PassQueen
a.k.a dumpsqueen.com

Jira Administrator Exam

Atlassian ACP-100

Version Demo

Total Demo Questions: 16

Total Premium Questions: 163

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Jira Administration	21
Topic 2, User Management	13
Topic 3, Project Configuration	15
Topic 4, Issue Configuration	42
Topic 5, Workflow Configuration	26
Topic 6, Permissions and Security	32
Topic 7, Notifications	11
Topic 8, Jira Software	3
Total	163

QUESTION NO: 1

A project workflow has a Reopen transition from Done to In Progress.

Users report that reopened issues continue to appear as resolved in reports.

Which workflow change will correct this problem?

A. Add a post function to clear the Resolution field on the Reopen transition.

B. Add a condition that requires the Resolution field to be empty on the Reopen transition.

C. Remove the Resolution field from the Done transition screen.

D. Change the name of the In Progress status.

E. Make Resolution optional in the field configuration.

ANSWER: A

Explanation:

Add a post function to the Reopen transition that clears the **Resolution** field. Jira considers an issue resolved when its Resolution field contains a value, independently of the status name. Moving an issue from Done to In Progress does not automatically clear Resolution unless the workflow is configured to do so.

Clearing Resolution as part of the Reopen transition ensures that the issue is treated as unresolved after it is reopened and that reports based on resolution state produce the expected results. See Atlassian's documentation on configuring advanced issue workflows.

QUESTION NO: 2

A medical clinic has decided to use Jira. Their project will allow patients to file medical complaints.

The requirements for the project are as follows:

Members of the group (jira-patients) must be able to see only their own complaints. Members of the group (medical-board) must be able to see all complaints.

Based only on these two requirements, which two configurations used together will satisfy them? (Choose

two.)

A. Implement an issue security scheme with three levels: (#1) Group (jira-patients), (#2) Reporter, and (#3) Group (medical-board).

B. Implement an issue security scheme with two levels: (#1) Reporter and (#2) Group (medical-board).

C. In the permission scheme, add Reporter and Group (anonymous) to Browse Projects and Create Issues.

D. In the permission scheme, add Group (jira-patients) and Group (medical-board) to Browse Projects and Create Issues permissions.

E. Implement an issue security scheme with one level: Reporter and Group (medical-board).

ANSWER: D E

Explanation:

Issue security and project permissions must be configured together because they control different parts of access. **Implement an issue security scheme with one level: Reporter and Group (medical-board).** provides the required issue-level visibility. Each complaint assigned this security level is visible to its own reporter, allowing a patient to access their own complaint, and to every member of `medical-board`, allowing the board to review all complaints. The security level should

be set as the project's default level or otherwise applied automatically so that every newly filed complaint receives this protection.

In the permission scheme, add Group (jira-patients) and Group (medical-board) to Browse Projects and Create Issues permissions. gives the relevant users access to the project and allows patients to submit complaints. Browse Projects is the baseline project-access permission, while the issue security level continues to restrict which individual issues a user can view after they enter the project. Thus, patients do not gain visibility into other patients' complaints merely from having project browse access, while medical-board members receive visibility through their membership in the security level.

See Atlassian's documentation on configuring issue security schemes and managing project permissions.

QUESTION NO: 3

You needed to replace the legacy Jira group all-staff-europe with a newly created all-staff-global group.

You created the new group and you migrated all users to the new group. Then you deleted the legacy group.

Which four problems might users report after the change? (Choose four.)

A. Filter subscriptions send out errors instead of issues statistics.

B. Workflow transitions are hidden from certain users.

C. Users are not able to perform bulk change operations.

D. Users are not able to log in to Jira anymore.

E. Comments that were restricted to the legacy group are lost.

F. Filter results return an incorrect number of issues.

ANSWER: B C E F

Explanation:

Replacing users in a group does not replace the group wherever Jira configuration refers to that group name. Jira stores group-based grants and restrictions in administrative configuration, including workflow conditions, global permissions, comment visibility restrictions, and filter-related permissions or queries. Consequently, a transition whose condition names `all-staff-europe` will no longer be offered to users solely because they belong to `all-staff-global`. Likewise, if Bulk Change was granted through the deleted group, affected users lose that global permission until the new group is added to the relevant permission configuration.

Comments restricted to the legacy group can no longer be used through the intended group-based visibility arrangement after that group is removed, so users may report that those restricted comments have been lost. Filters can also produce a different issue total when their sharing, visibility, or group-based JQL logic still relies on the deleted group; migrating memberships alone does not update those saved references. Administrators should inventory every group reference and explicitly substitute the replacement group before retiring the old one. Atlassian's guidance on group administration is available in Managing groups, and its documentation on access grants is available in Managing global permissions.

QUESTION NO: 4

You are tidying up a Jira project and find that the following two issue types are being used.

- Task
- Assignment

They seem very similar. If both are not needed, you could convert all existing Assignment issues in the project into Task issues and remove the Assignment issue type from the project.

Which project configurations would you check to see if it is necessary to keep the two as separate issue types instead? (Choose three.)

A. Issue Security Levels

B. Field Configurations

C. Components

D. Permissions

E. Workflows

F. Field Contexts

ANSWER: B E F

Explanation:

Field Configurations, **Workflows**, and **Field Contexts** should be reviewed before consolidating Assignment into Task. Jira can apply different field behavior to individual issue types through a field configuration scheme. For example, Assignment may have fields that are required, hidden, or use a different screen behavior than Task. If Assignment issues are converted, those field requirements and visibility rules may no longer apply as intended.

A workflow scheme can map each issue type to a distinct workflow. Therefore, Assignment may have its own statuses, transitions, validators, conditions, post-functions, or resolution behavior. Reviewing the workflow mapping and the workflow itself is essential before changing the issue type, because converted issues will follow the workflow associated with Task.

Custom-field contexts can also be limited to particular projects and issue types. Assignment may expose a different set of custom-field options, defaults, or even field applicability than Task. Checking contexts ensures that data entered on Assignment issues remains meaningful and available after conversion. Atlassian documents issue-type-specific workflow associations in Configure advanced issue workflows and field behavior by issue type in Associate field behavior with issue types.

QUESTION NO: 5

Some of your project owners would like to make their projects publicly accessible over the Internet. These projects will not require login.

You could support this by allowing read-only anonymous access to the projects.

Which two additional factors should you take into consideration when setting this up? (Choose two.)

A. Anonymous users could see other users' names.

B. Anonymous users could export all issues from Jira.

C. Licensed users might accidentally comment anonymously rather than logging in first.

D. Internet search engines could index data.

E. Anonymous users could find a full list of all your projects.

F. Spam bots could add comments.

ANSWER: B D

Explanation:

"Anonymous users could export all issues from Jira." is an important consideration because anonymous access is governed by the permissions granted to the Anyone group. When anonymous users can browse issues in public projects, they can use Jira's issue-search and export capabilities for the issues that are exposed to them, subject to the instance's export settings. Exporting makes it much easier to aggregate, copy, and redistribute project data than viewing individual issue pages, so administrators should ensure that public projects contain no information that should not be downloadable at scale.

“Internet search engines could index data.” is also correct because issue and project pages available without authentication can be discovered and crawled by search engines. Once indexed, titles, descriptions, comments, attachments or other exposed content may appear in search results and can remain cached or discoverable even after permissions are later tightened. Before enabling anonymous browsing, administrators should review the information published in each project and apply appropriate controls for public indexing where needed. Atlassian documents anonymous-access configuration and its security implications in its anonymous access documentation, and provides guidance on preventing crawler exposure in its search-engine indexing knowledge base article.

QUESTION NO: 6

You have two issue types in your HR project: Hire and Fire.

Which two requirements can be met through changes only to field configurations? (Choose two.)

A. For the Fire issue type, the Description field should have a default value of “Termination”.

B. For both issue types, the Employee Name custom field must be required upon creation and must never be

blank.

C. For the Hire issue type, the field description for the Due Date field should read “First day of work”.

D. For both issue types, the Resolution should be set once the issues are being resolved.

E. For both issue types, the Assignee field should be hidden when creating but not when viewing an issue.

F. For the Fire issue type, the default value for the Priority field should be Blocker.

ANSWER: B C

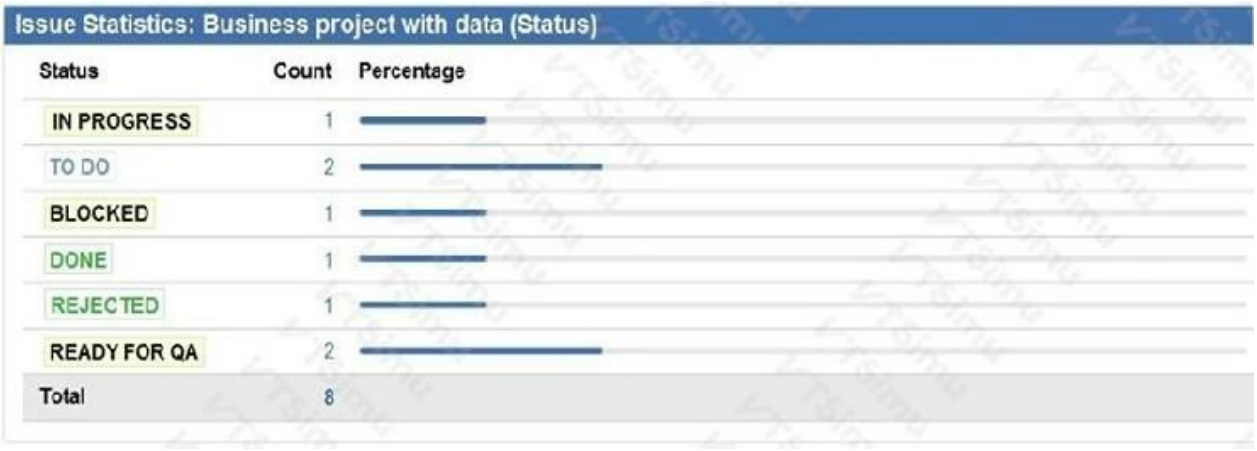
Explanation:

“For both issue types, the Employee Name custom field must be required upon creation and must never be blank.” can be met with a field configuration. A field configuration can mark a field as required. When the relevant field configuration is associated with both the Hire and Fire issue types through a field configuration scheme, Jira enforces that Employee Name has a value whenever the field is presented for required entry, including issue creation. This is appropriate for a data element that must always be supplied for these HR requests.

“For the Hire issue type, the field description for the Due Date field should read ‘First day of work’.” is also a field-configuration change. Administrators can edit the description associated with a field in a field configuration. By assigning a dedicated field configuration to the Hire issue type, the Due Date field can display guidance tailored to hiring work without changing the field’s description for Fire issues. Field configurations are mapped to issue types using field configuration schemes, enabling these issue-type-specific behaviors within the same project. Atlassian documents field descriptions, required settings, and field configuration associations in its field configuration documentation and field behavior by issue type guide.

QUESTION NO: 7

A dashboard displays an Issue Statistics gadget as shown.



Issue Statistics: Business project with data (Status)

Status	Count	Percentage
IN PROGRESS	1	
TO DO	2	
BLOCKED	1	
DONE	1	
REJECTED	1	
READY FOR QA	2	
Total	8	

The dashboard owner wants to change the order of the statuses shown in the gadget to appear as follows.

- To Do
- In Progress
- Ready For QA
- Blocked
- Rejected
- Done

Which action will permanently arrange the statuses into the required order?

A. Reorder the statues on the Status administration page.

B. Change the Sort Direction option in the gadget to Ascending.

C. Change the category of the statuses.

D. Add numbers to the status names to allow them to be sorted in numerical order.

E. Change the gadget Sort By field to Total.

ANSWER: D

Explanation:

Add numbers to the status names to allow them to be sorted in numerical order. The Issue Statistics gadget groups issues using the selected statistic type and applies its available sorting behavior to the displayed values; it does not provide a separate, arbitrary manual ordering for individual status values. Prefixing each status with an ordered numeric value creates a durable sort key in the status value itself. For example, naming the statuses “1 - To Do,” “2 - In Progress,” “3 - Ready For QA,” and so on makes the desired business-process sequence available to the gadget’s natural/alphabetical ordering. This produces a consistent sequence whenever the gadget is rendered, rather than depending on the current issue totals or a one-time dashboard arrangement. Numeric prefixes should use equal-width values where the sequence could exceed nine items, such as “01,” “02,” and “10,” so lexical ordering remains aligned with the intended numeric order. Statuses are global Jira configuration objects and their names can be managed by a Jira administrator, as described in Atlassian’s status administration documentation. The Issue Statistics gadget’s configuration and sorting concepts are documented in Atlassian’s Issue Statistics gadget documentation.

QUESTION NO: 8

The notification scheme used by your project is shown.

Whenever issues are deleted, only users in the Developers project role are notified but not members of Acme group. Where must Acme group be added to fix this?

A. Manage Group Filter Subscriptions global permission

B. Browse Projects project permission

C. Issue Created notification event

D. Delete Issues project permission

E. Issue Deleted notification event

ANSWER: E

Explanation:

Acme group must be added as a recipient for the **Issue Deleted notification event** in the notification scheme associated with the project. Jira notification schemes define who receives notifications for each individual issue event, rather than granting notification delivery through a project permission or global permission. Since members of the Developers project role already receive the deletion notification, the scheme is evidently configured with that role as a recipient for the deletion event. Adding Acme group to the same event's recipient list ensures that group members are also selected when Jira fires the event after an issue is deleted.

An administrator can make this change from Jira administration by opening the relevant notification scheme, locating the Issue Deleted event, choosing to add a notification recipient, and selecting the Acme group. The project must continue to use that notification scheme for the configuration to take effect. Atlassian's documentation explains that notification schemes map issue events to recipients and can notify groups or project roles: Creating a notification scheme. The available Jira issue events, including issue deletion, are documented at Issue events.

QUESTION NO: 9

Caleb was recently assigned to several issues in the DFV project but did not receive email notifications about the assignment. He received notifications about other changes to DEV issues. Identify a possible reason.

A. Assignable User permission

B. Assign Issues permission

C. Browse Projects permission

D. Issue Assigned event

E. Issue Updated event

ANSWER: D

Explanation:

Issue Assigned event is correct because Jira sends assignment notifications through its event-and-notification-scheme mechanism. When an issue's assignee changes, Jira raises the Issue Assigned event. The notification scheme associated with the specific project determines whether that event sends email and, importantly, which recipients are selected, such as the current assignee. Therefore, Caleb can receive notifications for activity in DEV while receiving no assignment email from DFV if DFV uses a different notification scheme whose Issue Assigned event does not notify the current assignee, has no recipients configured for that event, or otherwise has different event notification settings. Notification schemes are project-specific, so notification behavior is not necessarily consistent across projects for the same user. The fact pattern specifically concerns an assignment action rather than a general edit, making the assignment event the relevant configuration point to investigate. An administrator should review the notification scheme associated with DFV and inspect the recipients configured for the Issue Assigned event. Atlassian documents that notification schemes define which events generate notifications and who receives them: Configure notification schemes. Jira's event model, including the events used by notification schemes, is also described in Configuring events.

QUESTION NO: 10

Your Jira support project has allowed anonymous customers to create issues through an incoming mail

handler for some time.

In order to enhance efficiency, your project manager has inquired about the possibility of allowing anonymous users to also create issues using Jira instead of the mail handler, but without allowing further access or need

of a license.

Which two actions will let you meet the requirement? (Choose two.)

A. Create an issue security scheme with a default level allowing only licensed Jira users to access issues.

B. Ensure that the Jira mode in the general configuration has been set to Public.

C. Add Anyone to the Browse Projects permission in the project's permission scheme.

D. Add Anyone to the Create Issues permission in the project's permission scheme.

E. Ensure that the Reporter is not required in the project's field configuration scheme.

ANSWER: B C D

Explanation:

Anonymous users can submit issues through Jira only when Jira is configured to permit public (unauthenticated) access and the target project grants the relevant permissions to the special *Anyone* permission holder. Setting Jira mode to Public enables Jira to serve requests from people who are not logged in; it does not create accounts or consume Jira licenses. This is the required global setting for an anonymous web user to reach a project's available public functions.

At the project level, anonymous users must be able to browse the project and create issues. Browse Projects is the foundational project-access permission, while Create Issues authorizes submission of a new issue. Granting both permissions to Anyone limits anonymous access to the specific capabilities granted in that permission scheme; it does not grant a Jira license or general authenticated access. The special Anyone holder represents both authenticated and unauthenticated users and is configured directly in the permission scheme rather than as an ordinary Jira group.

For Jira Server/Data Center administration details, see Atlassian's documentation on configuring Jira application options and managing project permissions.

QUESTION NO: 11

One of the HR managers created a filter and shared the subscription with members of the hr-managers group. The filter contains the following valid JQL query:

Manager = currentUser() AND Manager in membersOf("hr-managers") Which issues will be included in the subscription?

A. Only issues where the user who created the filter is listed in the Manager field.

B. Only issues where the group hr-managers is listed in the Manager field.

C. Only issues where the recipient of the email is listed in the Manager field.

D. All issues where the user listed in the Manager field is a member of the hr-managers group.

E. All issues that are assigned to any member of the hr-managers group.

ANSWER: A

Explanation:

Only issues where the user who created the filter is listed in the Manager field is correct. A filter subscription is executed in the context of its owner, so `currentUser()` resolves to the user who owns (and, in this scenario, created) the filter subscription. It does not resolve separately for each person receiving the subscription email. The first clause therefore limits the results to issues whose `Manager` field contains that filter owner.

The second clause, `Manager in membersOf("hr-managers")`, further requires the user in the Manager field to belong to the `hr-managers` group. Since the query uses `AND`, an issue is included only when both conditions hold: the manager is

the subscription owner and that owner is a member of the specified group. In the stated scenario, the filter was created by an HR manager, so qualifying issues are those managed by that individual. Sharing a subscription controls who receives its email; it does not change the identity used by `currentUser()` when Jira evaluates the saved filter. Atlassian documents the behavior of `currentUser()` in its JQL function reference and filter-subscription administration in Manage filter subscriptions.

QUESTION NO: 12

Managers want to ensure that every issue in Jira always has an assignee.

Which change will definitely meet this requirement?

A. Update post functions to set the assignee appropriately at each workflow transition.

B. Set Default Assignee to Project Lead in every project.

C. Use components for automatic assignment in every project.

D. Make the assignee required on workflow transition screens.

E. Make the assignee required through field configurations.

F. Set the global option “Allow unassigned issues” to OFF.

ANSWER: F

Explanation:

Set the global option “Allow unassigned issues” to OFF is the change that enforces the requirement at the Jira-application level. When unassigned issues are not allowed, Jira requires an issue to have a valid assignee rather than permitting the assignee value to be left as *Unassigned*. This is a global setting, so its enforcement is not dependent on a particular project’s default-assignee configuration, component setup, field configuration, screen, or workflow design. Consequently, it provides the appropriate baseline control when the policy applies to every issue across Jira, including issues created through the normal create process and issue updates that would otherwise result in no assignee. Administrators should also ensure that relevant users and project roles have assignable users available, because Jira must be able to select a valid assignee when an issue is created or reassigned. Atlassian documents this setting under Jira application options and explains that it controls whether issues can remain unassigned. See Atlassian’s Jira application options documentation and Atlassian Support: Configure Jira application options.

QUESTION NO: 13

Three team members have left the company and their issues need to be re-assigned to various -users.

All of their issues are in the Marketing project which uses the Default Notification Scheme. The scheme has never been updated.

How do you inform the new assignees about their re-assigned issues?

A. Add an announcement banner to the marketing project to inform team members.

B. Perform a single bulk operation to mention all new assignees in a comment.

C. Add an announcement banner to each new assignee’s dashboard.

D. Perform bulk operations to re-assign the issues and notify the new assignees.

E. Use the Send email feature to inform the individual new assignees.

ANSWER: D

Explanation:

Perform bulk operations to re-assign the issues and notify the new assignees. Jira's Default Notification Scheme includes an *Issue Assigned* event notification for the current assignee. Consequently, when an administrator changes an issue's assignee, Jira generates the assignment event and emails the user who has become the assignee, provided email notifications are enabled for that user and the instance. Because the project uses the unmodified default scheme, this behavior is already configured; no notification-scheme change is required.

Bulk change is the appropriate administrative method because the issues belong to several former team members and can be selected and reassigned efficiently in one or more bulk operations. During the bulk transition, the administrator should retain the email-notification setting so the assignment events are sent. Jira applies the selected reassignment to each issue and triggers the standard notification mechanism for its resulting assignee. This both updates ownership and ensures each incoming owner receives notice through the project's configured notification scheme. Atlassian documents the recipients and events configured in notification schemes at Configure notification schemes, and documents the bulk issue change process at Bulk change issues.

QUESTION NO: 14

A project uses an issue security scheme to restrict access to sensitive issues.

Which three statements are true about issue security? (Choose three.)

A. A default security level can be applied automatically to new issues.

B. A user must have Browse Projects permission before issue security access can allow the user to view an issue.

C. Set Issue Security permission allows a user to change an issue's security level.

D. An issue security level can grant a user Browse Projects permission.

E. Every project using an issue security scheme must use a different security level.

F. Issue security levels can be configured only for closed issues.

ANSWER: A B C

Explanation:

A default security level can be configured in an issue security scheme. Jira applies that level automatically to newly created issues in projects associated with the scheme, unless another security level is explicitly set during creation or by automation.

A user needs the *Browse Projects* permission as well as access through the issue's security level to view a secured issue. Issue security further restricts project visibility; it does not grant access to a project that the user cannot browse.

The *Set Issue Security* project permission controls who can apply, change, or clear the security level on an issue. It does not by itself permit a user to view every issue protected by a security level. See Atlassian's documentation on issue security schemes and project permissions.

QUESTION NO: 15

Ann and Jake both clicked the Edit button on an issue in project ASTRO. While editing, the Priority field is displayed for Ann but not for Jake. Identify one possible reason.

A. Edit Issue screen

B. project permissions

C. custom field context

D. security levels

E. Configure Fields user setting

ANSWER: E

Explanation:

The correct answer is **Configure Fields user setting**. Jira lets each user personalize the fields displayed on issue operation screens, including the Edit Issue screen, through the Configure Fields control. This is a per-user preference: one user can hide a field from an operation screen while another user editing the very same issue continues to see it. Therefore, Ann and Jake can have different visible fields despite using the same project, issue type, workflow transition, and screen configuration. In this scenario, Jake may have hidden Priority in his personal field-display settings, whereas Ann has not. The field is not removed from the shared Edit Issue screen; it is simply not displayed for that individual user. Jira documentation describes how users can configure which fields appear during issue operations, and notes that these choices are retained as user preferences. See Atlassian's documentation on configuring fields on Jira issue screens and the Jira Server/Data Center screen configuration documentation for the distinction between shared screens and user-visible field behavior.

QUESTION NO: 16

After a recent upgrade to your Jira system, one of the apps your organization depends on is not working reliably.

Which two methods can you use to debug and resolve this issue? (Choose two.)

A. Ask the System Administrator for catalina.out logs and inspect for stack traces.

B. Ask the System Administrator to enable the SQL log.

C. Ask the System Administrator to set package com.atlassian to Trace logging level.

D. Ask the System Administrator to add the app's package to the logger.

E. Ask the System Administrator to set the logging level to FATAL on all package names, Under Logging &

Profiling.

ANSWER: C D

Explanation:

Temporarily setting the `com.atlassian` package to the TRACE logging level can provide detailed diagnostic events from Jira components while the failing workflow is reproduced. TRACE output includes more context than normal operational logging, which can help identify the sequence of calls, configuration interactions, and exceptions associated with the upgrade-related problem. Because this level can generate a substantial volume of data, it should be enabled only for the shortest practical period, with the time of reproduction recorded for correlation.

Adding the affected app's logging package to Jira's logger is the more targeted diagnostic method. Jira's Logging and Profiling administration page lets an administrator create a logger entry for a specific package or class and select an appropriate verbosity level. App vendors commonly provide the exact logger package and level needed for troubleshooting. This produces focused evidence in Jira's application logs, allowing the administrator or vendor to isolate the app behavior and validate the resolution without relying solely on broad platform-level output. Atlassian documents the use of custom logger entries and temporary diagnostic levels in Logging and profiling for Jira. Additional app troubleshooting guidance is available in the Jira Data Center knowledge base.