Conductor Roles and Permissions UX Evaluation

Interaction Design

Date: 07 November 2012

Version: 0.1

AEOLUS™

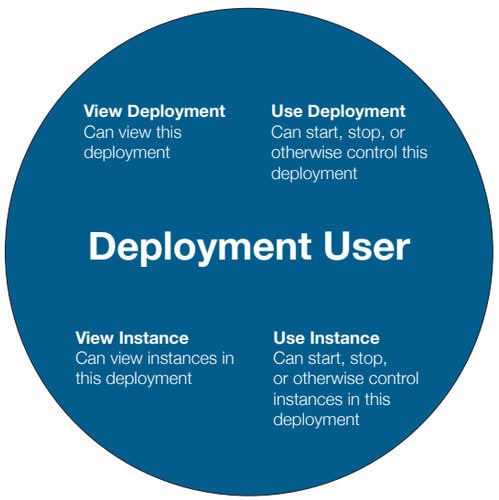
What's in this doc

- Summary of how permissions work in Conductor
- Review of the current user experience with notes and suggestions for improvement
- Concept wireframes

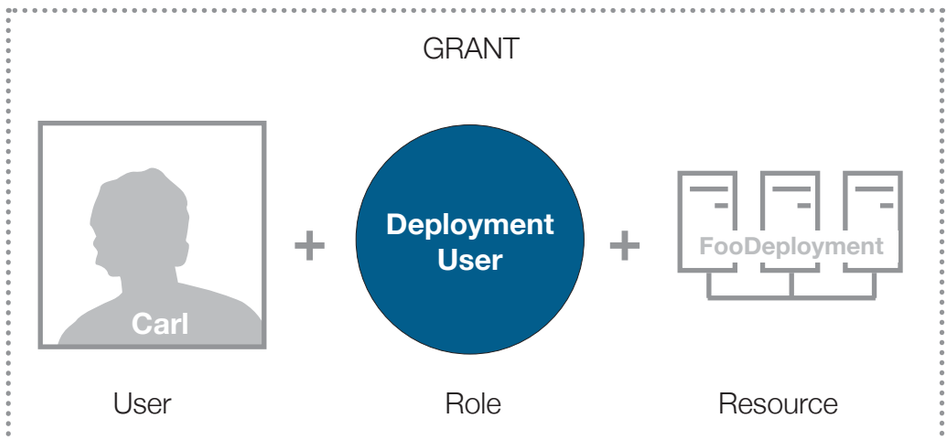
How permissions work in Conductor

A **role** is an abstract collection of lower-level privileges or actions. Things like “view”, “use”, “modify”, “create.” Sometimes it includes privileges on lower level objects.

When a user is **granted** a role on some resource, the user can perform the actions described in the role on that resource.



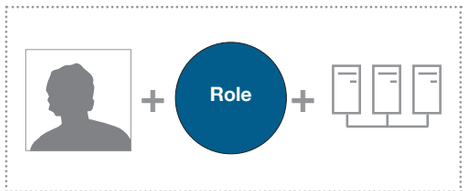
The **Deployment User** Role includes four permissions and covers two object types



Carl has **Deployment User** on **FooDeployment**, so he can view it, use it, and also view and use it’s instances.

Roles and Permissions: https://redmine.aeolusproject.org/redmine/projects/aeolus/wiki/Roles_and_Permissions
List of all Roles: https://redmine.aeolusproject.org/redmine/projects/aeolus/wiki/Roles_list

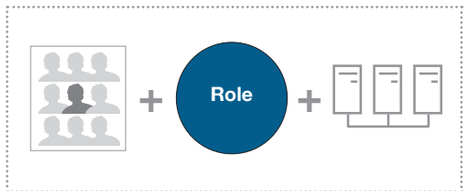
Users are granted roles on a given resource in several ways



Directly to the user

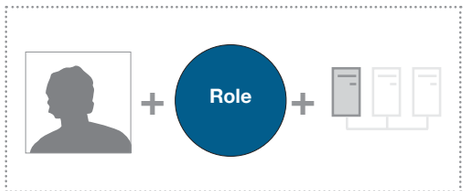
Someone, like an admin, sets the role of one user to one resource.

Or, the user creates a new resource, and is thus the “owner” of it.



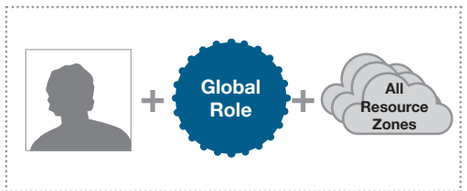
Indirectly via group membership

The user is placed in a group which itself has been granted a role on a resource



Via object inheritance

Permissions on higher-level resources, like a deployment, mean that users (and groups) also obtain the privileges defined in the role on instances contained within the deployment.



Via global roles

Global roles impart privileges across all resources of a given type. So a Global Cloud Resource Zone Administrator has full access to all Cloud Resource Zones. Global Roles can also be applied to Groups.

Roles and Permissions: https://redmine.aeolusproject.org/redmine/projects/aeolus/wiki/Roles_and_Permissions
List of all Roles: https://redmine.aeolusproject.org/redmine/projects/aeolus/wiki/Roles_list

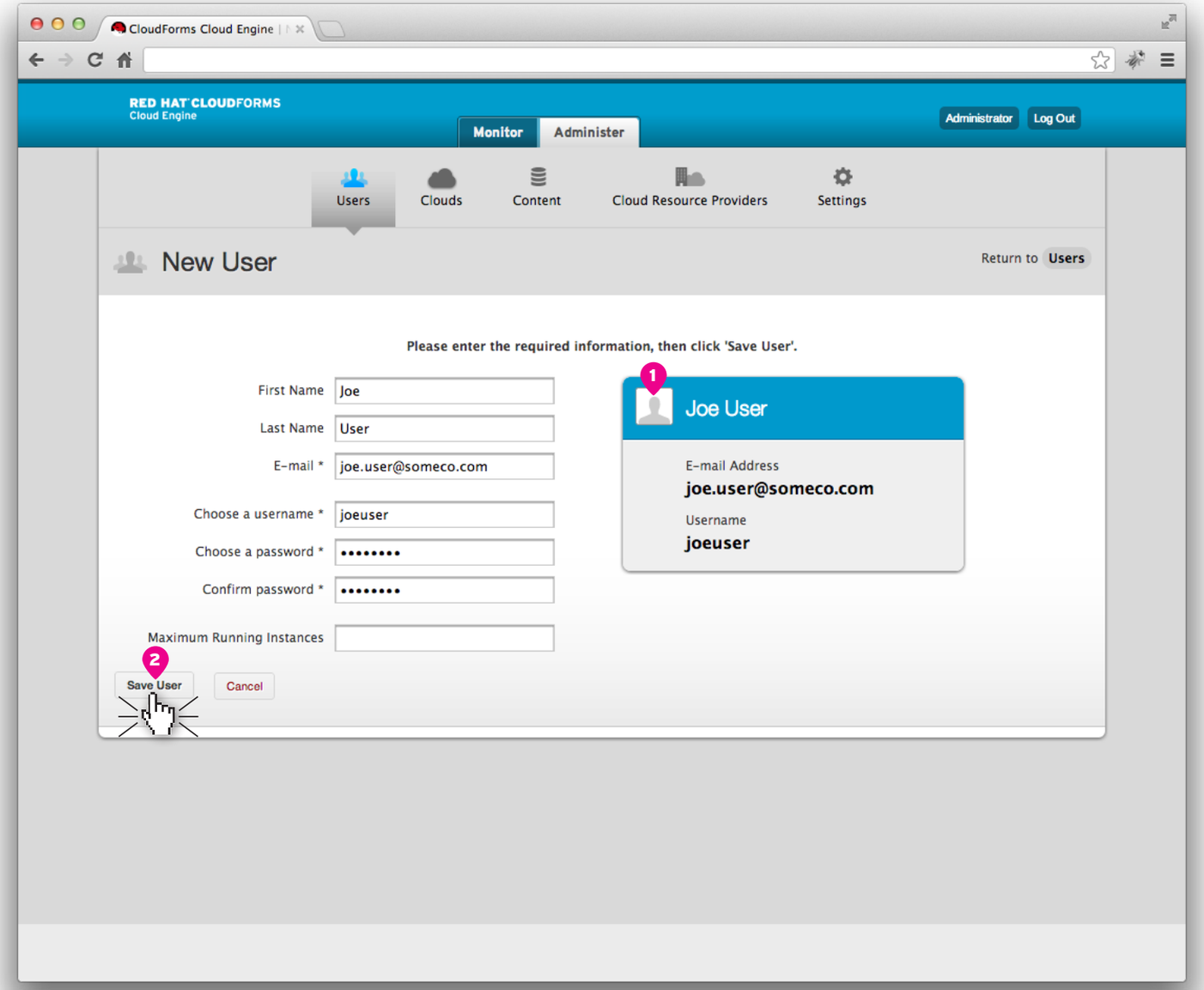
Looking at the current UX

This section is a review of user interfaces for viewing rand modifying roles and permissions in Conductor. The document identifies areas that may be confusing to users and offers suggestions for improvement in the user experience.

Areas and tasks examined

- Creating a User
- User and Group profile and working with permissions
- Role Assignments on objects
- Global Role Grants

Note: A recent build of the downstream version of the application was used for this evaluation.



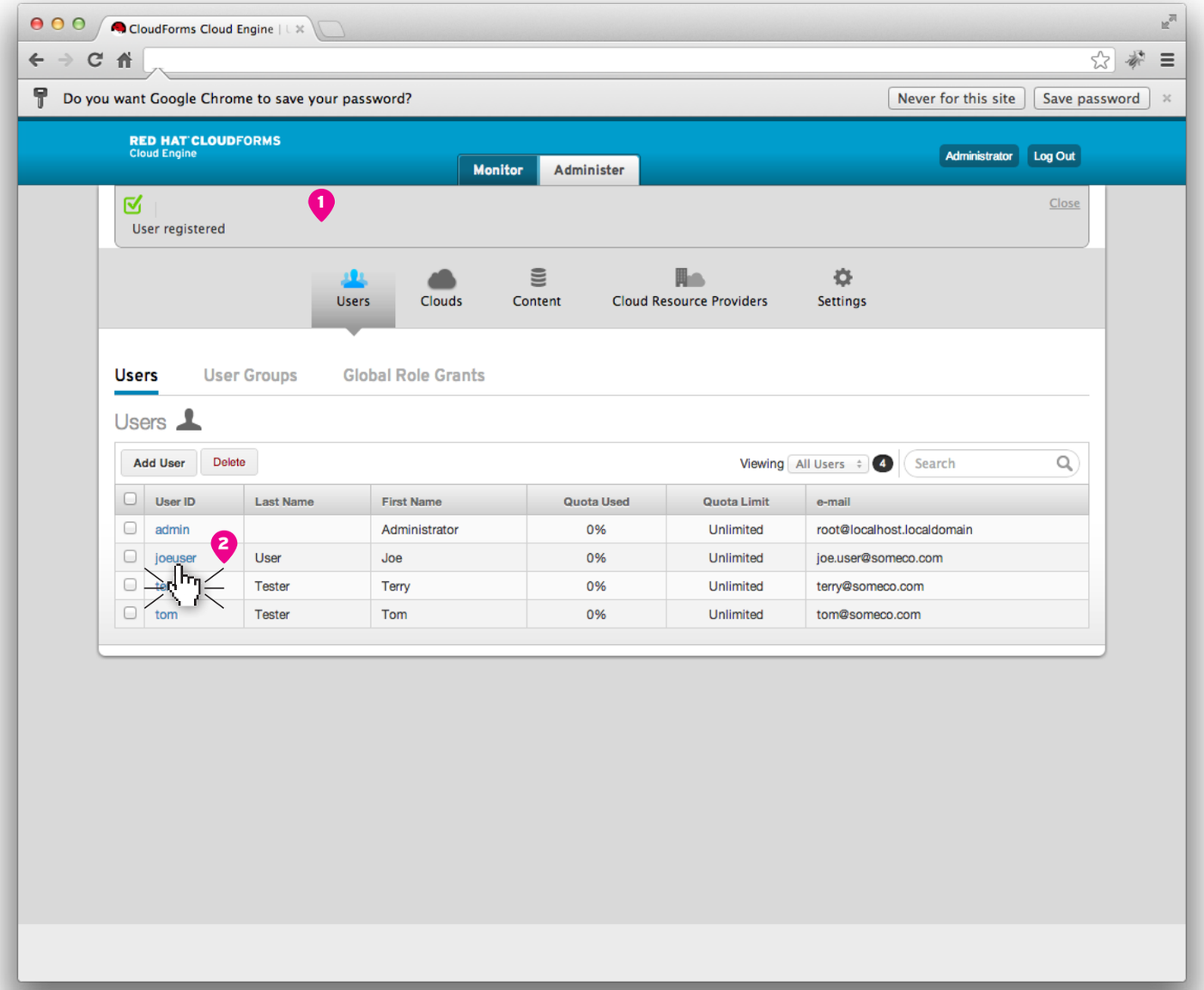
Creating a User

Suggestions:

1. The generic avatar image suggests that it can be customized. Because this invites clicks, this should either be removed, or use this image to visually indicate the users' level of access, if possible.
2. Currently this button takes you back to the list of users. There should at least be the option to continue on to adding permissions for this user. This might be an optional second step in this wizard, or simply navigating to the profile on the next screen.

Questions:

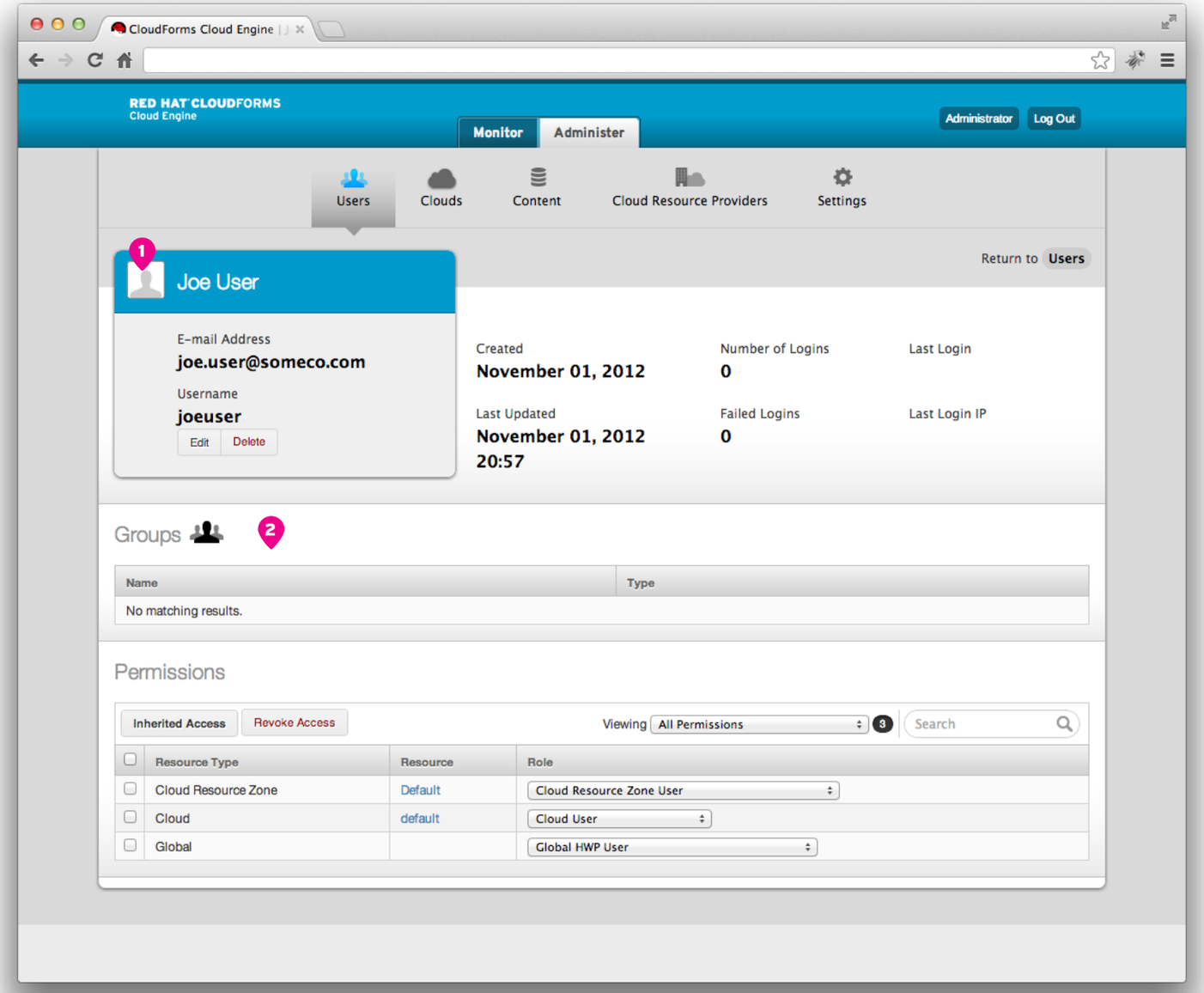
- Is there a need for a way in the GUI to create users in bulk? Perhaps by uploading a spreadsheet or via XML?



User Created Successfully

Suggestions:

1. The message displayed could be improved. What user? Maybe add a link to “Set permissions” for the new user.
2. As noted on previous page, returning to this screen is not optimal for cases when you now want to define groups and permissions for the user. If the user list is long, finding the user you just created could be tedious.



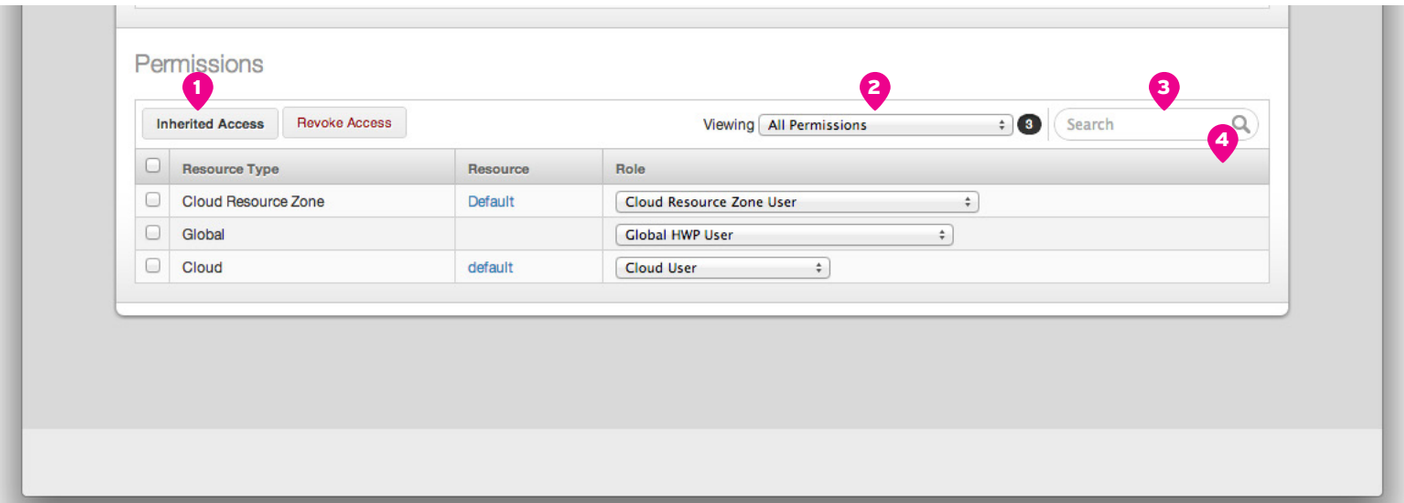
User Profile

This screenshot shows the user profile for Joe User, who has just been created by an Administrator.

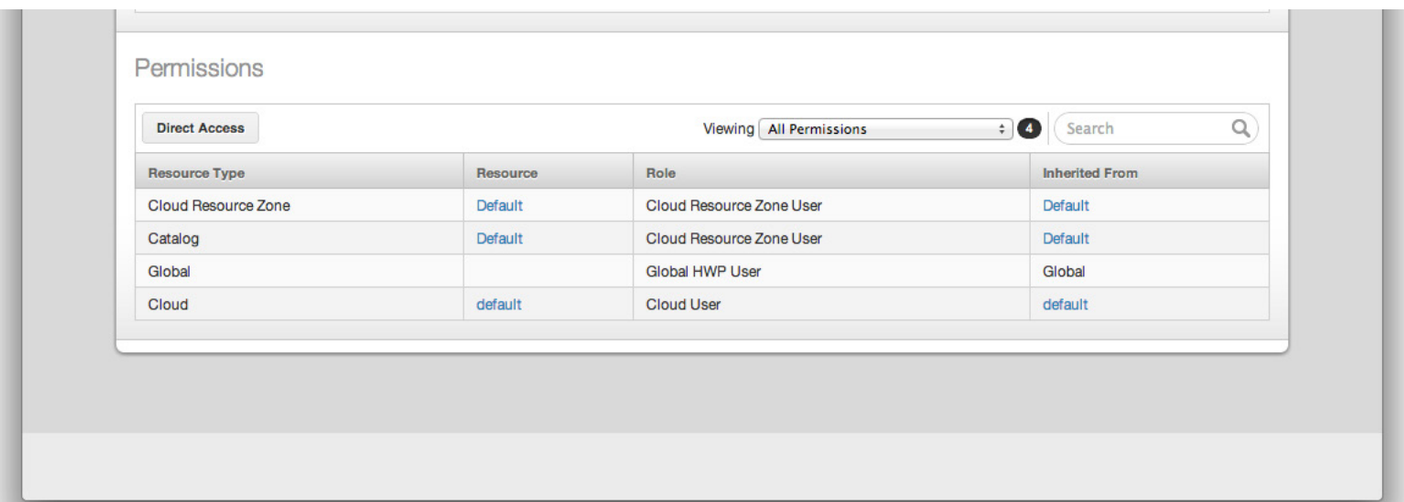
Suggestions:

1. Remove or change purpose of the avatar. Reconsider use of space in the top of the page overall.
2. Users will expect the ability to add or remove the user from a group from here. An Add button would display a screen with a list of all groups, allowing users to select 1 or more.

Direct access



Inherited access



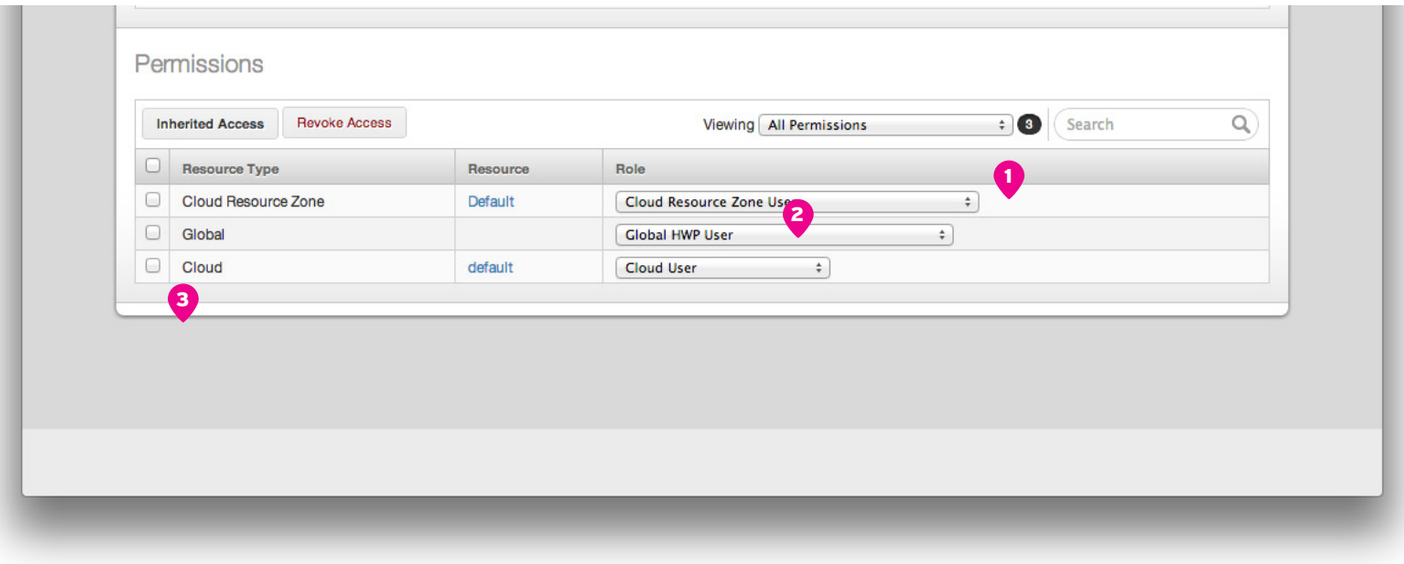
User Profile - Permissions

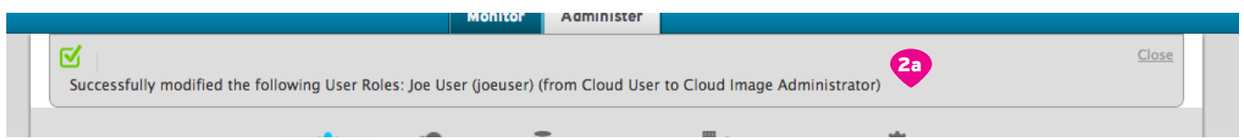
The Permissions section is easily the most complicated part of the user profile, and most in need of improvements.

Note: These observations and suggestions also apply to the Group profile page.

Suggestions:

1. Toggle for Inherited versus direct access is confusing as presented because it looks the same as an action button, and the views are not labeled to differentiate the two. It is unclear that inheritance here refers to inheritance via object hierarchy, not via group role assignments of the user.
2. Resource type filter is useful, but not as immediate as using sorting or grouping within the table view itself.
3. Search box does not seem to do anything - remove this or fix.
4. Column heads should be sortable.



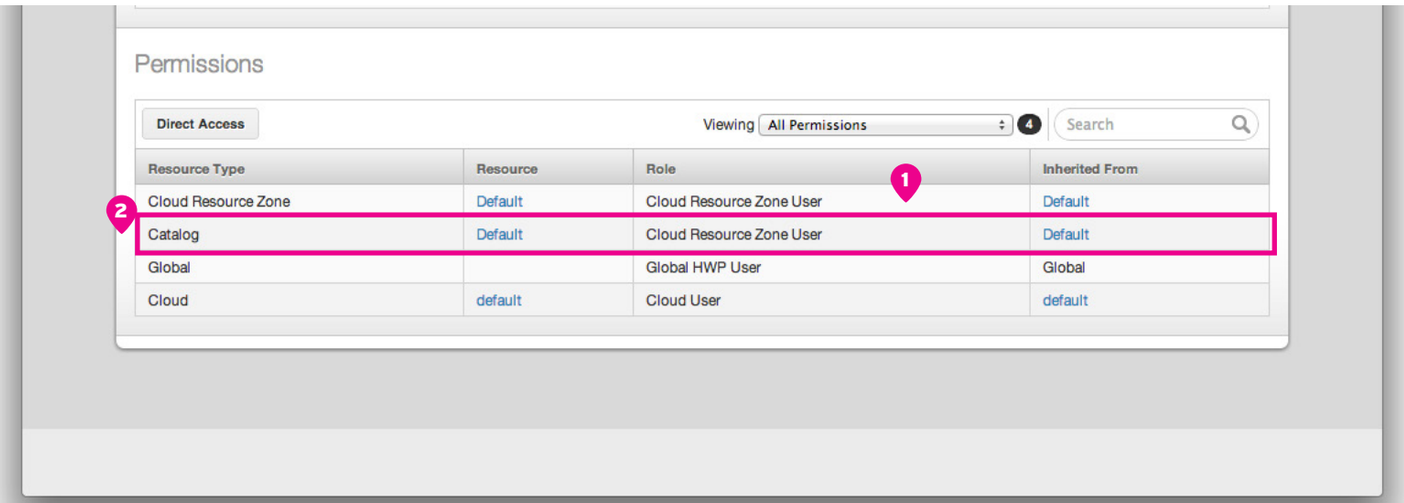


User Profile - Editing Direct Access Permissions

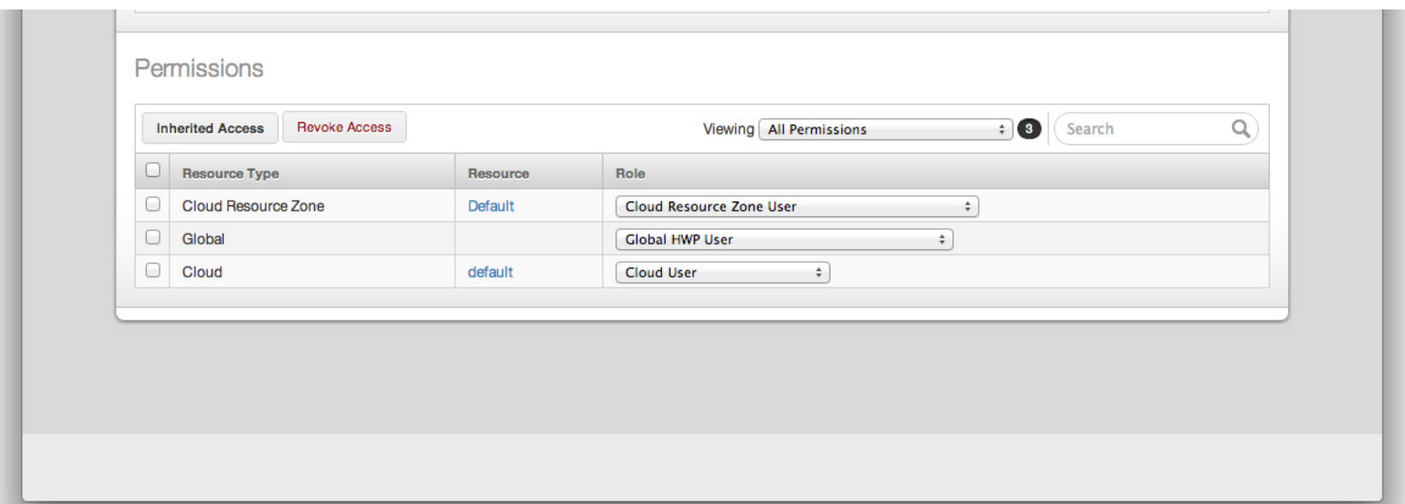
Suggestions:

1. Users need some way to read role descriptions to understand the roles, via help tip, etc. Even better, an entire guide to roles should be created and available from this page.
2. Users can easily change a Role by dropdown selection, without having to click save. Because there is some risk of making accidental changes, there should be a simple way to undo a change.
   a) This could be handled via the confirmation alert - add a link to Undo.
3. It would be useful to have a way to revert all permissions back to the "default" permissions - that is, the permissions the user would get when they are created.

Inherited access



Direct access



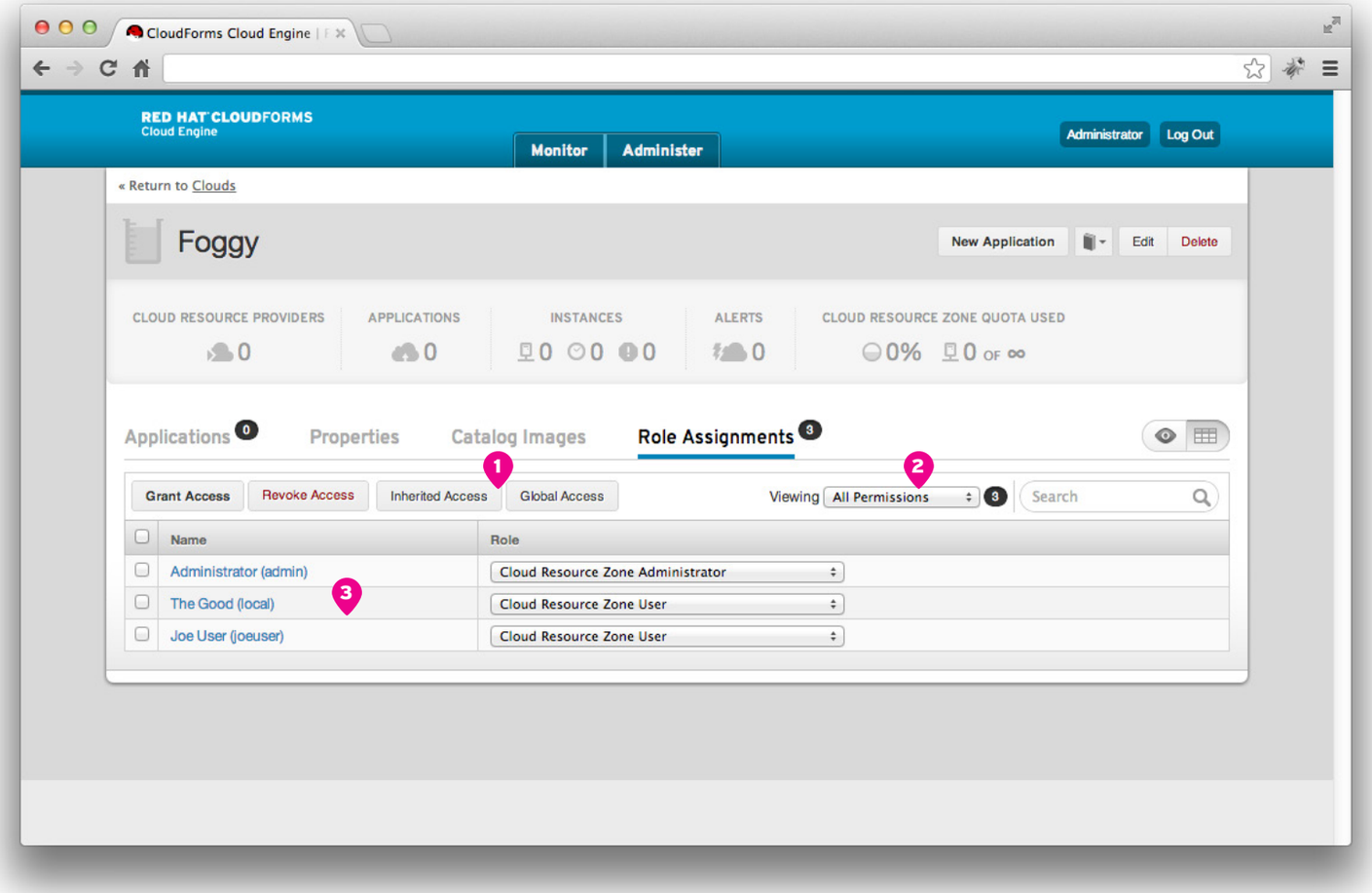
User Profile - Viewing Inherited Access

Suggestions:

1. As with direct access, users need access to role descriptions.
2. Much of the information in the Inherited view is redundant with the direct view. It would seem that only the Catalog “Default” should be seen in this view, because it is inherited from the Cloud Resource Zone “Default.” Meanwhile, the other three object to role mappings seem to show redundant self-inheritance.

Overall:

- It should be possible to consolidate the view, with perhaps a special mode to expand and also see inherited access.
- Note that because both the Cloud Resource Zone and the Catalog have the same name (“Default”), the relationship is further obscured.



Resource - Role Assignments

This screenshot shows the role assignments on a cloud named “Foggy”

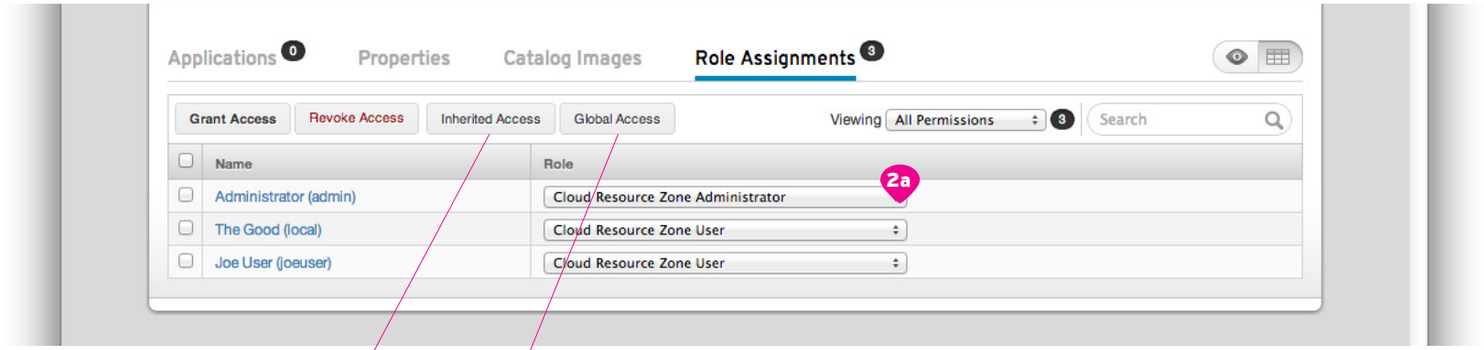
Suggestions:

1. Buttons to toggle to different views for Direct, Inherited, and Global access shouldn’t look like peers to actions like Grant Access.
2. The filter label is not obvious - in this case you can select to see only users, only groups, or “all permissions” which is users + groups.
3. Groups and Users should be better delineated in the list.

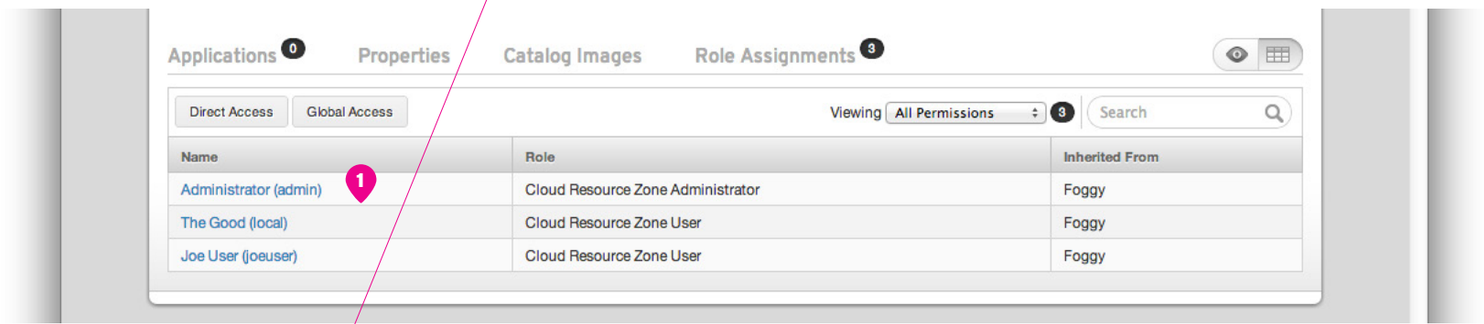
Overall:

- There is an opportunity to promote permission granting by groups, and lessen the emphasis on setting access on individual users. User grants should be a specialized case for most large installations.
- Would the view make more sense if it started with roles, then told you who had those roles?

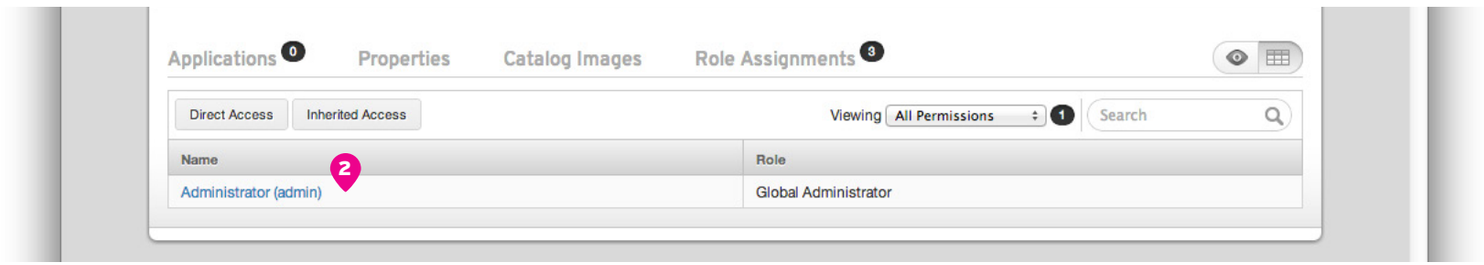
Direct access on Foggy



Inherited access on Foggy



Global access on Foggy



Resource - Types of Access

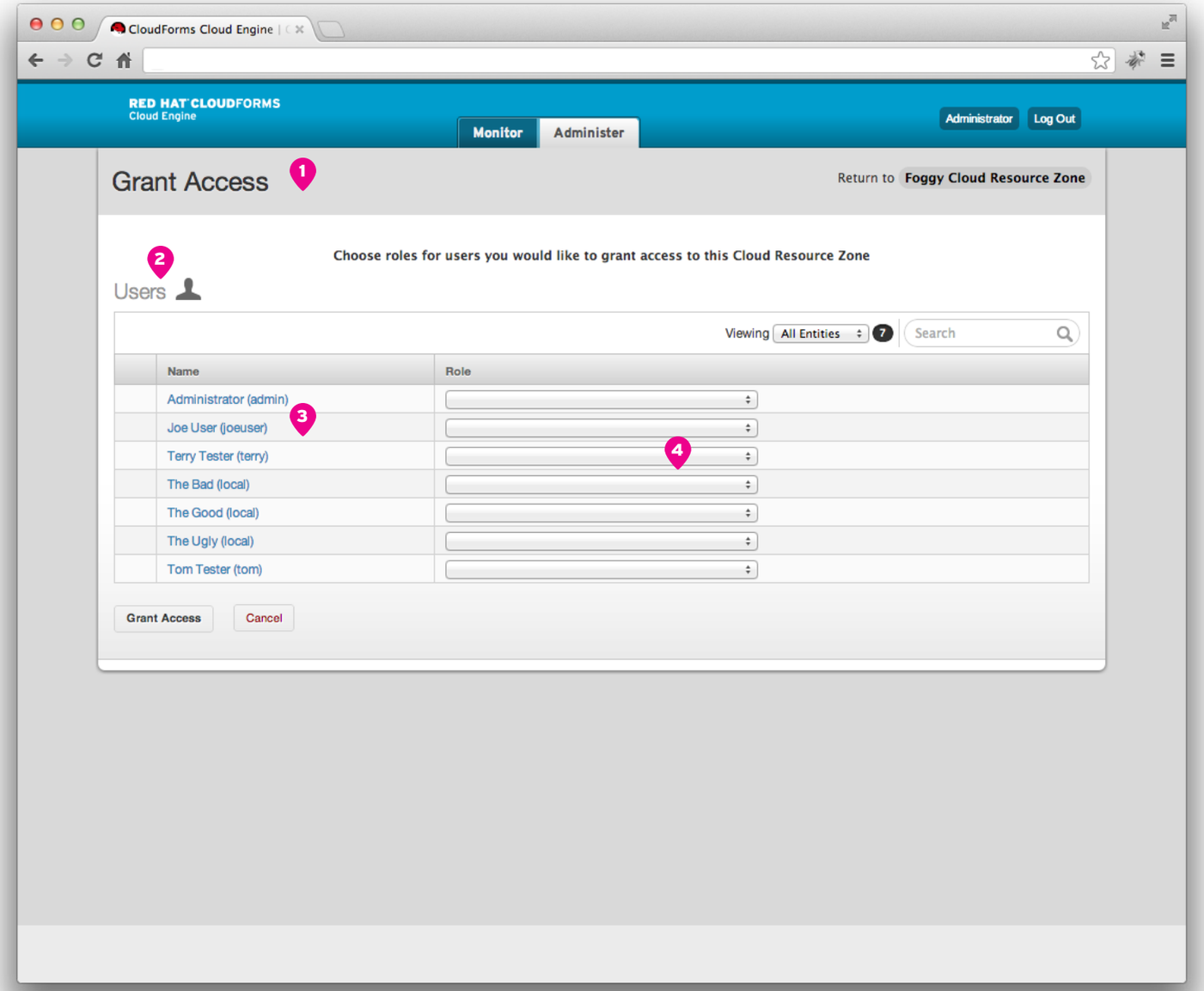
Direct, Inherited, and Global access is shown in 3 different views.

Suggestions:

1. Redundant info on inherited view is similar to the observation on User profile. Inherited relationship shown here seems recursive and not useful to the user.
2. It is unclear how the Administrator's Global access interacts with the Direct Access role, which was granted automatically when Administrator created this Cloud.
   a) Should this be editable?

Overall:

It should be possible to consolidate the view, with perhaps a special mode to expand and also see inherited and/or global access.

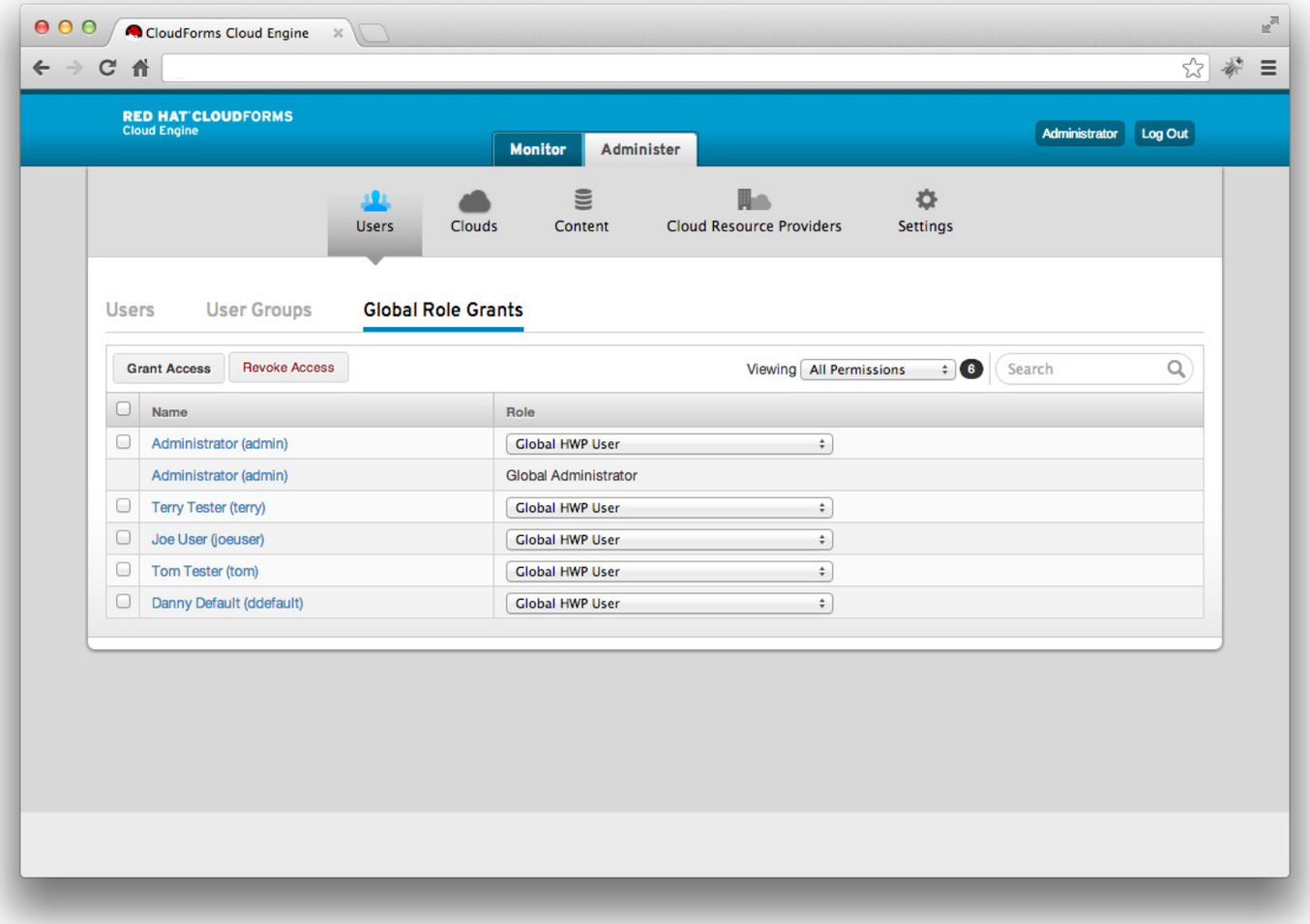


Resource - Role Assignments: Grant

When users click “Grant Access” button for a resource, this page is shown.

Suggestions:

1. Grant Access to what? Page title does not make the context clear, and breadcrumb and instruction is too subtle. Possibly this page is too much of a context shift.
2. Table heading says Users, but contains Users and Groups.
3. Since all users and all groups are shown (mixed) this list could be incredibly long. There is again an opportunity to promote permission granting by groups as the primary path, making user grants a separate case.
4. Where relevant, the role drop downs should show the current access for users and groups, not the null state.



Global Role Grants

The global role grants screen allows users to grant global roles to users and groups. This screen behaves fundamentally the same as any resource role assignments page.

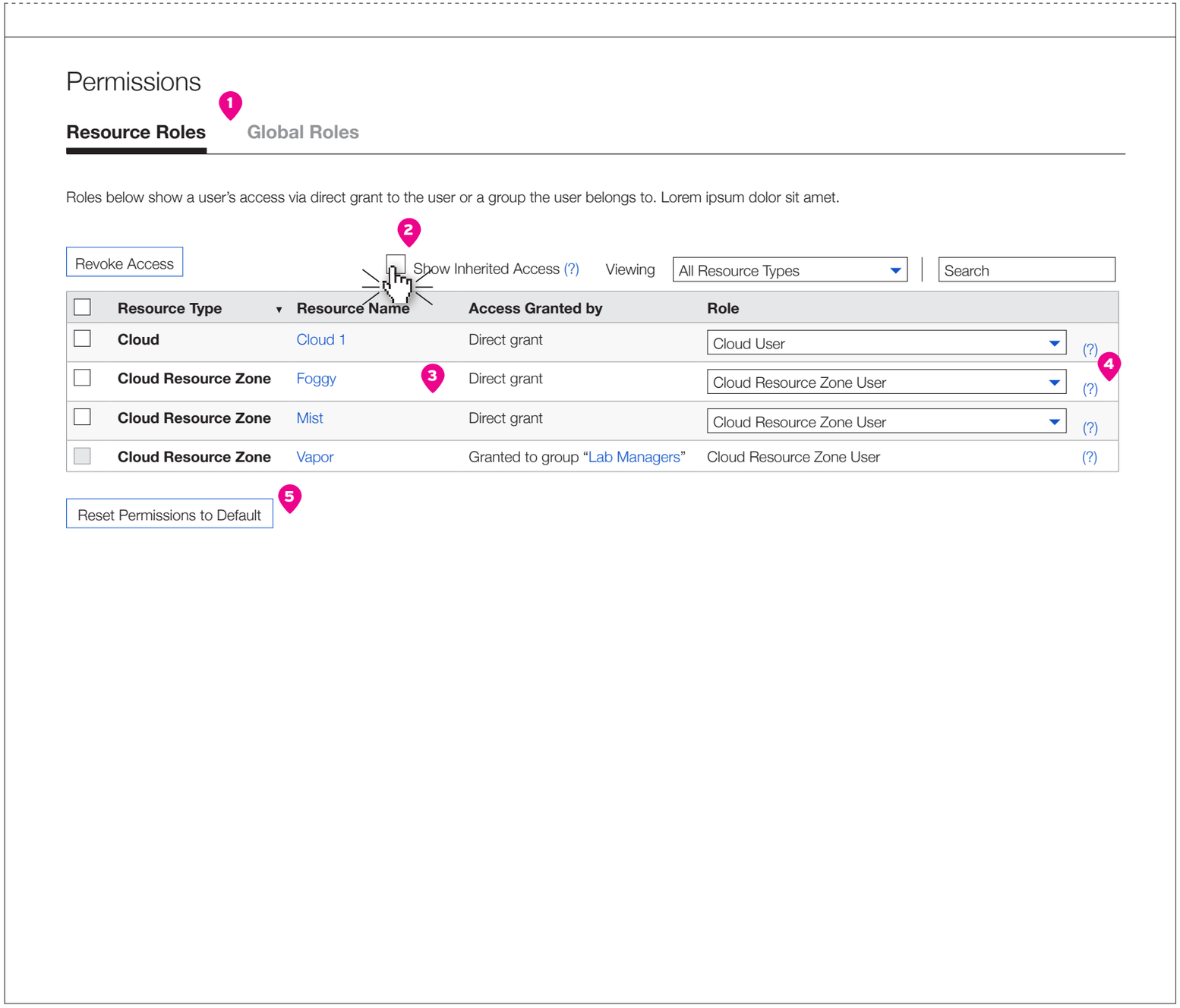
Overall:

- Global roles are useful for modeling “types” of users (e.g. Admin, Global App Blueprint Admin). The page should add more context to explain the implications of global roles and help users assemble the sets of global roles needed to model admin-class users in their organization.

Concepts

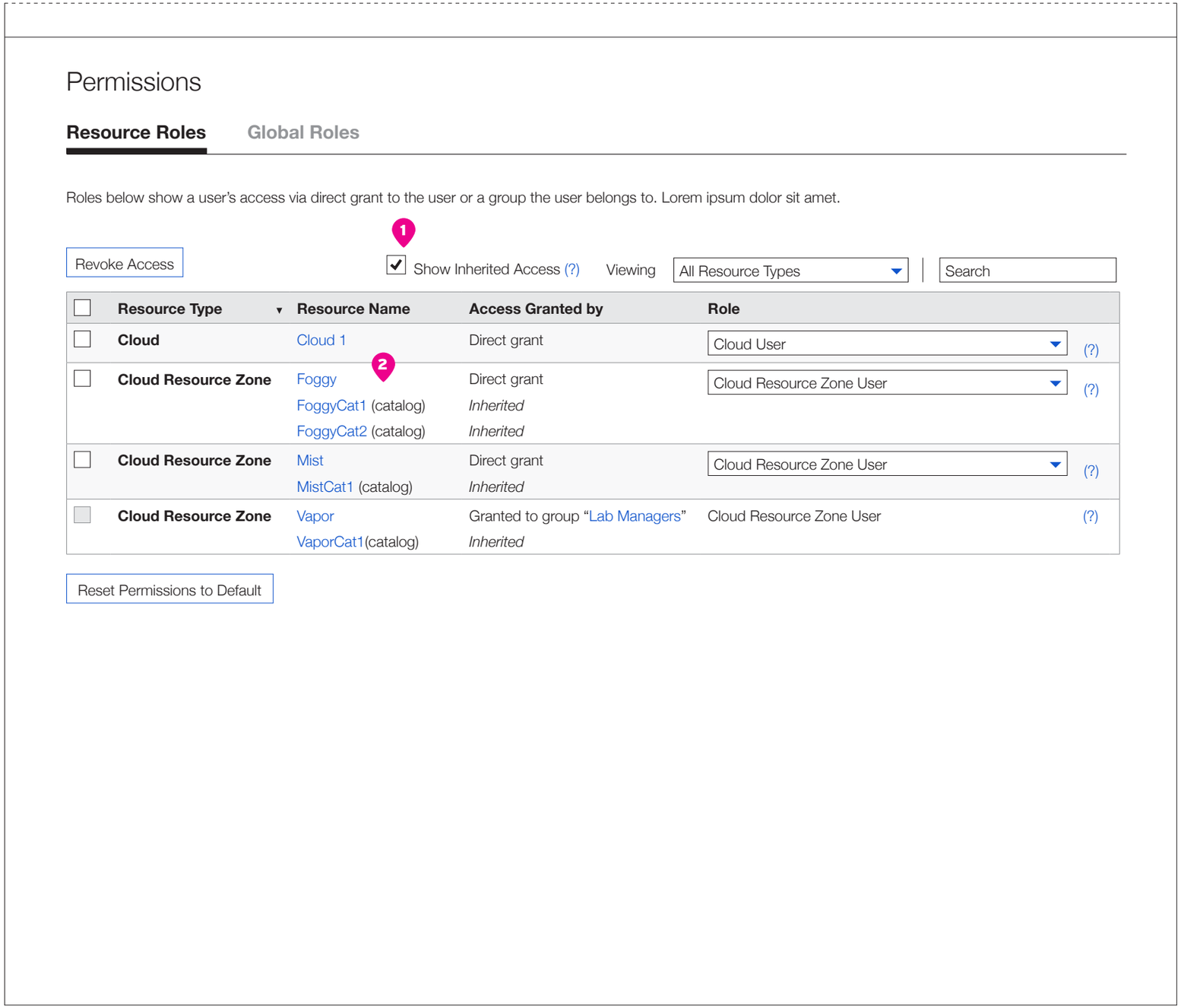
The following wireframes are an initial attempt at solving some of the usability issues noted earlier with iterative, rather than radical changes.

These are not yet a recommended design. Much more discussion and feedback is needed to develop the ideas.



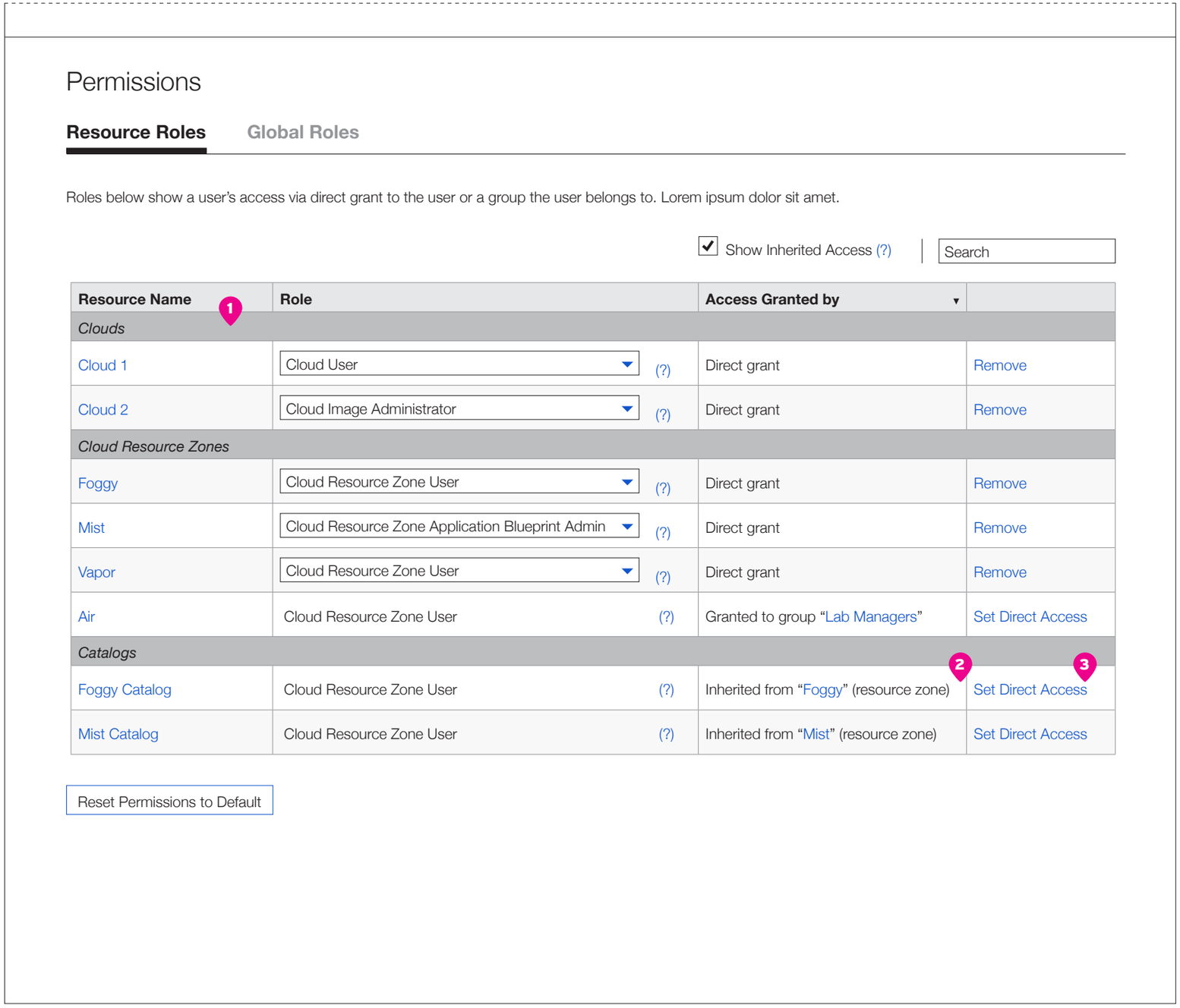
User Profile Resource Permissions concept 1

1. Permissions section is divided into tabs for resource roles and global roles.
2. Toggle to also show resources that the user can access via inheritance (see on next page)
3. Table of permissions showing resource type, name, how the access is granted (Direct vs group) and the role.
4. Click to see all role descriptions
5. Reset all directly granted permissions to the default - as if the user was just created. Note - this should not remove users from groups.



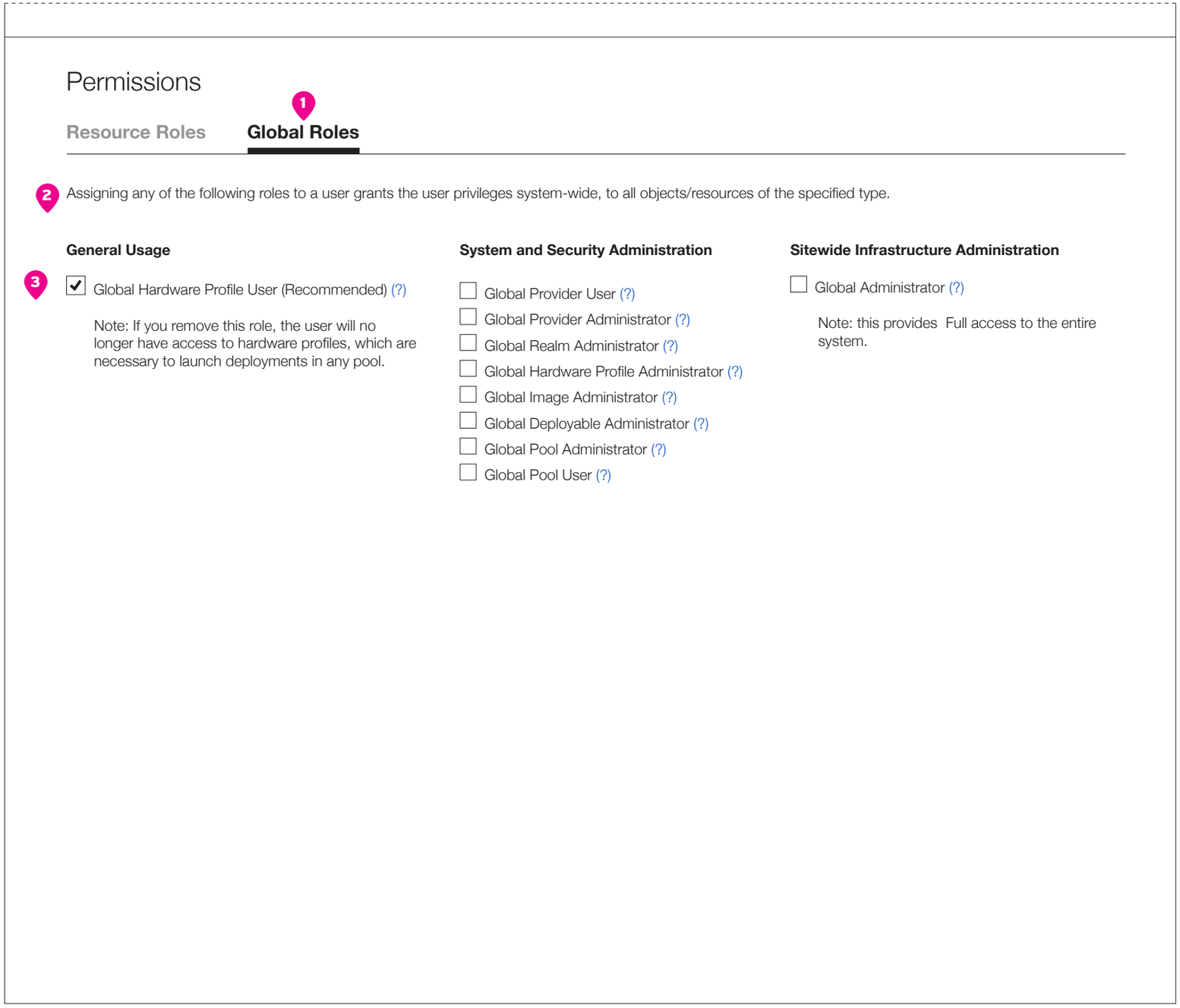
User Profile Resource Permissions concept 1

1. Showing object-inherited access adds more information to the view.
2. Those objects that have access via inheritance are shown with the parent that provides that access.



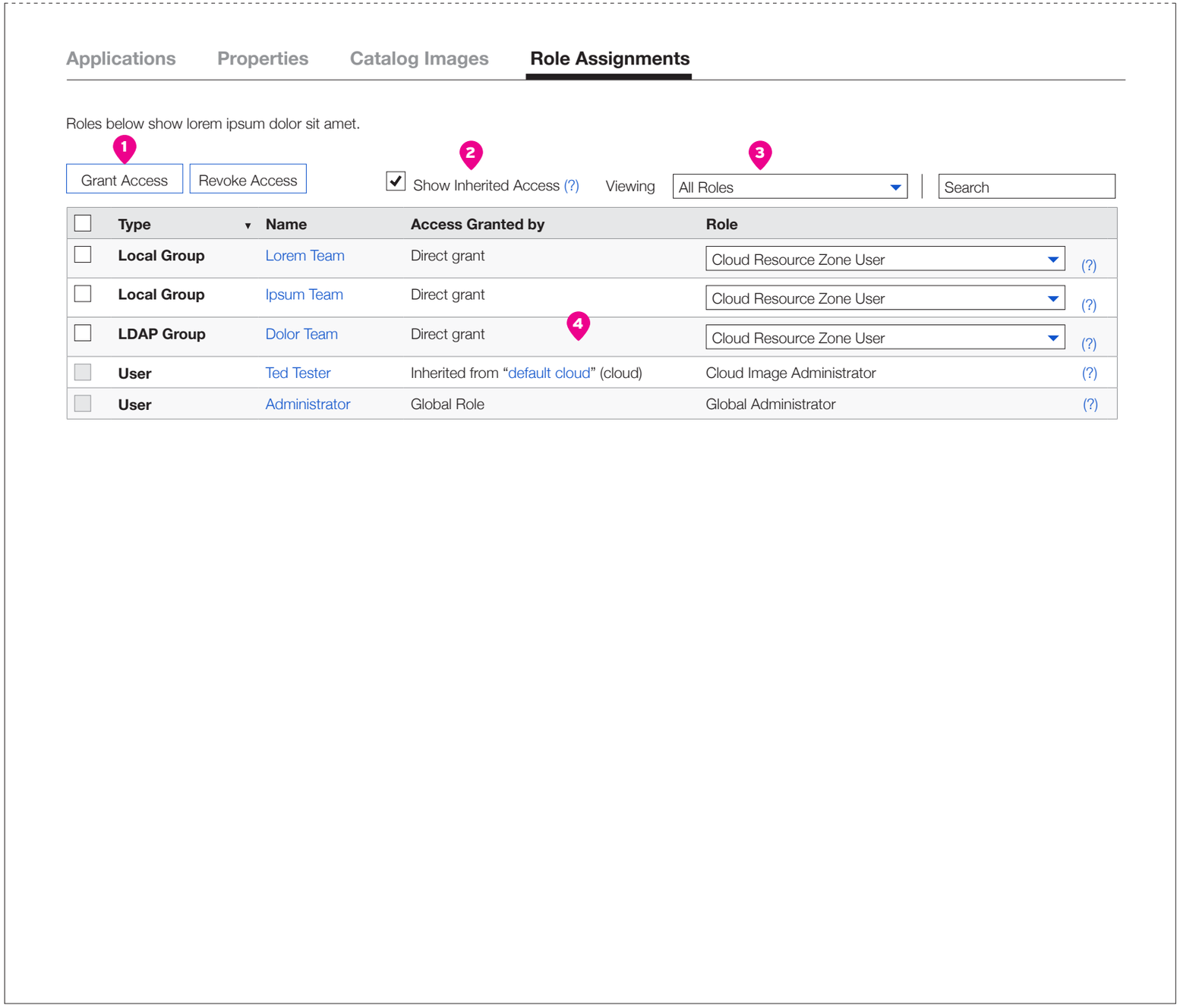
User Profile Resource Permissions concept 2

1. The table is strictly grouped by resource type, with a heading beginning each section.
2. If shown, Inheritance relationship is called out in the "Access Granted by" column
3. This concept shows an option where a user could set specific direct access that differs from the inherited access. This only makes sense when the direct access is granting more permissions, not less.



User Profile
Global Permissions

1. The Global Roles tab shows the global roles interface
2. User assistance text explains the nature of global roles.
3. Global roles can be arranged to suggest types of users (personas?) to whom the selections would apply. Additional text can explain the importance of specific global roles.



Resource Role Assignments

This idea uses a table that mirrors "concept 1" for resource permissions on a user profile.

1. Click Grant Access to see a screen that lets you select/search for groups or users.
2. Inherited access can be shown via toggle. Off by default.
3. Filter by Roles - the values in the right-most column.
4. The table is sorted so that groups are first. The center column denotes how the access is set. Only Direct access can be edited.

Closing Notes

This is just the beginning of a long conversation. Some of the suggestions here are simple, while others begin to point to much more involved changes to the model. Questions will and should continue to be asked.

Over time we should continue to understand the problem better through feedback and our own usage.

Users vs. Groups - The ability to set access on individual users as well as groups gives great flexibility, but comes at the cost of complexity. The experience could do more to encourage using groups to grant access to users. This should reduce complexity since there would, in theory, be fewer places where access would be set.

User assistance is missing throughout the interface, and in the area of permissions the pain is most acute. Screen tips, help panels, etc. are needed to help users understand terminology and role definitions.

Changes to navigation and layout patterns could have significant impact on the roles and permissions interfaces. Some of the problems noted may be solvable via system-wide changes, rather than specific moves noted in this doc.