MetacatUI - Bug #7079

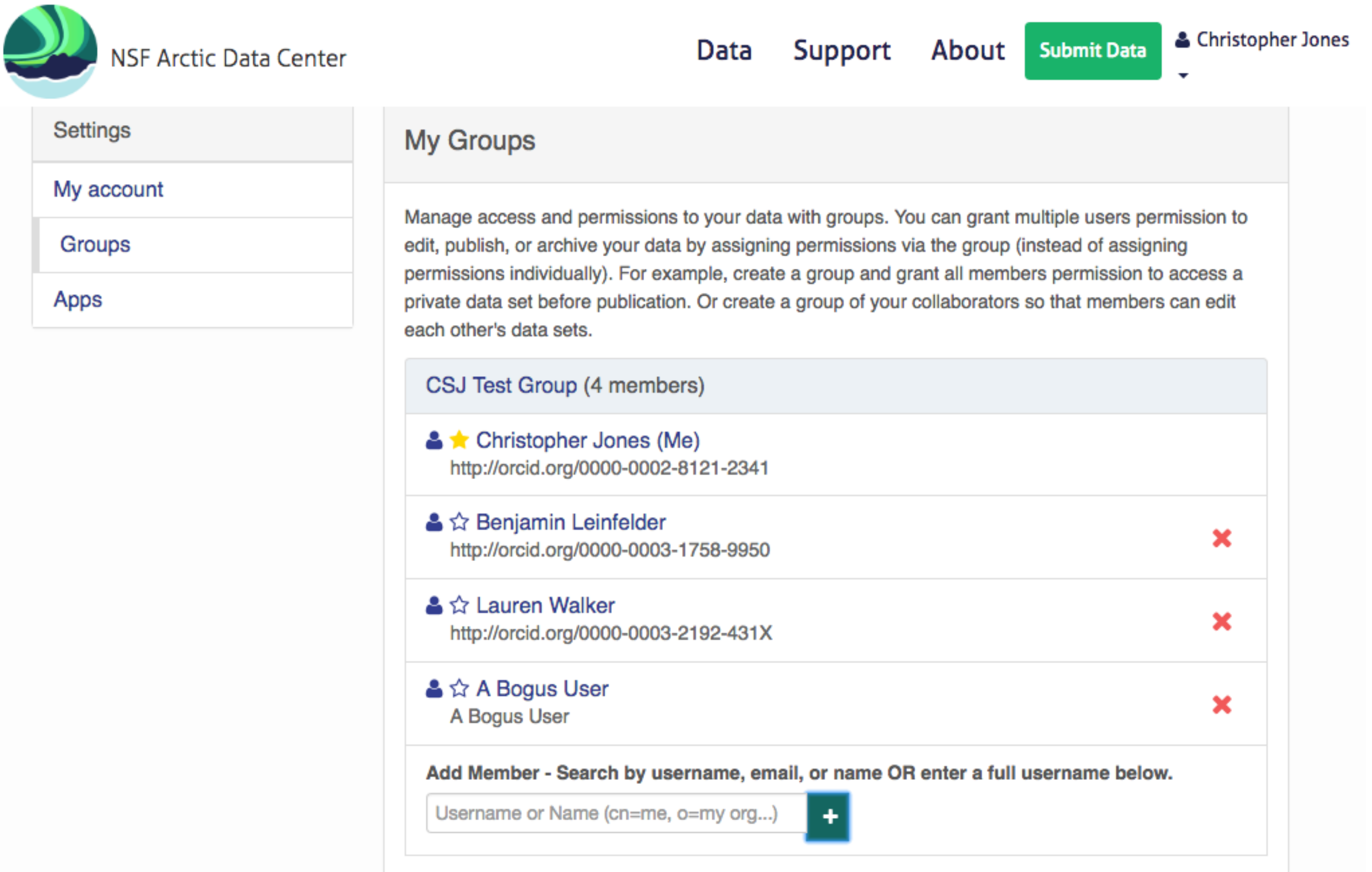
Group UI allows invalid entry causing Identity ServiceFailure

08/03/2016 11:43 AM - Chris Jones

Status:	Rejected	**Start date:**	08/03/2016
Priority:	Normal	**Due date:**	
Assignee:	Lauren Walker	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	1.12.0	**Spent time:**	0.00 hour
Bugzilla-Id:			

Description

When adding users to a Group in the MetacatUI -> My Profile -> Settings -> Groups web form, the form allows users to be added to the group that don't exist in the Accounts Registry. We need to validate the member DN prior to calling PUT /cn/v2/groups so an invalid entry doesn't get created by the CNIdentityLDAPImpl service.



My Groups

Manage access and permissions to your data with groups. You can grant multiple users permission to edit, publish, or archive your data by assigning permissions via the group (instead of assigning permissions individually). For example, create a group and grant all members permission to access a private data set before publication. Or create a group of your collaborators so that members can edit each other's data sets.

CSJ Test Group (4 members)

★ Christopher Jones (Me)
http://orcid.org/0000-0002-8121-2341

☆ Benjamin Leinfelder ✖
http://orcid.org/0000-0003-1758-9950

☆ Lauren Walker ✖
http://orcid.org/0000-0003-2192-431X

☆ A Bogus User ✖
A Bogus User

Add Member - Search by username, email, or name OR enter a full username below.

Username or Name (cn=me, o=my org...) +

Unfortunately, once a uniqueMember is is created in the group in LDAP, this causes the Accounts Registry service to throw a 500 ServiceFailure, so all other authenticated interactions with the CN fail, affecting all users. I'll add a ticket in the d1_identity_manager project to address this from the server side. See https://redmine.dataone.org/issues/7857

By removing the bogus uniqueMember entry in LDAP, the Accounts Registry service worked fine again.

History

#1 - 08/04/2016 09:53 AM - Lauren Walker

- Target version set to 1.12.0

#2 - 08/04/2016 10:04 AM - ben leinfelder

Since this actually doesn't break the account service (now) do we really need to restrict group member? Say I want to make a group of Orcid accounts but not all the the people in my group have logged in to DataONE before. They won't be in our system but I don't see why I shouldn't be able to add them.

#3 - 08/08/2016 10:28 AM - Lauren Walker

Will adding an orcid to a group cause an error? I can see it being helpful to be able to create a group of ORCIDs whether or not they are in the LDAP registry

#4 - 08/08/2016 10:35 AM - ben leinfelder

No, it should not be a problem and is exactly the kind of scenario I was imagining.

Lauren Walker wrote:

> Will adding an orcid to a group cause an error? I can see it being helpful to be able to create a group of ORCIDs whether or not they are in the LDAP registry

#5 - 08/08/2016 10:37 AM - Lauren Walker

So Chris, should the UI only allow:

- valid ORCIDs
- other usernames that are in the LDAP account registry

Anything else is rejected by the form.

#6 - 08/08/2016 10:41 AM - ben leinfelder

Why can't it allow anything that is a valid Subject format? Different MNs use lots of different identification systems. Sure, we try to have them use ORCIDs, but many don't. Maybe they will use DNs, but many don't... Point is we need to be as flexible as possible.

#7 - 08/09/2016 10:16 AM - Lauren Walker

- Status changed from New to Rejected

This was fixed in CCI 2.2.0, so the UI should allow users to enter any username since it won't cause an error

#8 - 08/09/2016 10:17 AM - Chris Jones

Agreed - it seems fine to let any Subject be added since (as Ben pointed out), the ServiceFailure bug on the CN was fixed.

Files

bogus-user-entry.png	134 KB	08/03/2016	Chris Jones