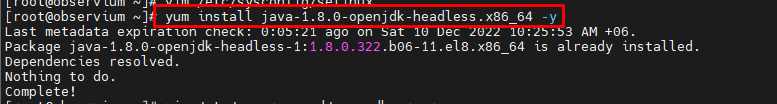
**Install Graylog Server on CentOS 8**

[root@observium ~]# yum install java-1.8.0-openjdk-headless.x86\_64 –y



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

[mongodb-org-4.0]

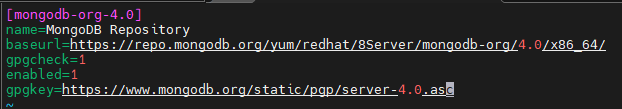
name=MongoDB Repository

baseurl=https://repo.mongodb.org/yum/redhat/8Server/mongodb-org/4.0/x86\_64/

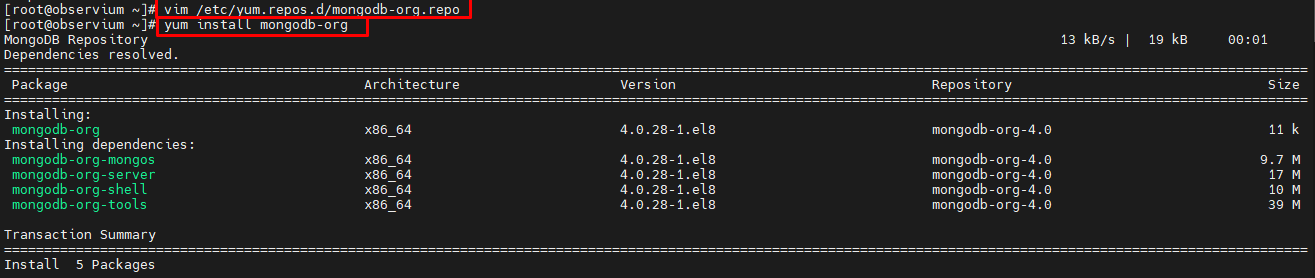
gpgcheck=1

enabled=1

gpgkey=https://www.mongodb.org/static/pgp/server-4.0.asc



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



[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 ~]# rpm --import <https://artifacts.elastic.co/GPG-KEY-elasticsearch>



[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

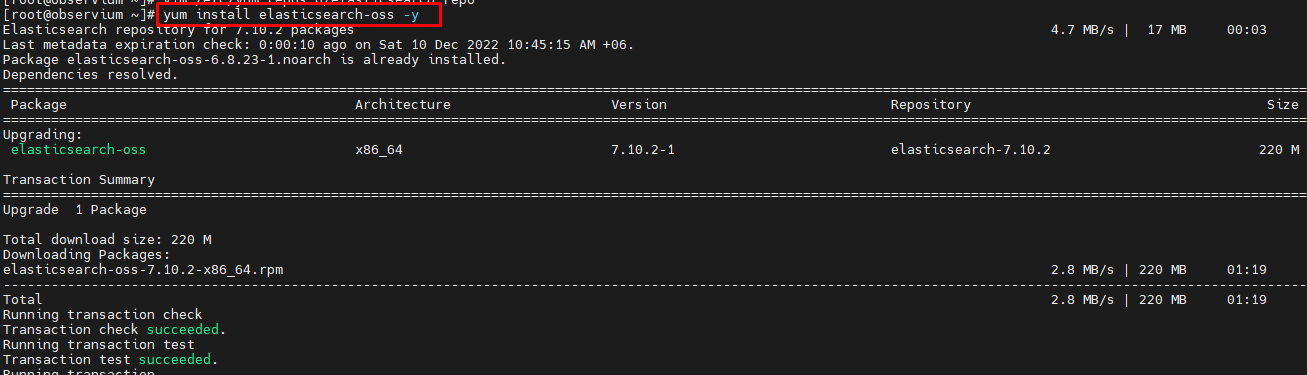
enabled=1

autorefresh=1

type=rpm-md



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



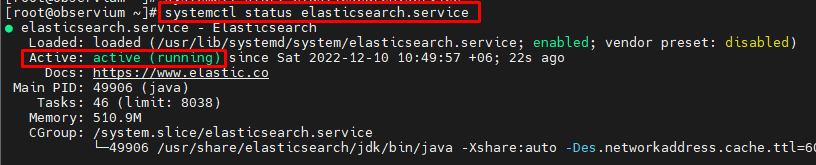
[root@observium ~]# systemctl enable elasticsearch.service



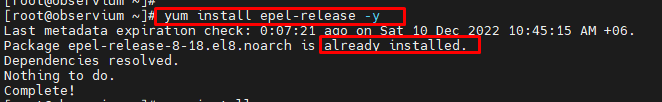
[root@observium ~]# systemctl restart elasticsearch.service

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

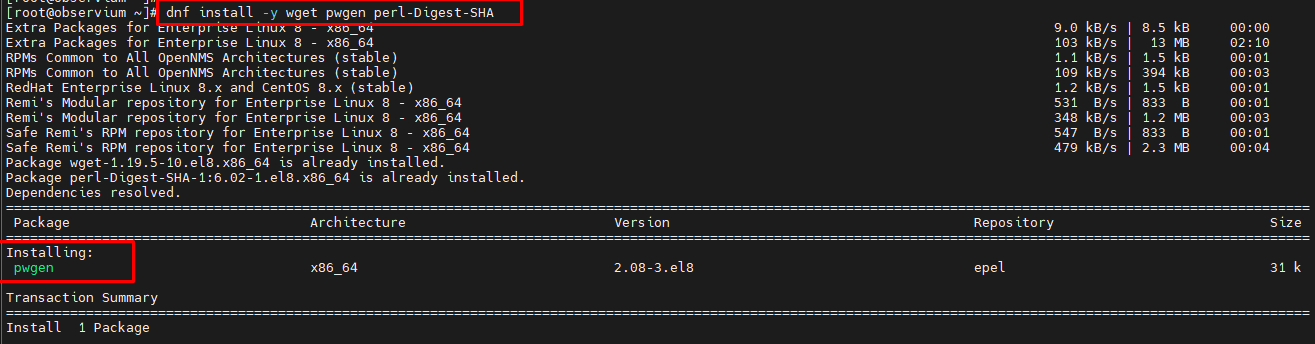
[root@observium ~]# systemctl status elasticsearch.service



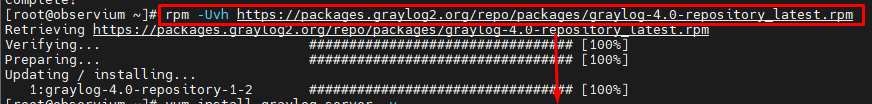
[root@observium ~]# yum install epel-release –y



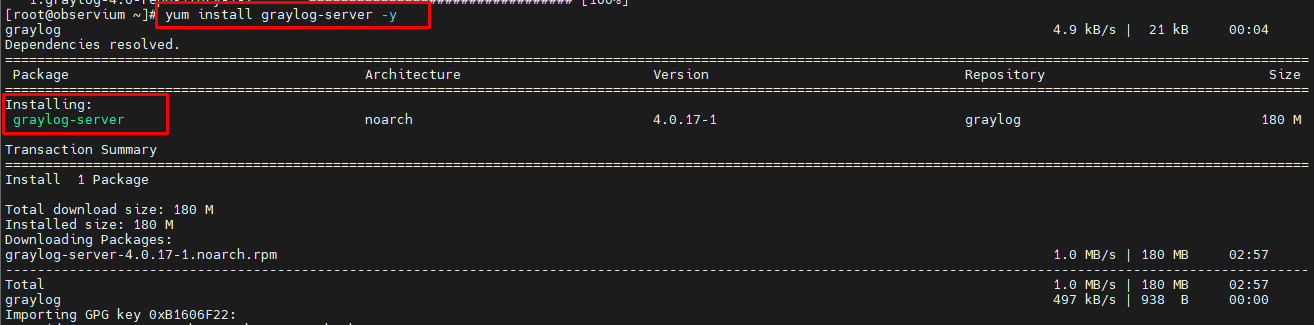
[root@observium ~]# yum install pwgen –y



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



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

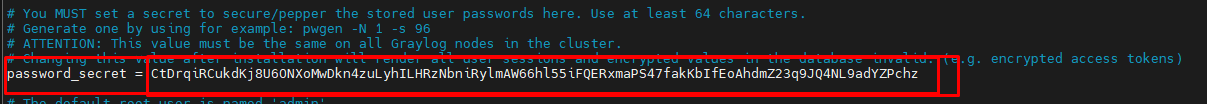


[root@observium ~]# pwgen -N 1 -s 96

CtDrqiRCukdKj8U6ONXoMwDkn4zuLyhILHRzNbniRylmAW66hl55iFQERxmaPS47fakKbIfEoAhdmZ23q9JQ4NL9adYZPchz



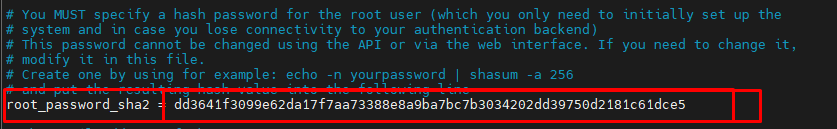
[root@observium ~]# vim /etc/graylog/server/server.conf

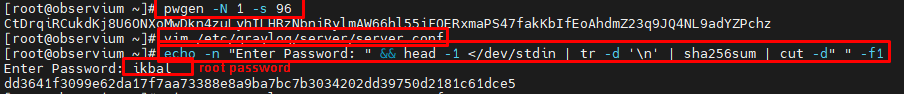


[root@observium ~]# echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1

Enter Password: ikbal

dd3641f3099e62da17f7aa73388e8a9ba7bc7b3034202dd39750d2181c61dce5





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

Server IP address:



[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 ~]#

[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

