Foreman - Bug #2108

Cannot delete or rename admin user via GUI

01/05/2013 06:08 AM - Anthony Somerset

Status:	Duplicate		
Priority:	Normal		
Assignee:			
Category:	Authentication		
Target version:			
Difficulty:	easy	**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

Using the Internal user AUTH system gives the default admin user with admin / changeme as the credentials

Currently you cannot delete this user via the user interface (it gives a nice error saying you cant delete it) it would be good to allow this account to be deleted IF there is another administrator account configured, this would help people being security conscious who use the foreman user auth system on its own to help prevent brute force attacks by not giving a would be attacker half of your user credentials out of the box

ultimately it would be awesome to be able to rename or control the username of the main admin account at setup time (in a wordpress style fashion to give a reasonable example)

Although this is a Feature request really, i would consider it a security bug personally so have left it as such pending better classification by others

I should point out also that I was able to successfully remove the admin user from the database via standard mysql tools and it has had no abnormal effects so far in my limited testing

Related issues:

Related to Foreman - Feature #3272: Separate internal admin account from user...	**Closed**	**10/16/2013**

History

#1 - 01/05/2013 07:08 AM - Ohad Levy

- Assignee deleted (Ohad Levy)

Sadly removing it is not a real option (we relay on the fact the user always exists)

We could consider

1. disable / lock the account
2. change our default admin user assumption to an internal locked account, this might be better long term for auditing where you could see which actions were triggered by a user and others by an event (e.g. fact import)

#2 - 01/05/2013 11:47 AM - Anthony Somerset

Disabling or locking does seem a sensible option - i did notice on my install that the account did just get recreated anyway

what is it actually needed for if login is enabled? (or more precisely what would break by not having the account)

i'm trying to write a patch to at least allow it to be renamed and assume it will always have ID 1 and use the ID for the search rather than the name to at least allow security conscious people to rename the account

#3 - 01/05/2013 12:37 PM - Ohad Levy

I think it would be probably best to add a locked attribute (or status that can handle multiple status - admin / locked / ..?)

and then simply add to the authentication method another check to ensure the account is not locked.

the admin account is always recreated, so I'm not sure relaying on the user id is the right way forward.

#4 - 02/27/2014 06:50 PM - Benjamin Papillon

- Related to Feature #3272: Separate internal admin account from user admin accounts added

#5 - 05/13/2014 02:34 PM - Dominic Cleal

- Description updated

- Status changed from New to Duplicate

Closing, as we're tackling this via #3272. The suggested patch uses an internal-only account where necessary, but then allows the interactive admin account to be replaced, deleted, renamed etc.