

pfSense - Bug #9259

User with "Deny Config Write" privilege is not fully prevented from creating accounts

01/07/2019 04:24 AM - Stefan Beckers

Status:	Feedback	Start date:	01/07/2019
Priority:	Normal	Due date:	
Assignee:	Jim Pingle	% Done:	100%
Category:	User Manager / Privileges	Estimated time:	0.00 hour
Target version:	2.5.0		
Affected Version:	2.3.4_1	Affected Architecture:	All

Description

I do log into the web GUI as a user "myuser" with admin group membership (other than the builtin admin/root). I used to be able to add a user to the system.

Now the creation of a new user fails and

- the console gives me hostname php-fpm[12038]: Save config permission denied by the 'User - Config: Deny Config Write' permission for user 'myuser@192.168.1.1 (Local Database)'.
- The user is invisible in the GUI
- The user was created in /etc/passwd and the rest of the system

I have not altered the "admin" group and "myuser" is member in the admin group. We do have other groups with restrictions, which do not apply to the user "myuser", used above.

Interestingly the next try on the GUI fails, stating in the GUI "That username is reserved by the system." Reason: the new user was created on system level but stays invisible in the web GUI.

How to resolve this:

- Clean up the system from your last try
 - rmuser
- log in as builtin "admin" user on web GUI
- create user as usual

Associated revisions

Revision acd7e560 - 08/27/2019 12:19 PM - Jim Pingle

User & Group Manager: Improve Deny Config Write Handling. Fixes #9259

- Denies all changes if a user has the Deny Config Write privilege. Previously it only denied the config write but some OS operations were performed.
- Sets an input error so the user is notified that their attempt failed.
- Hides the add and delete buttons so read only users don't see the option to perform those actions (but are still denied if they submit the form through other means)

Revision 585bbbd3 - 08/27/2019 12:21 PM - Jim Pingle

User & Group Manager: Improve Deny Config Write Handling. Fixes #9259

- Denies all changes if a user has the Deny Config Write privilege. Previously it only denied the config write but some OS operations were performed.

- Sets an input error so the user is notified that their attempt failed.
- Hides the add and delete buttons so read only users don't see the option to perform those actions (but are still denied if they submit the form through other means)

(cherry picked from commit acd7e5601ac6bc8b079bd6ea7f8b637a5ec89b5f)

History

#1 - 01/07/2019 08:17 AM - Jim Pingle

- Subject changed from *Creating a new user on Backend local Database fails halfway, when done with account other than builtin "admin" to User with "Deny Config Write" privilege is not fully prevented from creating accounts*

- Assignee changed from Renato Botelho to Jim Pingle

- Target version set to 48

- Affected Architecture set to All

You must have incorrectly added the "User - Config: Deny Config Write" privilege to your admin group, which is common when unnecessarily using "select all" on the privilege list without considering the consequences.

There is still a bug here, but it did deny the config.xml change as expected. Since that was not technically a config.xml change, the privilege did what it was told to do and blocked only the config.xml change. It should probably also block the shell account portion from being added.

#2 - 01/07/2019 11:04 AM - Stefan Beckers

That is not the case. I just have tried another system, where this issue does not show. My latest install does behave well.

At least on all three systems, I have compared yet, the "custom" admin users do have

- admins WebCfg - All pages Allow access to all pages (admin privilege)

the "admin" user does have:

- admins WebCfg - All pages Allow access to all pages (admin privilege)
- User - System: Shell account access Indicates whether the user is able to login for example via SSH. (admin privilege)

and the admin group only has

- "WebCfg - All pages Allow access to all pages (admin privilege)"

assigned.

It is not like that only older systems which have undergone multiple Updates and Upgrades and lots of configuration changes. It seems to be showing only on some systems. Others do behave well.

Any additional information I can compile for you here?

#3 - 01/07/2019 11:28 AM - Jim Pingle

The only way you can see that "Deny Config Write" message is if your user, or a group they are in, has the "Deny Config Write" privilege. That is 100% a configuration error and not the bug you are seeing here.

The other systems work because you don't have "Deny Config Write" in those privilege lists.

If you need more explanation, post on the forum.

#4 - 03/12/2019 10:55 AM - Jim Pingle

- *Target version changed from 48 to 2.5.0*

#5 - 08/27/2019 12:30 PM - Jim Pingle

- *Status changed from New to Feedback*

- *% Done changed from 0 to 100*

Applied in changeset [acd7e5601ac6bc8b079bd6ea7f8b637a5ec89b5f](#).