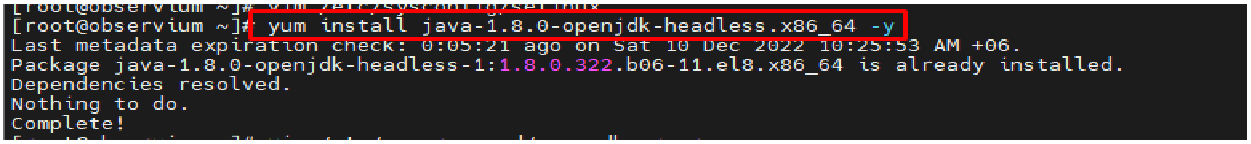
Install Graylog Server on CentOS 8

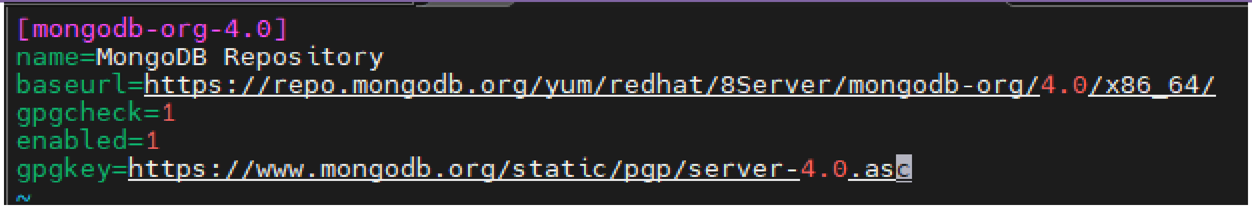
```
[root@observium ~]# yum install java-1.8.0-openjdk-headless.x86_64 –y
```



```
[root@observium ~]# yum install java-1.8.0-openjdk-headless.x86_64 -y
Last metadata expiration check: 0:05:21 ago on Sat 10 Dec 2022 10:25:53 AM +06.
Package java-1.8.0-openjdk-headless-1:1.8.0.322.b06-11.el8.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
```

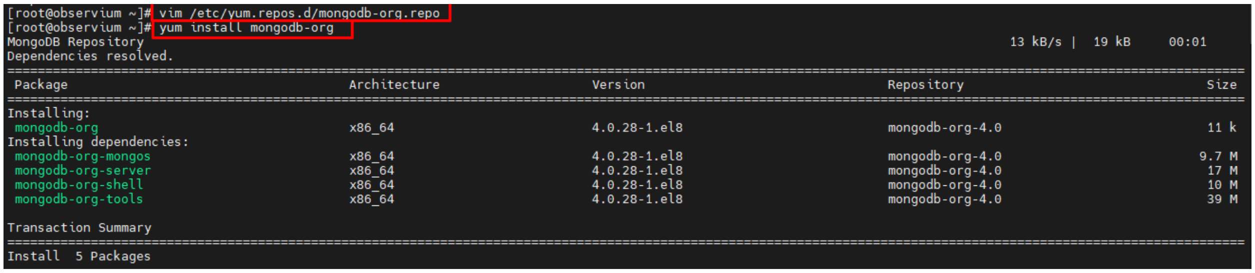
```
[root@observium ~]# vim /etc/yum.repos.d/mongodb-org.repo
```

```
[mongodb-org-4.0]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/8Server/mongodb-org/4.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://www.mongodb.org/static/pgp/server-4.0.asc
```



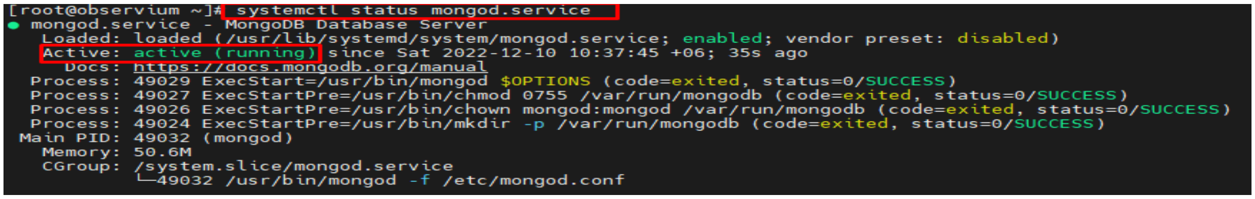
```
[mongodb-org-4.0]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/8Server/mongodb-org/4.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://www.mongodb.org/static/pgp/server-4.0.asc
~
```

```
[root@observium ~]# yum install mongodb-org -y
```



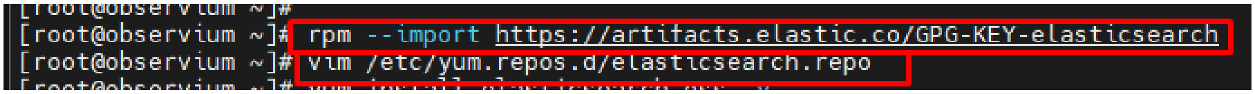
```
[root@observium ~]# vim /etc/yum.repos.d/mongodb-org.repo
[root@observium ~]# yum install mongodb-org
MongoDB Repository                                                                    13 kB/s |  19 kB     00:01
Dependencies resolved.
=====================================================================================================================
 Package                      Architecture          Version                   Repository                       Size
=====================================================================================================================
Installing:
 mongodb-org                  x86_64                4.0.28-1.el8              mongodb-org-4.0                  11 k
Installing dependencies:
 mongodb-org-mongos           x86_64                4.0.28-1.el8              mongodb-org-4.0                 9.7 M
 mongodb-org-server           x86_64                4.0.28-1.el8              mongodb-org-4.0                  17 M
 mongodb-org-shell            x86_64                4.0.28-1.el8              mongodb-org-4.0                  10 M
 mongodb-org-tools            x86_64                4.0.28-1.el8              mongodb-org-4.0                  39 M

Transaction Summary
=====================================================================================================================
Install  5 Packages
```

```
 [root@observium ~]# systemctl enable mongod.service

[root@observium ~]# systemctl restart mongod.service

[root@observium ~]# systemctl start mongod.service

[root@observium ~]# systemctl status mongod.service
```



```
[root@observium ~]# systemctl status mongod.service
● mongod.service - MongoDB Database Server
   Loaded: loaded (/usr/lib/systemd/system/mongod.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2022-12-10 10:37:45 +06; 35s ago
     Docs: https://docs.mongodb.org/manual
  Process: 49029 ExecStart=/usr/bin/mongod $OPTIONS (code=exited, status=0/SUCCESS)
  Process: 49027 ExecStartPre=/usr/bin/chmod 0755 /var/run/mongodb (code=exited, status=0/SUCCESS)
  Process: 49026 ExecStartPre=/usr/bin/chown mongod:mongod /var/run/mongodb (code=exited, status=0/SUCCESS)
  Process: 49024 ExecStartPre=/usr/bin/mkdir -p /var/run/mongodb (code=exited, status=0/SUCCESS)
 Main PID: 49032 (mongod)
   Memory: 50.6M
   CGroup: /system.slice/mongod.service
           └─49032 /usr/bin/mongod -f /etc/mongod.conf
```

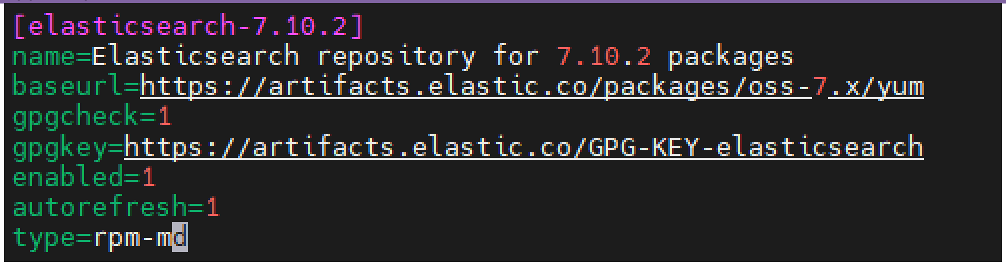
[root@observium ~]# rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch



```
[root@observium ~]#
[root@observium ~]# rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch
[root@observium ~]# vim /etc/yum.repos.d/elasticsearch.repo
```

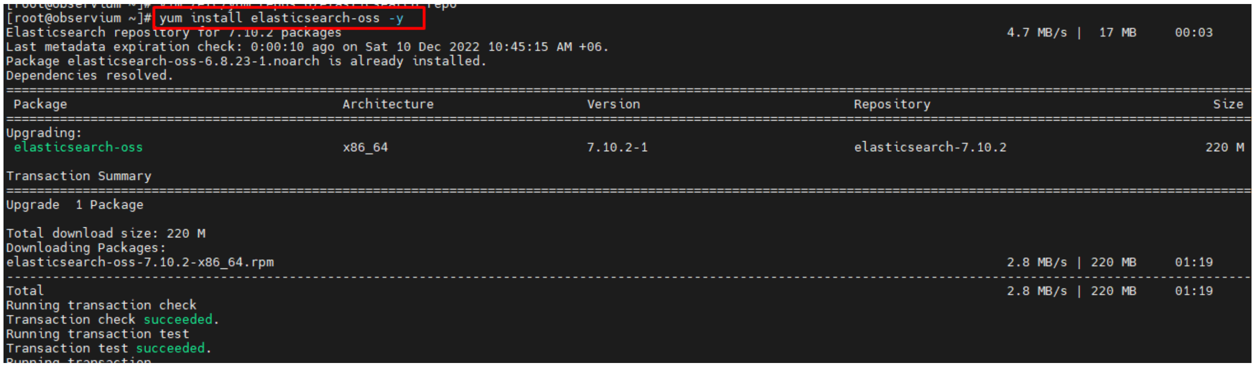
[root@observium ~]# vim /etc/yum.repos.d/elasticsearch.repo

```
[elasticsearch-7.10.2]
name=Elasticsearch repository for 7.10.2 packages
baseurl=https://artifacts.elastic.co/packages/oss-7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```



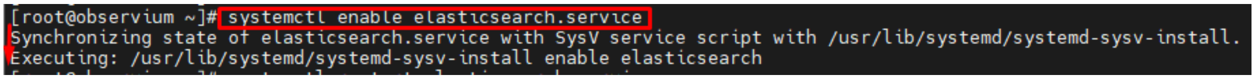
```
[elasticsearch-7.10.2]
name=Elasticsearch repository for 7.10.2 packages
baseurl=https://artifacts.elastic.co/packages/oss-7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

[root@observium ~]# yum install elasticsearch-oss –y



```
[root@observium ~]# yum install elasticsearch-oss -y
Elasticsearch repository for 7.10.2 packages                                          4.7 MB/s |  17 MB     00:03
Last metadata expiration check: 0:00:10 ago on Sat 10 Dec 2022 10:45:15 AM +06.
Package elasticsearch-oss-6.8.23-1.noarch is already installed.
Dependencies resolved.
========================================================================================================================
 Package                        Architecture              Version                    Repository                    Size
========================================================================================================================
Upgrading:
 elasticsearch-oss              x86_64                    7.10.2-1                   elasticsearch-7.10.2         220 M

Transaction Summary
========================================================================================================================
Upgrade  1 Package

Total download size: 220 M
Downloading Packages:
elasticsearch-oss-7.10.2-x86_64.rpm                                                   2.8 MB/s | 220 MB     01:19
------------------------------------------------------------------------------------------------------------------------
Total                                                                                 2.8 MB/s | 220 MB     01:19
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
```

[root@observium ~]# systemctl enable elasticsearch.service

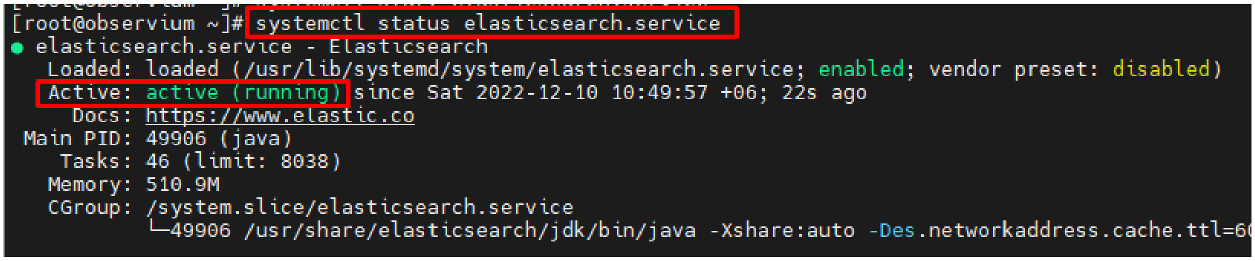


```
[root@observium ~]# systemctl enable elasticsearch.service
Synchronizing state of elasticsearch.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable elasticsearch
```

[root@observium ~]# systemctl restart elasticsearch.service

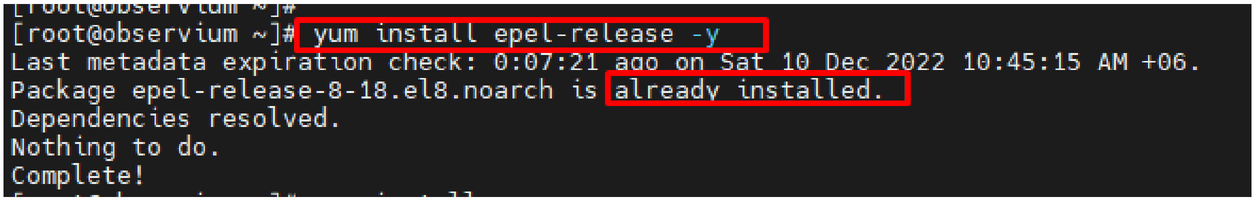
[root@observium ~]# systemctl start elasticsearch.service

[root@observium ~]# systemctl status elasticsearch.service



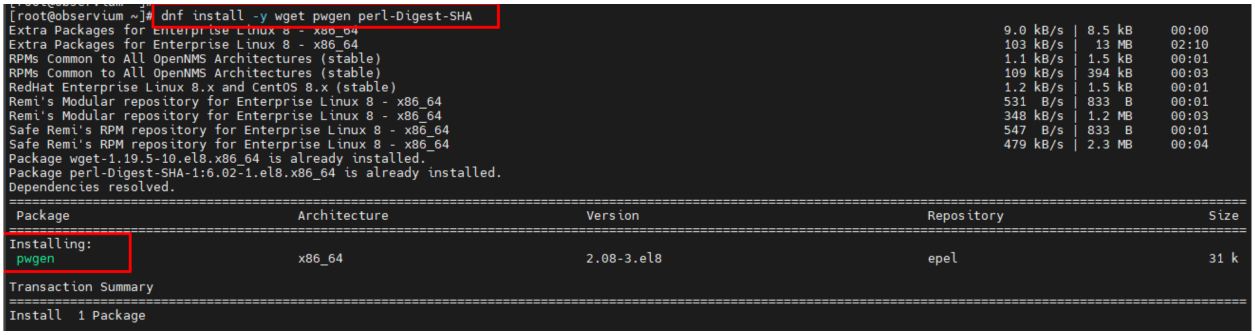
```
[root@observium ~]# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2022-12-10 10:49:57 +06; 22s ago
     Docs: https://www.elastic.co
 Main PID: 49906 (java)
    Tasks: 46 (limit: 8038)
   Memory: 510.9M
   CGroup: /system.slice/elasticsearch.service
           └─49906 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60
```

[root@observium ~]# yum install epel-release –y



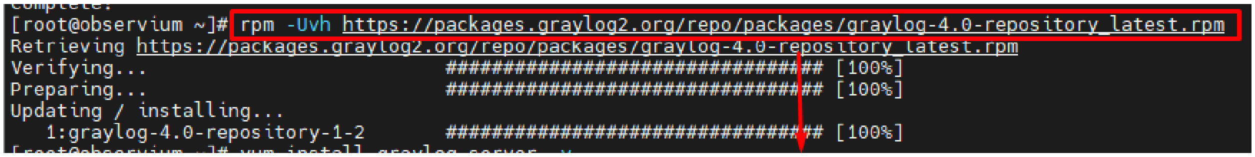
```
[root@observium ~]# yum install epel-release -y
Last metadata expiration check: 0:07:21 ago on Sat 10 Dec 2022 10:45:15 AM +06.
Package epel-release-8-18.el8.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!
```

[root@observium ~]# yum install pwgen –y



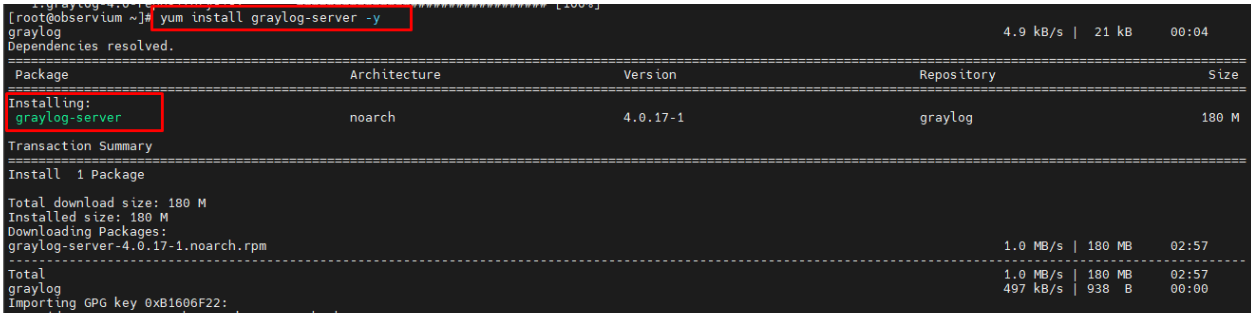
```
[root@observium ~]# dnf install -y wget pwgen perl-Digest-SHA
Extra Packages for Enterprise Linux 8 - x86_64                                  9.0 kB/s | 8.5 kB     00:00
Extra Packages for Enterprise Linux 8 - x86_64                                  103 kB/s |  13 MB     02:10
RPMs Common to All OpenNMS Architectures (stable)                               1.1 kB/s | 1.5 kB     00:01
RPMs Common to All OpenNMS Architectures (stable)                               109 kB/s | 394 kB     00:03
RedHat Enterprise Linux 8.x and CentOS 8.x (stable)                             1.2 kB/s | 1.5 kB     00:01
Remi's Modular repository for Enterprise Linux 8 - x86_64                       531  B/s | 833  B     00:01
Remi's Modular repository for Enterprise Linux 8 - x86_64                       348 kB/s | 1.2 MB     00:03
Safe Remi's RPM repository for Enterprise Linux 8 - x86_64                      547  B/s | 833  B     00:01
Safe Remi's RPM repository for Enterprise Linux 8 - x86_64                      479 kB/s | 2.3 MB     00:04
Package wget-1.19.5-10.el8.x86_64 is already installed.
Package perl-Digest-SHA-1:6.02-1.el8.x86_64 is already installed.
Dependencies resolved.
==================================================================================================================
 Package                       Architecture                Version                        Repository        Size
==================================================================================================================
Installing:
 pwgen                         x86_64                      2.08-3.el8                     epel              31 k

Transaction Summary
==================================================================================================================
Install  1 Package
```

[root@observium ~]# rpm -Uvh https://packages.graylog2.org/repo/packages/graylog-4.0-repository_latest.rpm



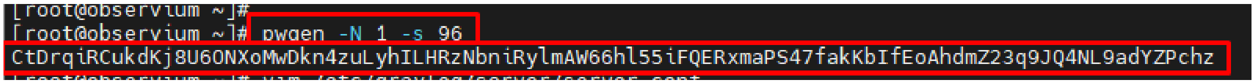
```
[root@observium ~]# rpm -Uvh https://packages.graylog2.org/repo/packages/graylog-4.0-repository_latest.rpm
Retrieving https://packages.graylog2.org/repo/packages/graylog-4.0-repository_latest.rpm
Verifying...                          ################################# [100%]
Preparing...                          ################################# [100%]
Updating / installing...
   1:graylog-4.0-repository-1-2       ################################# [100%]
```

[root@observium ~]# yum install graylog-server –y



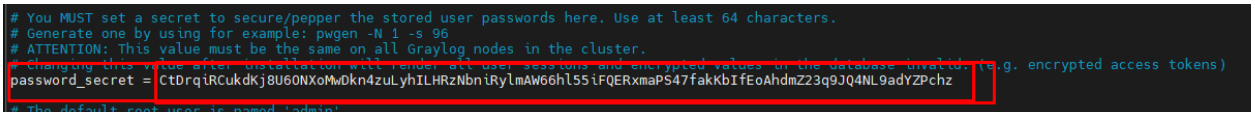
```
[root@observium ~]# yum install graylog-server -y
graylog                                                                         4.9 kB/s |  21 kB     00:04
Dependencies resolved.
==================================================================================================================
 Package                       Architecture             Version                   Repository                Size
==================================================================================================================
Installing:
 graylog-server                noarch                   4.0.17-1                  graylog                  180 M

Transaction Summary
==================================================================================================================
Install  1 Package

Total download size: 180 M
Installed size: 180 M
Downloading Packages:
graylog-server-4.0.17-1.noarch.rpm                                              1.0 MB/s | 180 MB     02:57
------------------------------------------------------------------------------------------------------------------
Total                                                                           1.0 MB/s | 180 MB     02:57
graylog                                                                         497 kB/s | 938  B     00:00
Importing GPG key 0xB1606F22:
```

```
[root@observium ~]# pwgen -N 1 -s 96

CtDrqiRCukdKj8U6ONXoMwDkn4zuLyhILHRzNbniRylmAW66hl55iFQERxmaPS47fakKbIfEoAhdmZ23q9JQ4NL9adYZPchz
```



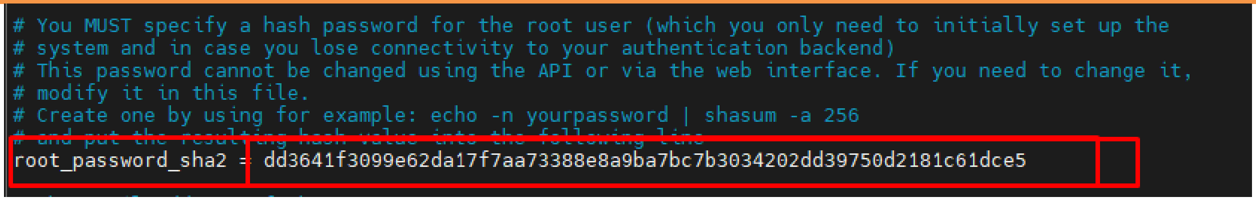
```
[root@observium ~]#
[root@observium ~]# pwgen -N 1 -s 96
CtDrqiRCukdKj8U6ONXoMwDkn4zuLyhILHRzNbniRylmAW66hl55iFQERxmaPS47fakKbIfEoAhdmZ23q9JQ4NL9adYZPchz
```

```
[root@observium ~]# vim /etc/graylog/server/server.conf
```

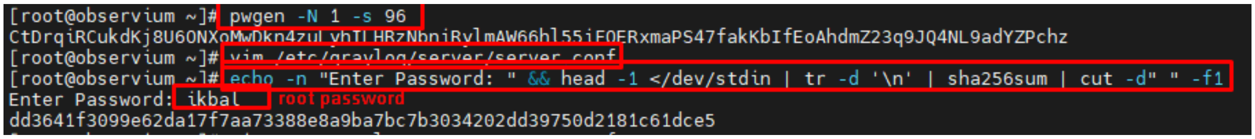


```
# You MUST set a secret to secure/pepper the stored user passwords here. Use at least 64 characters.
# Generate one by using for example: pwgen -N 1 -s 96
# ATTENTION: This value must be the same on all Graylog nodes in the cluster.
# Changing this value after installation will render all user sessions and encrypted values in the database invalid. (e.g. encrypted access tokens)
password_secret = CtDrqiRCukdKj8U6ONXoMwDkn4zuLyhILHRzNbniRylmAW66hl55iFQERxmaPS47fakKbIfEoAhdmZ23q9JQ4NL9adYZPchz
```

```
[root@observium ~]# echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1

Enter Password: ikbal
dd3641f3099e62da17f7aa73388e8a9ba7bc7b3034202dd39750d2181c61dce5
```



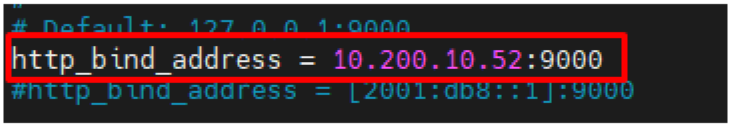
```
# You MUST specify a hash password for the root user (which you only need to initially set up the
# system and in case you lose connectivity to your authentication backend)
# This password cannot be changed using the API or via the web interface. If you need to change it,
# modify it in this file.
# Create one by using for example: echo -n yourpassword | shasum -a 256
# and put the resulting hash value into the following line
root_password_sha2 = dd3641f3099e62da17f7aa73388e8a9ba7bc7b3034202dd39750d2181c61dce5
```



```
[root@observium ~]# pwgen -N 1 -s 96
CtDrqiRCukdKj8U6ONXoMwDkn4zuLyhILHRzNbniRylmAW66hl55iFQERxmaPS47fakKbIfEoAhdmZ23q9JQ4NL9adYZPchz
[root@observium ~]# vim /etc/graylog/server/server.conf
[root@observium ~]# echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1
Enter Password: ikbal   root password
dd3641f3099e62da17f7aa73388e8a9ba7bc7b3034202dd39750d2181c61dce5
```

```
[root@observium ~]# vim /etc/graylog/server/server.conf
```

Server IP address:

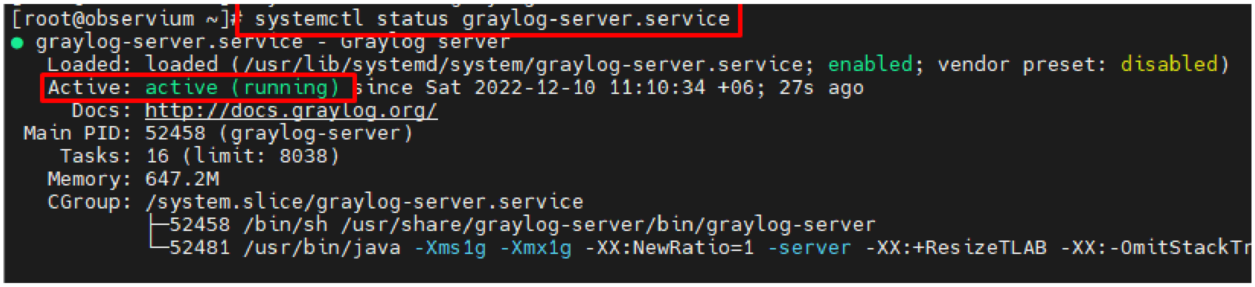


```
# Default: 127.0.0.1:9000
http_bind_address = 10.200.10.52:9000
#http_bind_address = [2001:db8::1]:9000
```

```
[root@observium ~]# systemctl enable graylog-server.service

Synchronizing state of graylog-server.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable graylog-server
Created symlink /etc/systemd/system/multi-user.target.wants/graylog-server.service →
/usr/lib/systemd/system/graylog-server.service.
```

```
[root@observium ~]# systemctl restart graylog-server.service
```

```
[root@observium ~]# systemctl start graylog-server.service

[root@observium ~]# systemctl status graylog-server.service
```



```
[root@observium ~]# systemctl status graylog-server.service
● graylog-server.service - Graylog server
   Loaded: loaded (/usr/lib/systemd/system/graylog-server.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2022-12-10 11:10:34 +06; 27s ago
     Docs: http://docs.graylog.org/
 Main PID: 52458 (graylog-server)
    Tasks: 16 (limit: 8038)
   Memory: 647.2M
   CGroup: /system.slice/graylog-server.service
           ├─52458 /bin/sh /usr/share/graylog-server/bin/graylog-server
           └─52481 /usr/bin/java -Xms1g -Xmx1g -XX:NewRatio=1 -server -XX:+ResizeTLAB -XX:-OmitStackTr
```

```
[root@observium ~]#

[root@observium ~]# setsebool -P httpd_can_network_connect 1

[root@observium ~]# sudo semanage port -a -t mongod_port_t -p tcp 27017

[root@observium ~]# firewall-cmd --zone=public --add-port=9000/tcp --permanent

success

[root@observium ~]# firewall-cmd --reload

Success

[root@observium ~]# firewall-cmd  --list-all

public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client http mysql ssh
  ports: 9000/tcp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

```
[root@observium ~]# systemctl enable graylog-server.service
```

```
Synchronizing state of graylog-server.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable graylog-server
```

```
[root@observium ~]# systemctl start graylog-server.service

[root@observium ~]# systemctl daemon-reload

[root@observium ~]# systemctl enable mongod.service

[root@observium ~]# systemctl start mongod.service

[root@observium ~]# systemctl enable elasticsearch.service

Synchronizing state of elasticsearch.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable elasticsearch
```

```
[root@observium ~]# systemctl restart elasticsearch.service

[root@observium ~]# systemctl enable graylog-server.service

Synchronizing state of graylog-server.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable graylog-server

[root@observium ~]# systemctl start graylog-server.service

[root@observium ~]#
```

Source link:

https://go2docs.graylog.org/5-0/downloading_and_installing_graylog/red_hat_installation.htm?tocpath=Downloading%20and%20Installing%20Graylog%7CInstalling%20Graylog%7C_____7

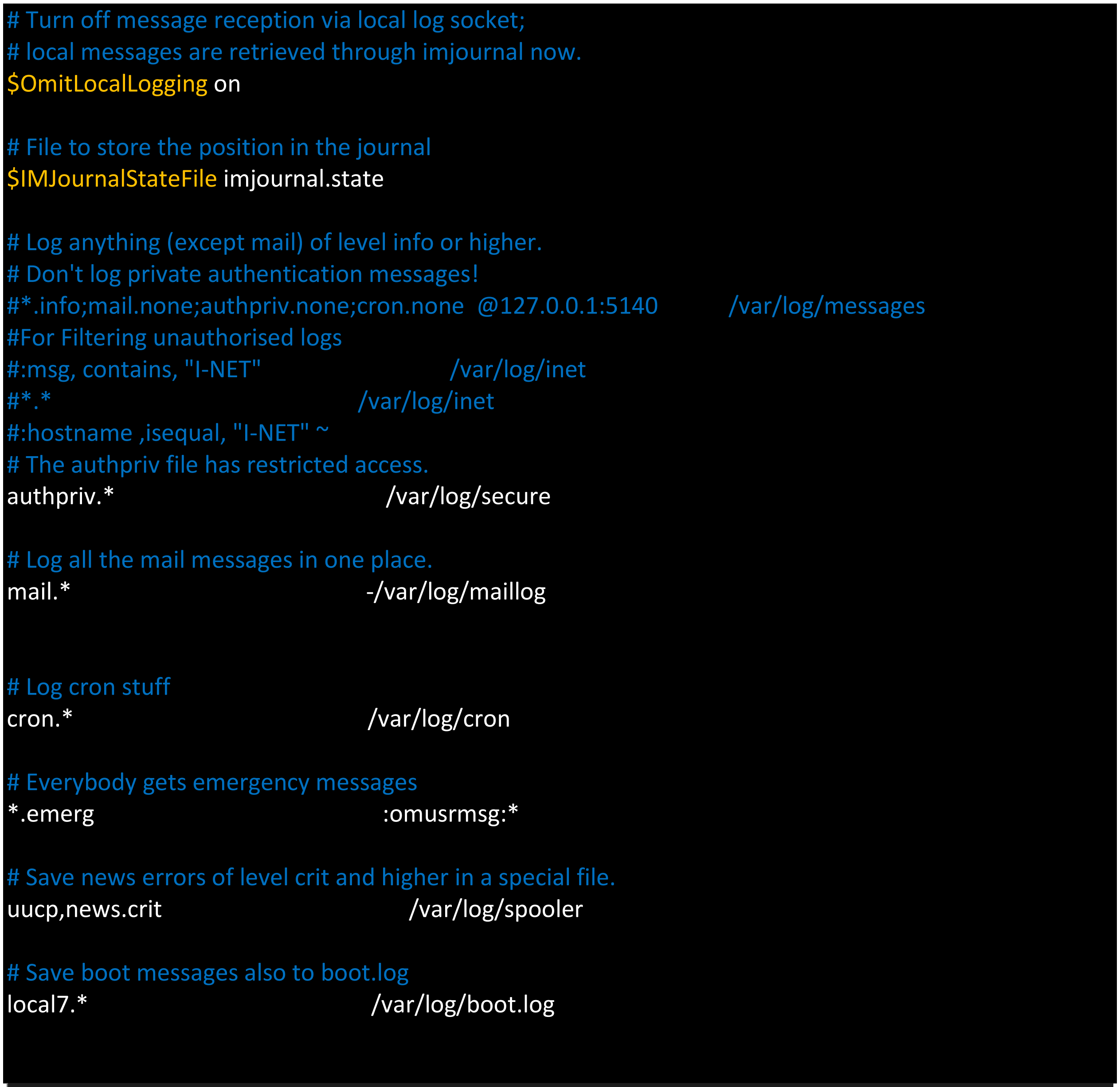
https://www.youtube.com/watch?v=UXBOAuqUoko&ab_channel=SEKANLINPRINCIPE

https://github.com/kipling752/monitoring/blob/main/configuration%20graylog

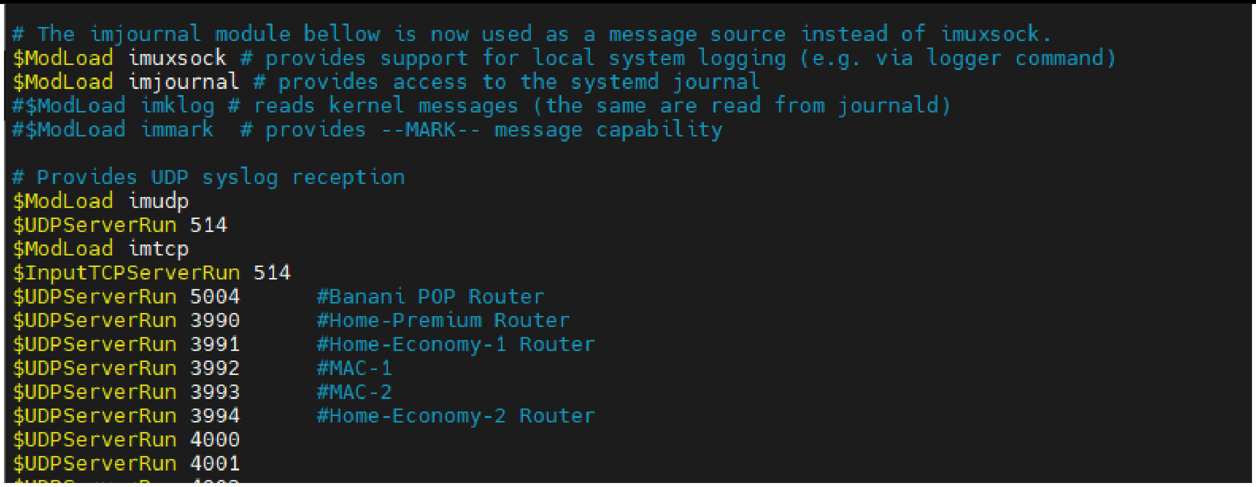
Log Server Log Add PORT Use korta hoy

Log Server Log Router Add:

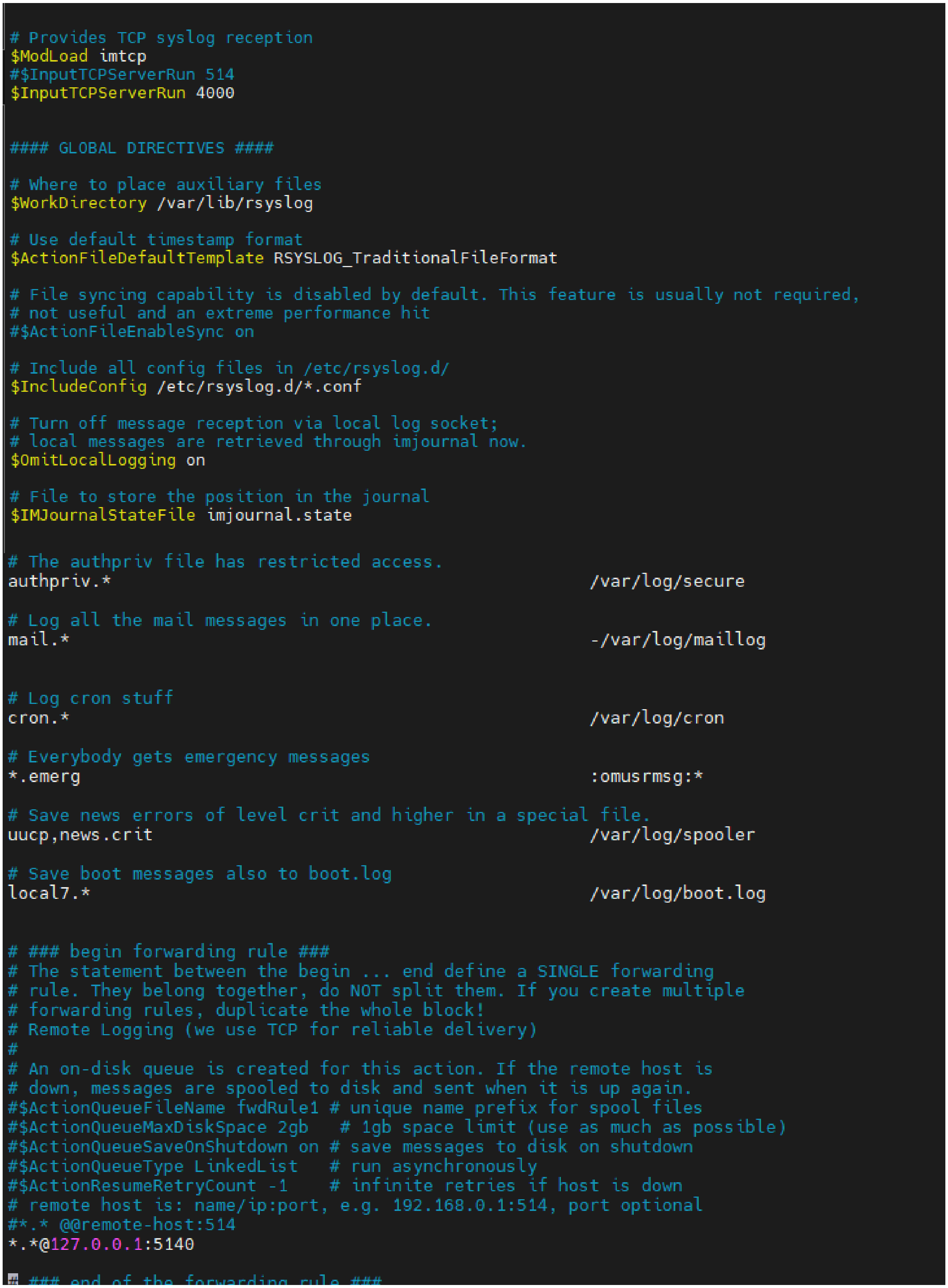
```
[root@flow ~]# vim /etc/rsyslog.conf

# The imjournal module bellow is now used as a message source instead of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
#$ModLoad immark  # provides --MARK-- message capability

# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
$ModLoad imtcp
$InputTCPServerRun 514
$UDPServerRun 5004     #Banani POP Router
$UDPServerRun 3990     #Home-Premium Router
$UDPServerRun 3991     #Home-Economy-1 Router
$UDPServerRun 3992     #MAC-1
$UDPServerRun 3993     #MAC-2
$UDPServerRun 3994     #Home-Economy-2 Router
$UDPServerRun 4000
$UDPServerRun 4001


# Provides TCP syslog reception
$ModLoad imtcp
#$InputTCPServerRun 514
$InputTCPServerRun 4000


#### GLOBAL DIRECTIVES ####

# Where to place auxiliary files
$WorkDirectory /var/lib/rsyslog

# Use default timestamp format
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# File syncing capability is disabled by default. This feature is usually not required,
# not useful and an extreme performance hit
#$ActionFileEnableSync on

# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf
```



```
# Turn off message reception via local log socket;
# local messages are retrieved through imjournal now.
$OmitLocalLogging on

# File to store the position in the journal
$IMJournalStateFile imjournal.state

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
#*.info;mail.none;authpriv.none;cron.none  @127.0.0.1:5140          /var/log/messages
#For Filtering unauthorised logs
#:msg, contains, "I-NET"                          /var/log/inet
#*.*                                      /var/log/inet
#:hostname ,isequal, "I-NET" ~
# The authpriv file has restricted access.
authpriv.*                                      /var/log/secure

# Log all the mail messages in one place.
mail.*                                        -/var/log/maillog


# Log cron stuff
cron.*                                        /var/log/cron

# Everybody gets emergency messages
*.emerg                                         :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                    /var/log/spooler

# Save boot messages also to boot.log
local7.*                                        /var/log/boot.log
```



```
# The imjournal module bellow is now used as a message source instead of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
#$ModLoad immark  # provides --MARK-- message capability

# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
$ModLoad imtcp
$InputTCPServerRun 514
$UDPServerRun 5004      #Banani POP Router
$UDPServerRun 3990      #Home-Premium Router
$UDPServerRun 3991      #Home-Economy-1 Router
$UDPServerRun 3992      #MAC-1
$UDPServerRun 3993      #MAC-2
$UDPServerRun 3994      #Home-Economy-2 Router
$UDPServerRun 4000
$UDPServerRun 4001
```



```
# Provides TCP syslog reception
$ModLoad imtcp
#$InputTCPServerRun 514
$InputTCPServerRun 4000


#### GLOBAL DIRECTIVES ####

# Where to place auxiliary files
$WorkDirectory /var/lib/rsyslog

# Use default timestamp format
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# File syncing capability is disabled by default. This feature is usually not required,
# not useful and an extreme performance hit
#$ActionFileEnableSync on

# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf

# Turn off message reception via local log socket;
# local messages are retrieved through imjournal now.
$OmitLocalLogging on

# File to store the position in the journal
$IMJournalStateFile imjournal.state

# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure

# Log all the mail messages in one place.
mail.*                                                  -/var/log/maillog


# Log cron stuff
cron.*                                                  /var/log/cron

# Everybody gets emergency messages
*.emerg                                                 :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                          /var/log/spooler

# Save boot messages also to boot.log
local7.*                                                /var/log/boot.log


# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 2gb   # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList   # run asynchronously
#$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host:514
*.*@127.0.0.1:5140

# ### end of the forwarding rule ###
```