Central Script to run command on multiple gateway added to MDS or Management

SCENARIO 1

Customer requirement: For audit of check point firewall customer's information security team is using qualys tool . Qualys do a ssh to firewall and execute some linux command to grep the output . qualys needs a bash shell access .

Challenge: Operation team does not wants to give bash shell access as qualys can run disruptive command like shutdown or they just want to restrict bash shell access to certain command

Workaround: Put those command in to a file on gateway and add it on clish using extended command .Create a new RO user and give it access to extended command

Customer accepted the solution but was not agree to do this change manually and wanted to do it via automation script.

Provided solution:

Solution is based on **sk85621** and **sk101047**

STEP 1 : Following the sk85621 collect all the IP of gateway to text file in this case **gateway_ip_list.txt** or manually put the IP address of all the gateway to a file called **gateway_ip_list.txt**

```
[Expert@Management:0]# pwd
/home/admin
[Expert@Management:0]# ls
copy.sh  gateway_ip_list.txt  qualys
[Expert@Management:0]# cat gateway_ip_list.txt
10.1.1.101
10.1.1.104
```

STEP 2 : add qualys command to a file and change its permission and rename as **.sh**, you can have one file for one command or one file for all command . In this example I am using two commands q1 and q2.

```
[Expert@Management:0]# pwd
/home/admin/qualys
[Expert@Management:0]# ls
```


q1.sh q2.sh

```
[Expert@Management:0]# cat q1.sh
q1=`clish -c "show password-controls min-password-length" | grep -i Minimum; 2>/dev/null|
sed -e 's/^[[:blank:]]*//g' -e 's/[[:blank:]]*$//g' -e 's/[[:blank:]][[:blank:]]*/ /g' -e '/^$/d'`; if [ -n
"$q1" ]; then printf "%s" "$q1"; else printf 'Setting not found'; fi;
[Expert@Management:0]# cat q2.sh
q1=`cpstat os | grep "SVN Foundation Version String:" | awk -F":" '{print $2}' | sed -e
's/[[:blank:]]//g'`; if [ ! -z "$q1" ]; then echo "$q1"; else echo 'Setting not found'; fi;
[Expert@Management:0]#
```

STEP 3 : **Copy.sh** is central script that copies files from management to gateway and add it to extended list . This is just an first draft this can be modified to add another command and to perform another function centrally. script is based on cprid utility Please read the **sk101047**

Note : Adding wrong command to copy.sh can cause serious impact as script does not ask any authentication it uses SIC to send command to gateways . Handle with care .

```
[Expert@Management:0]# cat copy.sh
#!/bin/bash
for dest in $(<gateway_ip_list.txt); do
echo "copying files and adding command to firewall $dest "
cprid_util putfile -server  $dest  -local_file /home/admin/qualys/q1.sh -remote_  file
/home/admin/q1.sh
cprid_util putfile -server  $dest  -local_file /home/admin/qualys/q2.sh -remote_  file
/home/admin/q2.sh

cprid_util -server $dest -verbose rexec -rcmd /bin/bash -c "chmod 777 /home/admin/q1.sh "
cprid_util -server $dest -verbose rexec -rcmd /bin/bash -c "chmod 777 /home/admin/q2.sh "

cprid_util -server $dest -verbose rexec -rcmd /bin/clish -s -c 'lock database override'
cprid_util -server $dest -verbose rexec -rcmd /bin/clish -s -c 'add command q1 path
/home/admin/q1.sh description q1'
cprid_util -server $dest -verbose rexec -rcmd /bin/clish -s -c 'add command q2 path
/home/admin/q2.sh description q2'
cprid_util -server $dest -verbose rexec -rcmd /bin/clish -s -c 'save config'
done
[Expert@Management:0]#
```

Step 4 : Execute the script

```
[Expert@Management:0]# ./copy.sh
```

copying and adding command to firewall 10.1.1.101

CLINFR0771 Config lock is owned by admin. Use the command 'lock database override' to acquire the lock.

Command (q1) was added.
Save the configuration and re sign in for changes to take place.

Command (q2) was added.
Save the configuration and re sign in for changes to take place.

copying and adding command to firewall 10.1.1.104

CLINFR0771 Config lock is owned by admin. Use the command 'lock database override' to acquire the lock.

Command (q1) was added.
Save the configuration and re sign in for changes to take place.

Command (q2) was added.
Save the configuration and re sign in for changes to take place.

[Expert@Management:0]#

SCENARIO 2 :

Customer requirement: For firewall hardening or day to day operation for gateway level change like configuring snmp ,NTP , gateway backup, collecting version info or to know enabled blade customer has to do the changes on each gateway . They wanted to perform all these task from central management

Provided solution: **rcommand.sh** script gives user a choice to run bash or clish command to run on all the gateways which has working SIC .

STEP 1 : Following the sk85621 collect all the IP of gateway to text file in this case **gateway_ip_list.txt** or manually put the IP address of all the gateway to a file called **gateway_ip_list.txt**

STEP 2: create a file and name it as **rcommand.sh** and change its permission to 777

*********below is the script *************
[Expert@Management:0]# cat **rcommand.sh**
#!/bin/bash

echo "Do you want to run bash or clish command"
read shell
echo "please input the $shell command to run on all the gateway"
read input
for dest in $(<gateway_ip_list.txt); do
echo "running the $shell command $input on $dest "

cprid_util -server $dest -verbose rexec -rcmd /bin/$shell -c "$input"
done

[Expert@Management:0]#

****

STEP 3 : Execute the script

[Expert@Management:0]# ./**rcommand.sh**
Do you want to run **bash** or **clish** command
bash
please input the bash command to run on all the gateway
enabled_blades.sh
running the bash command enabled_blades.sh on **10.1.1.101**
fw vpn

running the bash command enabled_blades.sh on **10.1.1.104**
fw

[Expert@Management:0]# **./rcommand.sh**
Do you want to run **bash** or **clish** command
clish
please input the clish command to run on all the gateway
show hostname
running the clish command show hostname on **10.1.1.101**
GW-Perimeter

running the clish command show hostname on **10.1.1.104**
TEST-GW01

END**********************************

