules

B: Web tabs

C: Page layouts

D: Profiles

E: Roles

Correct Answer:

D

Explanation:

Profiles are the primary mechanism for controlling user access to applications, objects, and fields. To disable an application for a specific group of users, a system administrator would edit the profile(s) assigned to those users. Within the profile settings, under "Assigned Apps," the administrator can uncheck the "Visible" setting for the desired application. This action removes the application from the App Launcher for all users assigned to that profile, effectively disabling it for them.

Why Incorrect Options are Wrong:

A: Sharing Rules: These are used to grant wider access to individual records, not to restrict or disable entire applications.

B: Web tabs: These are components within an application used to display external web pages; they do not control access to the application itself.

C: Page layouts: These control the visibility and arrangement of fields and related lists on object record pages, not access to applications.

E: Roles: Roles primarily control record-level access visibility through a hierarchy, determining which records users can see, not which applications they can use.

References:

1. Salesforce Help Documentation, "Profiles": "A profile is a collection of settings and permissions. Profiles control what users can do in Salesforce. They control access to apps,

tabs, objects, and fields." This document explicitly states that profiles control access to apps.

2. Salesforce Help Documentation, "Assign Apps to Profiles in the Original Profile User Interface": "You can specify the apps that are visible to users of a particular profile... In the Assigned Apps page, specify which apps are visible in the app menu." This provides the specific steps for using profiles to manage application visibility.

3. Salesforce Security Guide, "Data Security Model" (PDF): This guide details the layers of Salesforce security. It clearly places application and object access under the control of Profiles and Permission Sets, while record-level access is managed by Organization-Wide Defaults, Role Hierarchies, and Sharing Rules (See "Summary of Data Access and Visibility Features" table). This differentiates the function of Profiles (D) from Roles (E) and Sharing Rules (A).

Question: 21

If a user tries to login outside the IP range specified in their profile, the result will be.

A: They will be logged in as normal

B: They will have to reset their password

C: They will be prompted to activate their computer

D: They will be denied access

E: None of the above

Correct Answer:

D

Explanation:

Profile-level IP login ranges are a security control that restricts user access to a specified range of IP addresses. When a user attempts to log in from an IP address that falls outside of the valid range defined on their assigned profile, Salesforce will explicitly block the login attempt. The user receives a login error message and is denied access to the organization. This feature ensures that users can only access the system from approved locations, such as a corporate network or VPN.

Why Incorrect Options are Wrong:

A: This is incorrect because allowing a login would defeat the entire purpose of the IP restriction security feature.

B: A password reset is a response to a forgotten password or a lockout policy, not an IP range violation.

C: Computer activation, or identity verification, is triggered by a login from an unrecognized browser or device, not a restricted IP address.

References:

1. Salesforce Help, "Restrict Login IP Ranges in the Original Profile User Interface." This document states, "When you define IP address restrictions for a profile, a login from an undesignated IP address is denied."

2. Salesforce Help, "Control Login Access." This guide explains, "If you set IP restrictions at the profile level and a user with that profile logs in from an unrestricted IP address, that user is denied access to your org."

Question: 22

Used to set the default levels of access for users to records they do not own.

A: Organization Wide Defaults

B: Roles Hierarchy

C: Profiles

D: Sharing Rules

E: Manual Sharing

Correct Answer:

A

Explanation:

Organization-Wide Defaults (OWDs) are the cornerstone of the Salesforce sharing model. They define the most restrictive, baseline level of access a user has to records they do not own. All other record access tools, such as role hierarchies and sharing rules, are used to grant additional access beyond this default level. OWDs directly answer the question by establishing the default access for non-owned records across the entire organization before any other sharing mechanisms are applied.

Why Incorrect Options are Wrong:

B: Roles Hierarchy: Grants access vertically up the hierarchy to managers for records owned by their subordinates; it does not set the organization's default access level.

C: Profiles: Control object-level permissions (e.g., Create, Read, Edit, Delete) and field-level security, not the default access to specific records a user doesn't own.

D: Sharing Rules: Act as exceptions to OWDs to grant wider access to records for specific groups of users, rather than setting the default.

E: Manual Sharing: Allows individual users to grant access to their specific records on a case-by-case basis, which is not a default setting.

References:

1. Salesforce Help, "Organization-Wide Sharing Defaults": This document states, "Organization-wide sharing settings specify the default level of access that users have to

each other’s records. You use organization-wide sharing settings to lock down your data to the most restrictive level."

2. Salesforce Security Guide, "Record-Level Access": In the section "Controlling Access Using the Organization-Wide Defaults," it explains, "The first step in setting up record-level access is to set the organization-wide defaults for each object. The organization-wide defaults specify the baseline level of access that the most restricted user should have." (See page 13).

3. Salesforce Help, "Control Who Sees What": This guide presents a layered model for data access, clearly identifying Organization-Wide Defaults as the foundational first layer that controls the default access for all users.

Question: 23

If there are any users in the organization that shouldn't have view access to Account records, the OWD for Accounts should be set to

A: Public Read Only

B: Public Read/Write/Transfer

C: Private

D: None of the above

Correct Answer:

C

Explanation:

The principle of least privilege dictates that the organization-wide default (OWD) should be set to the most restrictive level required by the business. If there are any users who should not have view access to Account records they do not own, the OWD must be set to 'Private'. This setting ensures that, by default, only the record owner and users above them in the role hierarchy can view the record. Access for other users can then be selectively granted through other sharing mechanisms like sharing rules, manual sharing, or teams.

Why Incorrect Options are Wrong:

A: Public Read Only: This setting would grant all users in the organization view access to all Account records, which directly contradicts the stated requirement.

B: Public Read/Write/Transfer: This is even more permissive than Public Read Only and would grant all users broad access, violating the requirement that some users have no access.

D: None of the above: This is incorrect because 'Private' is the appropriate and available setting for this security requirement.

References:

1. Salesforce Help, Organization-Wide Sharing Defaults: This document defines the access levels for OWDs. It states for the 'Private' setting: "Only the record owner, and users above that role in the hierarchy, can view, edit, and report on these records." This confirms that 'Private' is the necessary baseline if some users must be prevented from viewing records.

2. Salesforce Security Guide, Chapter 3: Controlling Access to Records: This guide explains the sharing model. It emphasizes starting with the most restrictive settings (OWDs) and then opening up access. The guide states, "The first step in this level is to set your organization-wide sharing defaults... Set the default to the most restrictive level that you can." (p. 23). This supports the choice of 'Private' as the most restrictive option.

Question: 24

Which of the following are not standard objects?

A: Opportunities

B: Solutions

C: Job Applicants

D: Accounts

E: Campaigns

Correct Answer:

C

Explanation:

Standard objects are core objects included with every Salesforce org. Accounts, Opportunities, Campaigns, and Solutions are all examples of standard objects that support fundamental business processes in sales, marketing, and service. In contrast, "Job Applicants" is not a standard object provided by Salesforce. It represents a specific business need (recruiting) and is a classic example of a custom object that an administrator would create to extend the platform's functionality. The ability to create custom objects like "Job Applicants" is a key feature of the Salesforce platform's flexible data model.

Why Incorrect Options are Wrong:

A: Opportunities: This is a fundamental standard object used to track sales deals and potential revenue.

B: Solutions: This is a standard object used for creating and managing a knowledge base of common customer problems and their resolutions.

D: Accounts: This is a core standard object representing organizations, companies, or individuals with whom you have a business relationship.

E: Campaigns: This is a standard object used by marketing teams to plan, manage, and track marketing initiatives.

References:

1. Salesforce Help, Salesforce Objects Reference Guide, "Standard Objects": This official guide lists and describes the standard objects available in Salesforce. It includes Accounts,

Campaigns, Opportunities, and Solutions. "Job Applicants" is not listed as a standard object.

2. Trailhead, Admin Beginner Trail, "Data Modeling" Module, "Understand Custom & Standard Objects" Unit: This module explicitly defines standard objects as those included with Salesforce, citing "Account, Contact, Lead, and Opportunity" as examples. It then defines custom objects as those created by users to store information specific to their company, a category into which "Job Applicants" would fall.

3. Salesforce Developer Documentation, "Object-Oriented Programming for Admins", "What Are Objects, Fields, and Records?": This documentation clarifies the distinction: "Salesforce comes with a set of prebuilt objects, which we call standard objects... But what if you have a business need that isn’t covered by the standard objects? That’s when you build a custom object." This directly supports the concept of creating an object like "Job Applicants" to meet a unique business requirement.

Question: 25

A _________ defines a collection of settings and permissions that determines what users can see in the user interface, and what they can do.

A: Role

B: Chatter feed

C: Profile

D: Company Profile

Correct Answer:

C

Explanation:

A Profile is the fundamental Salesforce component that defines a user's experience. It is a collection of settings and permissions that governs what a user can access and perform within the application. This includes object permissions (Create, Read, Update, Delete), field-level security, which apps and tabs are visible, which page layouts and record types they can use, and various system-level permissions. Every user is assigned exactly one profile, which acts as the baseline for their access rights.

Why Incorrect Options are Wrong:

A: Role: A Role primarily controls record-level access visibility through the role hierarchy. It determines which records users can see, not their fundamental permissions or UI settings.

B: Chatter feed: A Chatter feed is a real-time collaboration tool for users to post updates and communicate. It does not define permissions or application settings.

D: Company Profile: The Company Profile (Company Information) stores organization-wide data, such as the company address, default time zone, and fiscal year, not user-specific permissions.

References:

1. Salesforce Help Documentation, "Profiles." This document states, "Profiles define how users access objects and data, and what they can do within the application. When you create users, you assign a profile to each one." It further lists the settings controlled by a profile, including object permissions, field permissions, app settings, and tab settings. (Salesforce Help, Article 000323378, "User Management > Profiles").

2. Salesforce Help Documentation, "Control Who Sees What." This guide explains the different layers of data access. In the section "Object-Level Security," it explicitly states, "The simplest way to control which users have access to which data is to control the objects a user can see, create, edit, or delete. You manage object-level permissions with profiles and permission sets." (Salesforce Help, "Control Who Sees What" PDF, Object-Level Security section).

3. Salesforce Help Documentation, "Overview of Roles." This resource clarifies the function of roles: "Roles control the level of visibility that users have into your organization's data. Users at any given role level can view, edit, and report on all data owned by or shared with users below them in the role hierarchy..." This confirms roles are for record access, not the broad permissions described in the question. (Salesforce Help, Article 000323389, "User Management > Roles").

Question: 26

When a user logs in the first time to Salesforce, the following takes place (Choose all that apply.)

A: A cookie is placed in the browser

B: Pop ups are automatically disabled

C: Their IP address is added to a trusted list

D: They are prompted to answer a security question

Correct Answer:

A, D

Explanation:

When a user logs into Salesforce for the first time from a given browser or device, two key events occur. First, Salesforce places a session cookie in the user's browser (A), which is essential for maintaining the authenticated session and application functionality. Second, because the browser or device is unrecognized, Salesforce initiates an identity verification challenge to ensure security (D). Answering a security question is a standard, configurable method for this verification process. Upon successful verification, an additional cookie is typically set to "trust" the browser for future logins.

Why Incorrect Options are Wrong:

B: Salesforce does not control browser-level settings like pop-up blocking. This is managed by the user within their web browser's preferences.

C: Trusted IP ranges are configured manually by an administrator under Network Access settings. A user's IP is not automatically added to this list upon login.

References:

1. Salesforce Help. (n.d.). Identity Verification. This document states, "When users log in to Salesforce from an unrecognized browser or device... they’re prompted to verify their identity." It lists several verification methods, including answering a security question.

2. Salesforce Help. (n.d.). Set or Change Your Security Question. This page notes, "If your Salesforce admin requires a security question for password resets or other identity verification scenarios, you’re prompted to set one up." This confirms the security question is an integral part of Salesforce's identity features.

3. Salesforce Help. (n.d.). Supported Browsers and Devices for Lightning Experience. This documentation implicitly confirms the use of cookies by stating browser privacy settings that block cookies can cause issues with Salesforce functionality. It notes, "Salesforce requires you to enable cookies in your browser to use all of its features."

Question: 27

In order to enable multi-currency feature in Salesforce, you must

A: Contact Salesforce.com

B: Check the Enable Multi-currency checkbox in your Chatter profile

C: Operate your business in at least two different countries

D: You cannot enable this feature once you've implemented Salesforce.

Correct Answer:

A

Explanation:

Enabling the multi-currency feature is an irreversible action with significant, permanent implications for an organization's data, particularly in reporting and forecasting. Due to the gravity and finality of this change, the standard procedure requires an administrator to contact Salesforce Support to request its activation. This ensures that the customer fully understands the consequences, as the feature cannot be disabled once it is turned on.

Why Incorrect Options are Wrong:

B: Chatter profile settings are for user collaboration and personal preferences, not for organization-wide currency configurations.

C: While operating in multiple countries is the business justification for using this feature, it is not the technical step required to enable it.

D: This statement is false. The multi-currency feature can be enabled at any time after implementation, but the action is permanent.

References:

1. Salesforce Help, Article ID 000387221, "Enable Multiple Currencies": This document outlines the process and implications. It states, "After you enable multiple currencies for your organization, you can't disable it." The requirement to contact Salesforce is the established safe-gate procedure for such a permanent change.

2. Salesforce Help, Article ID 000384695, "Considerations for Enabling Multiple Currencies": This resource emphasizes the permanence of the action: "Enabling multiple currencies is a permanent change that you can't undo. Before you enable it, make sure that you

understand the implications." This supports the rationale for involving Salesforce Support (Option A) to ensure due diligence.

Question: 28

A system administrator can opt to lock users out of the Salesforce org if they exceed a certain number of failed login attempts.

A: True

B: False

Correct Answer:

True

Explanation:

Salesforce provides system administrators with granular control over security settings, including password policies. An administrator can define the "Maximum invalid login attempts" a user can make before their account is locked. This is a fundamental security feature to prevent brute-force attacks. The administrator can also set the "Lockout effective period," which determines how long the user remains locked out. These settings can be configured for the entire organization or customized for specific user profiles.

Why Incorrect Options are Wrong:

References:

1. Salesforce Help Documentation, "Set Password Policies": This official document explicitly details the settings available to administrators. It lists the following fields:

Maximum invalid login attempts: "The number of login failures allowed for a user before they are locked out of Salesforce. Possible values are 3, 5, 10, or No limit."

Lockout effective period: "The duration for which a user is locked out after too many login failures. Possible values are 15 minutes, 30 minutes, 60 minutes, or Forever."

Source Reference: Salesforce Help, Article Number 000385101, "Set Password Policies".

2. Salesforce Trailhead, "User Authentication" Module, "Control Login Access" Unit: This official training module explains how administrators manage user access and security. It states: "You can determine the level of security for user passwords in your Salesforce org. You can set password history, length, and complexity requirements. You can also specify what to do when a user forgets a password. [...] You can also set the session timeout length and what happens during a timeout. And you can lock users out of the org after a certain number of failed login attempts."

Source Reference: Trailhead by Salesforce, Module: User Authentication, Unit: Control Login Access.

Question: 29

Locale settings control how users view date formats, time formats and number formats.

A: True

B: False

Correct Answer:

[True]

Explanation:

The statement is correct. In Salesforce, the "Locale" setting is a fundamental user-level and organization-level configuration that directly controls the display format for specific data types. It ensures that users see dates, times, numbers, and addresses in a format that is conventional for their geographical region. For example, a user with a "United States" locale will see dates as MM/DD/YYYY and numbers with a period as the decimal separator (e.g., 1,234.56), whereas a user with a "German (Germany)" locale will see dates as DD.MM.YYYY and numbers with a comma as the decimal separator (e.g., 1.234,56).

Why Incorrect Options are Wrong:

References:

1. Salesforce Help Documentation, "Supported Locales": This official document explicitly states, "The locale setting determines the display formats for date and time, user names, addresses, and commas and periods in numbers." This directly confirms the elements mentioned in the question.

Source: Salesforce Help, "Supported Locales".

2. Salesforce Help Documentation, "Edit Your Personal Information": When describing the user detail page, this document explains the function of the Locale field: "Determines the display format of date, time, and number fields, for example, 12/31/2020 and 1,000.00."

Source: Salesforce Help, "Edit Your Personal Information", User Detail Fields section.

3. Salesforce Help Documentation, "Define Company Information": This document details the organization-wide default settings. For "Default Locale," it states: "Determines the display format of date, time, number, and phone number fields for all users in your organization."

Source: Salesforce Help, "Define Company Information", Company Information Fields section.

Question: 30

User interface settings are global settings and apply to all users of an org.

A: True

B: False

Correct Answer:

[True]

Explanation:

The settings found within the "User Interface" page in Salesforce Setup are considered global, or org-wide, configurations. When an administrator modifies these settings—such as enabling inline editing, collapsible sections, or hover details—these changes are applied universally across the organization. They define the baseline user experience for all users and are not controlled on a per-profile or per-user basis.

Why Incorrect Options are Wrong:

References:

1. Salesforce Help Documentation: User Interface Settings.

Location: Salesforce Help Portal.

Reference: The documentation page is titled "User Interface Settings" and its introductory sentence states, "Control the user interface for your organization." The term "organization" signifies that these settings are global and not specific to a subset of users. The page then lists numerous org-wide settings like "Enable Collapsible Sections" and "Enable Inline Editing."

2. Trailhead by Salesforce: User Engagement Module, Customize the User Interface Unit.

Location: Trailhead, User Engagement Module.

Reference: In the "Customize the User Interface" unit, the text explains, "Let’s check out some of the most common UI settings you can configure for your org." This phrasing explicitly confirms that the configuration is done at the organizational ("org") level, affecting all users within it.