Omgamganapathayenamaha

Omgamganapathayenamaha

Omgamganapathayenamaha

How to install ryslog?

$ sudo apt-get install rsyslog

Where is the Configuration?

qnc-jdi-regression:/etc/rsyslog.d> pwd

/etc/rsyslog.d

[root@qnc-ng-crm-vm01:/etc/rsyslog.d#](mailto:root@qnc-ng-crm-vm01:/etc/rsyslog.d) ls -ltr

total 16

-rw-r--r-- 1 root root 1655 Dec 2 2015 50-default.conf

-rw-r--r-- 1 root root 242 Oct 25 2017 postfix.conf

-rw-r--r-- 1 root root 705 May 15 03:19 01-json-template.conf

-rw-r--r-- 1 root root 279 May 15 03:22 tmpl.conf

[root@qnc-ng-crm-vm01:/etc/rsyslog.d#](mailto:root@qnc-ng-crm-vm01:/etc/rsyslog.d)

[root@qnc-ng-crm-vm01:/etc/rsyslog.d#](mailto:root@qnc-ng-crm-vm01:/etc/rsyslog.d) cat tmpl.conf

$template TmplAuth, "/var/log/client\_logs/%HOSTNAME%/%PROGRAMNAME%.log"

$template TmplMsg, "/var/log/client\_logs/%HOSTNAME%/%PROGRAMNAME%.log"

\*.\* @10.47.227.190:10514;json-template

authpriv.\* ?TmplAuth

\*.info;mail.none;authpriv.none;cron.none ?TmplMsg

[root@qnc-ng-crm-vm01:/etc/rsyslog.d#](mailto:root@qnc-ng-crm-vm01:/etc/rsyslog.d)

root@qnc-jdi-regression:~# ls -ltr /etc/rsyslog.conf

-rw-r--r-- 1 root root 1892 Apr 9 12:46 /etc/rsyslog.conf

root@qnc-jdi-regression:~#

[root@qnc-ng-crm-vm01:/etc/rsyslog.d#](mailto:root@qnc-ng-crm-vm01:/etc/rsyslog.d) sudo service rsyslog start

[root@qnc-ng-crm-vm01:/etc/rsyslog.d#](mailto:root@qnc-ng-crm-vm01:/etc/rsyslog.d) sudo service rsyslog restart

[root@qnc-ng-crm-vm01:~/kvsr/elastic/logstash-6.2.1#](mailto:root@qnc-ng-crm-vm01:~/kvsr/elastic/logstash-6.2.1) ps auxxx | grep rsyslog

syslog 10776 0.0 0.0 437292 3752 ? Ssl 03:30 0:00 /usr/sbin/rsyslogd -n

root 11128 0.0 0.0 12948 1088 pts/0 R+ 03:35 0:00 grep --color=auto rsyslog

[root@qnc-ng-crm-vm01:~/kvsr/elastic/logstash-6.2.1#](mailto:root@qnc-ng-crm-vm01:~/kvsr/elastic/logstash-6.2.1)

Where are the Router Logs?

qnc-jdi-regression:/var/log/client\_logs> pwd

/var/log/client\_logs

qnc-jdi-regression:/var/log/client\_logs> ls -ltr

total 20K

drwxr-xr-x 2 syslog syslog 4096 Apr 10 03:32 qnc-jdi-regression

drwxr-xr-x 2 syslog syslog 4096 Apr 10 03:53 r0d

drwxr-xr-x 2 syslog syslog 4096 Apr 10 04:00 r1d

drwxr-xr-x 2 syslog syslog 4096 Apr 10 04:00 r1a

drwxr-xr-x 2 syslog syslog 4096 Apr 10 04:04 r1b

qnc-jdi-regression:/var/log/client\_logs>

Demo Topo

r0d 🡪 qnc-ng-crm-vm01 (10.47.227.190) (rsyslog + logstash installed on this VM)

regress@r0d# show system syslog | display set

set system syslog host 10.47.227.190 any any

set system syslog host 10.47.227.190 interactive-commands any

set system syslog host 10.47.227.190 port 514

[edit]

regress@r0d#

r1a 🡪 qnc-ng-crm-vm03 (10.47.227.192) (rsyslog + logstash installed on this VM)

regress@r1a# show system syslog | display set

set system syslog host 10.47.227.192 any info

set system syslog host 10.47.227.192 interactive-commands any

set system syslog host 10.47.227.192 match "(requested 'commit' operation)|(requested 'commit synchronize' operation)|(copying configuration to juniper.save)|(commit complete)|ifAdminStatus|(FRU power)|(FRU removal)|(FRU insertion)|(link UP)|transitioned|Transferred|transfer-file|(license add)|(license delete)|(package -X update)|(package -X delete)|(FRU Online)|(FRU Offline)|(plugged in)|(unplugged)|CFMD\_CCM\_DEFECT| LFMD\_3AH | RPD\_MPLS\_PATH\_BFD|(Master Unchanged, Members Changed)|(Master Changed, Members Changed)|(Master Detected, Members Changed)|(vc add)|(vc delete)|(Master detected)|(Master changed)|(Backup detected)|(Backup changed)|(interface vcp-)"

set system syslog host 10.47.227.192 port 514

set system syslog host 10.47.227.192 structured-data

[edit]

regress@r1a#

r1b 🡪 qnc-jdi-regression (10.50.40.70) (rsyslog + logstash installed on this VM)

regress@r1b# show system syslog | display set

set system syslog host 10.50.40.70 any any

[edit]

regress@r1b#

r1d 🡪 qnc-jdi-regression (10.50.40.70) (rsyslog + logstash installed on this VM)

regress@r1d# show system syslog | display set

set system syslog host 10.50.40.70 any any

[edit]

regress@r1d#

Elasticsearch + Kibana 🡪 qnc-ng-crm-vm02 (10.47.227.191)

3 NG CRM VMs are 2 mins ahead of qnc-jdi-regression VM (Have to think of a solution here)

Changing baseline configuration of the Devices

Update ‘syslog.conf’ into ‘cc\_config block’ of system-test/machine/megafon/config

cvs commit -m"updated" system-test/machine/megafon/config

systest-cvsupdate --prefix machine --file megafon/config

clean\_config -r megafon

Thanks and Regards,

Sastry