# Role-based Privilege Management

The APV appliance authorizes authenticated users with resources based on the qualifications of user roles. User roles allow more flexible, accurate and fine-grained user identification. Administrators can define one or multiple qualification rules for each user role, and each qualification rule can contain at most 32 conditions. Supported conditions include login time, user name, group name, source IP address and the used AAA methods etc.

Commands to create Role-based Privilege Management:

**role name** <*role_name*>
This command is used to define a role. The system allows up to 32 roles.

**role permit** <*role_name*> <*filter_string*>
This command is used to configure a “Permit” privilege rule for the specified role. The system allows up to 256 privilege rules per role.

**role deny** <*role_name*> <*filter_string*>

This command is used to configure a “Deny” privilege rule for the specified role. The system allows up to 256 privilege rules per role.

**user** <*user_name*> <*password*> *[level]*

This command is used to create an administrator account and set its password and privilege level.

**Note: For an existing administrator account, to modify its privilege level, you need to delete it and then recreate one.**

**role user** <*user_name*> <*role_name*>
This command is used to assign a specific role to a given administrator, to grant the privileges (configured using the “**role deny**” and “**role permit**” commands) of the specific role to the administrator. One administrator can be assigned up to 8 roles.

**Note:**

If an administrator is not assigned any role, the administrator has the privilege to execute all the commands of his access control level.

If any role assigned to an administrator permits the execution of a command, then the administrator can execute this command; if all roles assigned to an administrator deny (or none of the roles permits) the execution of a command, the administrator cannot execute this command.

**On the WebUI, after defining a role for an administrator account, the administrator must configure a “Permit” privilege rule to allow this role to perform “show…” commands. Otherwise, this administrator account might encounter “500 internal error”.**

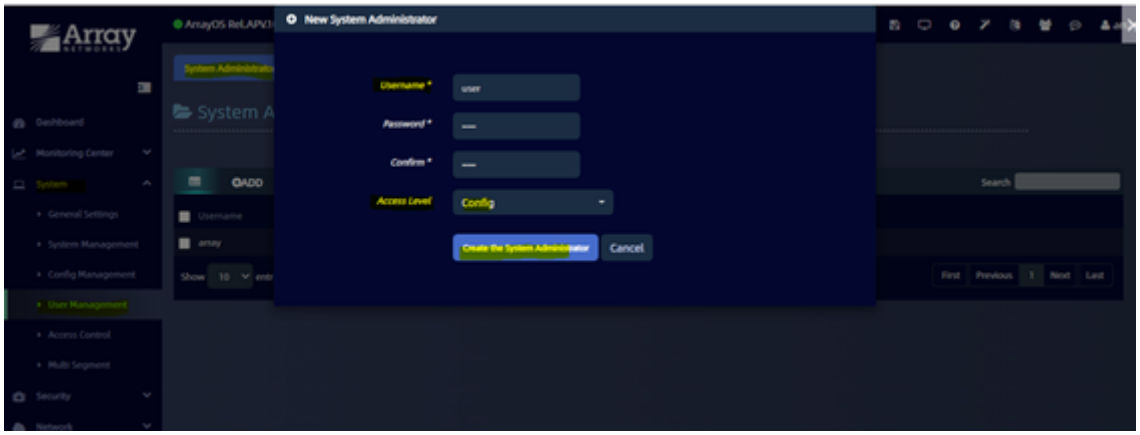
Example: -
**Requirement:**
Customer want to allow only SLB (virtual service, real server and group) configuration permission to user1 on WEBUI, but should not have permission to do other configuration than SLB.

PFB example CLI commands to create above requirement:
#role name "Test_SLB"
#role permit "Test_SLB" "show"
#role permit "Test_SLB" "slb"
#user "user1" "XXXXXXXXX$6$v7jn.taEX22eDaB4$sH.Xn.L5LEFKs12DvWm2vzI2wVAnY50dSCXY/6inF28koYaak9GgPMj.Et3BemNCmA7XPHKjPPCFy3yXz3hhU." "config"
#role user "user1" "Test_SLB"
#wr me

**Steps to configure via Webui:**

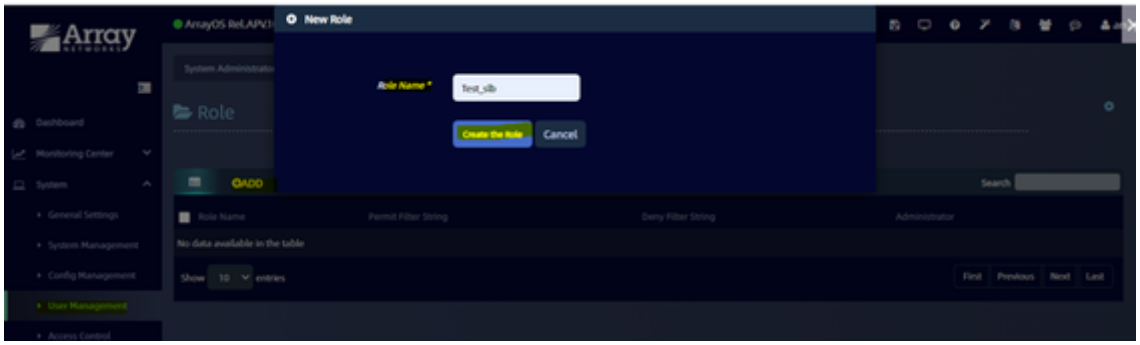
1. Create new user for testing username “user1”

Login to Webui  System  User management  Add àProvide required details PFB screen shot.



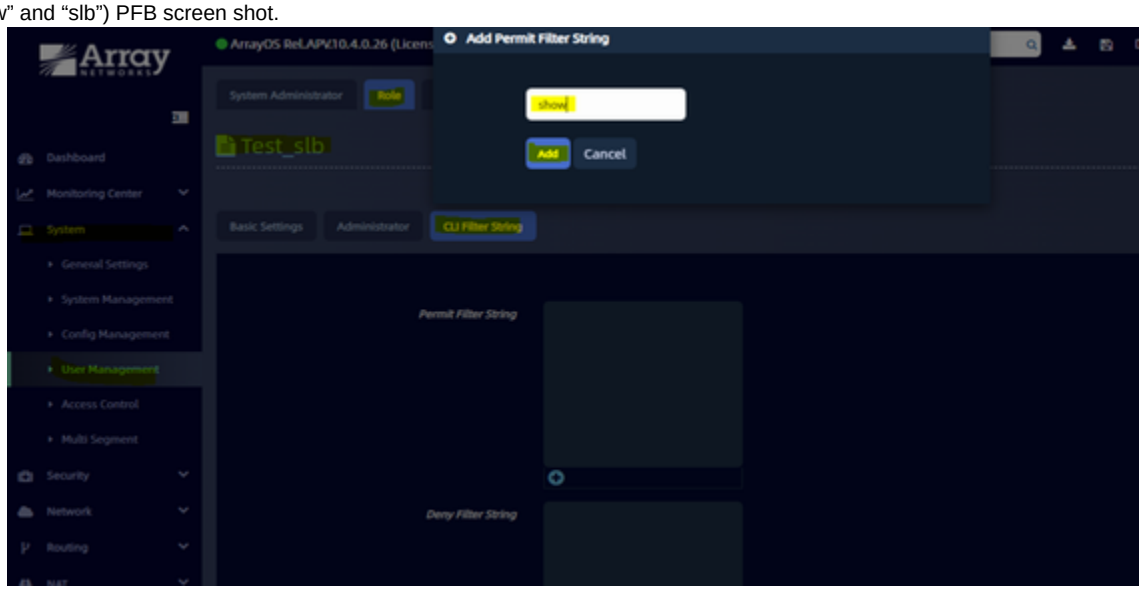

2. Create Role name

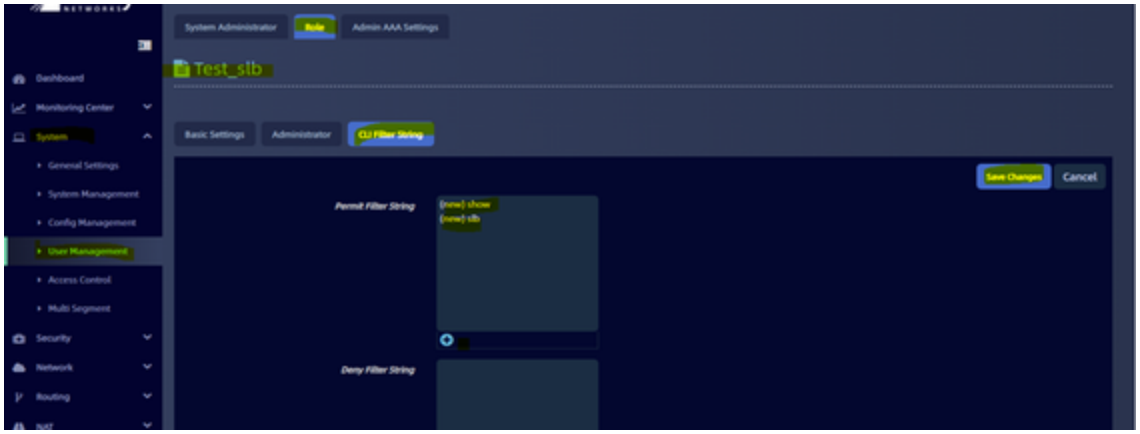
Login to Webui  System  User management  Role  Provide role name ”Test_slb” PFB screen shot.



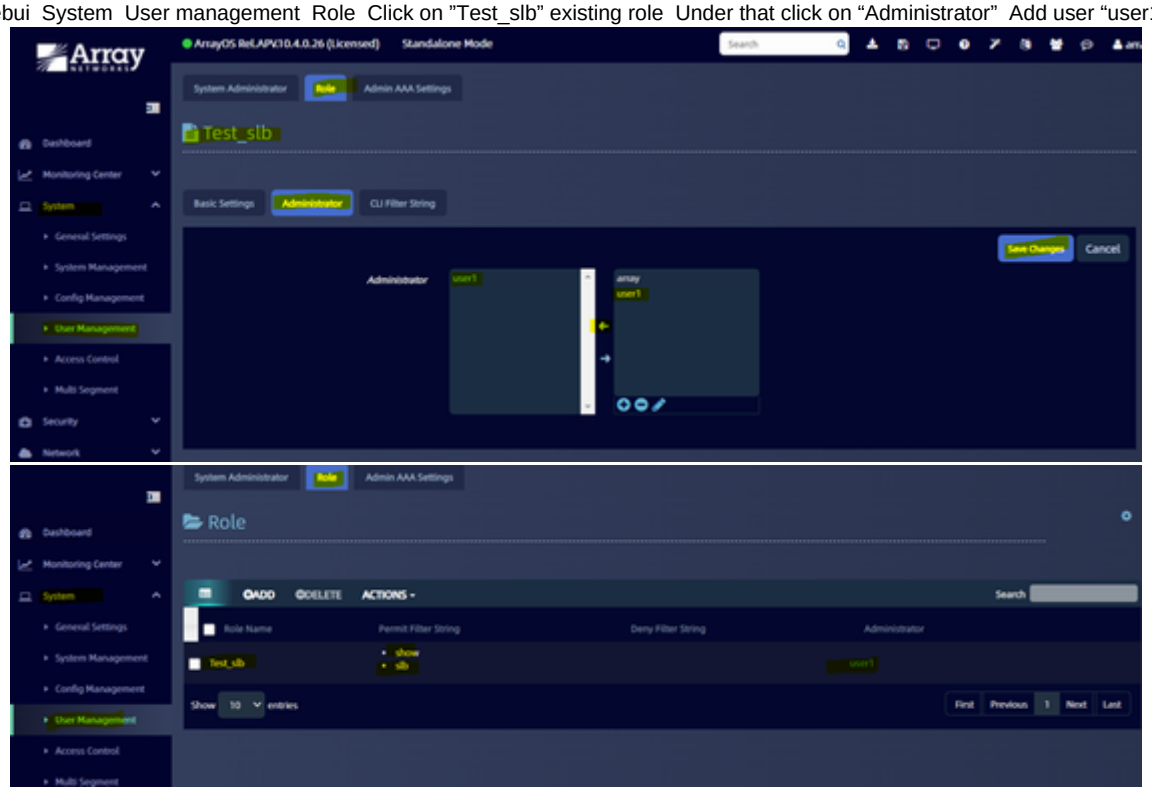

3.Conifgure “Permit” privilege to existing role name. “show” and “slb”

Login to Webui  System  User management  Role  click on ”Test_slb” existing role  Under that click on “CLI Filer String” and add permit filter string (“show” and “slb”) PFB screen shot.

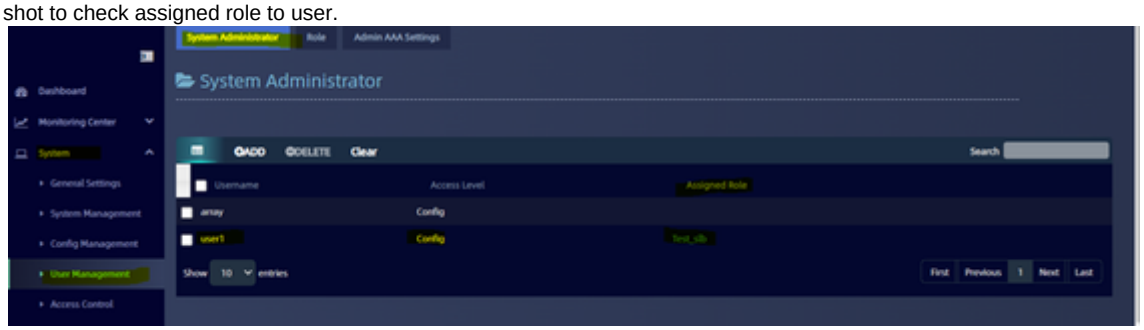





4.Add user to specific role “Test_slb”
Login to Webui  System  User management  Role  Click on ”Test_slb” existing role  Under that click on “Administrator”  Add user “user1”.



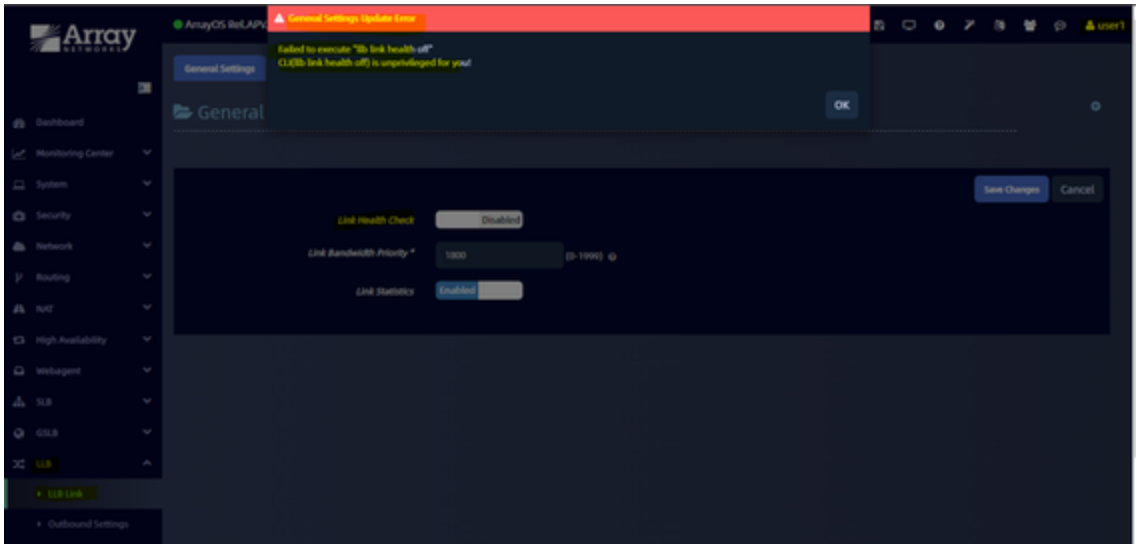

PFB screen shot to check assigned role to user.




**Test result of created user “user1”:**

Login to webui using username “user1” and password then try to configure other than SLB configuration, it should not work and if we tried will through an error.

PFB screen shot for reference, we tried to do some configuration on LLB part, its denied and throwing an error, because we have permitted only SLB.


General Settings Update Error
Failed to execute "lb link health off"
CLI(lb link health off) is unprivileged for you!
OK
General Settings
General
Save Changes
Cancel
Link Health Check
Disabled
Link Bandwidth Priority *
1000
(0-1999)
Link Statistics
Enabled
user1