Foreman - Bug #30413

Adding more than 600+ roles to non-admin user causes 500 error and Ruby stacktrace

07/15/2020 11:35 AM - Will Foster

Status:	New		
Priority:	Normal		
Assignee:			
Category:			
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:	No	**Found in Releases:**	1.19.1, 1.23.0
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

Hello Foreman team,

We've discovered what looks like a RBAC scalability bug where if you associate more than 600+ roles to a non-admin user it breaks their UI and hammer CLI and returns 500 errors.

We've been able to reproduce this on both 1.19.1 and 1.23.0.

This is what our process looks like (we manage large-scale R&D scale/performance environments in engineering via QUADS - https://quads.dev/)

1) associate one role per bare-metal system (named either via FQDN or short hostname)

hammer role create --name host01.example.com

2) associate one filter for that role with permissions

hammer filter create --role host01.example.com --search "name = host01.example.com" --permissions view_hosts,edit_hosts,build_hosts,power_hosts,console_hosts --role-id $(hammer role info --name host01.example.com | egrep ^Id: | awk '{ print $NF }')

3) add a non-admin user

hammer user create --login cloud01 --password password --mail quads@example.com --auth-source-id 1

4) add that role to the new user.

5) Do this 635+ times for 635+ hosts or more.

- Up until 500+ you can still get the return of hammer host list -u cloud01 -p mypassword
- After 500-600 roles you only get 500's for that user only.

We have since moved to using system ownership in lieu of 1 x role per bare-metal system, however we think this is a scalability bug and it can be easily recreated by creating a non-admin user, creating 600+ roles with filters, then associating those roles to that user and trying to login to the UI or run any hammer host commands.

History

#1 - 07/15/2020 12:19 PM - Will Foster

On a related note, tbrisker on #theforeman / Freenode suggested that we switch to system-ownership based views so we've made appropriate adjustments to our project codebase to use this instead:

https://review.gerrithub.io/c/redhat-performance/quads/+/498032
https://github.com/redhat-performance/quads/commit/f2f6643884c68d044c3f7e1eab908c175edda194

However, we still feel that we're not "holding it wrong" (Apple iphone 4 antenna bug gaffe) and there can still be valid use cases that folks might need more than 600+ roles associated with a non-admin user so hence filing this.

Files

foreman_rbac_roles_bug.txt	908 KB	07/15/2020	Will Foster