**CONFIGURACION DE MONGO DB EN SERVER DE PRODUCCION**

**Nota:** La configuración se a realizado utilizando Droplets, el proveedor de servidores **Digital Ocean** con la versión de **MongoDB 4.4** y una versión de **Centos RHEL 8**.

1. **Configure el sistema de gestión de paquetes (yum).**

Cree un archivo /etc/yum.repos.d/mongodb-org-4.4.repo para que pueda instalar MongoDB directamente usando yum:

Pegar lo siguiente en el archivo creado:

**[mongodb-org-4.4]**

name=MongoDB Repository

baseurl=https://repo.mongodb.org/yum/redhat/$releasever/mongodb-org/4.4/x86\_64/

gpgcheck=1

enabled=1

gpgkey=https://www.mongodb.org/static/pgp/server-4.4.asc

1. **Luego de guardar el archivo ejecutamos:**

sudo yum update

1. **Seguido de esto ejecutar:**

sudo yum install -y mongodb-org

1. **Etiquetamos el puerto que vayamos a utilizar para mongo, se recomiendo no usar el port por defecto por seguridad para este ejemplo usaremos el puerto 27064.**

sudo semanage port -a -t mongod\_port\_t -p tcp 27064

1. **Agregamos permisos al firewall sobre el puerto a utilizarse:**

sudo firewall-cmd --add-port = 27064 / tcp --permanent

sudo firewall-cmd --reload

1. **También se puede limitar el acceso según la dirección ip de origen:**

sudo firewall-cmd --permanent --add-rich-rule "rule family="ipv4" \

source address="ip\_addres" port protocol="tcp" port="27064" accept"

1. **Habilitamos acceso fuera del server**

Editamos el archivo /etc/mongod.conf el cual debe quedar de la siguiente manera:

**Nota:** Lo marcado con color rojo es lo que se tiene que agregar al archivo

systemLog:

destination: file

logAppend: true

path: /var/log/mongodb/mongod.log

# Where and how to store data.

storage:

dbPath: /var/lib/mongo

journal:

enabled: true

# engine:

# wiredTiger:

# how the process runs

processManagement:

fork: true # fork and run in background

pidFilePath: /var/run/mongodb/mongod.pid # location of pidfile

timeZoneInfo: /usr/share/zoneinfo

# network interfaces

net:

port: 27087

bindIp: 127.0.0.1 **,here\_your\_server\_ip\_address**

**security:**

**authorization: enabled**

1. **Recargar deamon**

systemctl daemon-reload

1. **Iniciar y habilitar mongo database:**

systemctl start mongod

systemctl enable mongod

1. **Creación de usuario global con restricciones de autenticación por ip**

Ingresamos a la consola de mongo db:

$ mongo

Ingresamos a la base admin para crear el usuario:

> use admin

**Nota:** La siguiente operación crea un usuario. Este usuario solo puede autenticarse si se conecta de una dirección IP XXX.X.X.X a otra ZZZ.ZZ.ZZZ.Z

db.createUser({user: "your\_user", pwd: "your\_password", roles: [{role: "root", db: "admin"}],authenticationRestrictions:[{clientSource:[ " XXX.X.X.X ","add\_other\_ip" ],serverAddress:[ " ZZZ.ZZ.ZZZ.Z" ]}]})

1. **Crearemos un usuario para una base de datos en específico por seguridad**

Primero nos situamos en la base de datos que queremos crear el usuario:

> use nueva\_base

Luego creamos el usuario con las restricciones de acceso por ip, roles y base de datos a la que va a pertenecer:

db.createUser({user: "your\_user", pwd: "your\_password", roles: [{role: "readWrite", db: "nueva\_base"}],authenticationRestrictions:[{clientSource:[ " XXX.X.X.X ","add\_other\_ip" ],serverAddress:[ " ZZZ.ZZ.ZZZ.Z" ]}]})

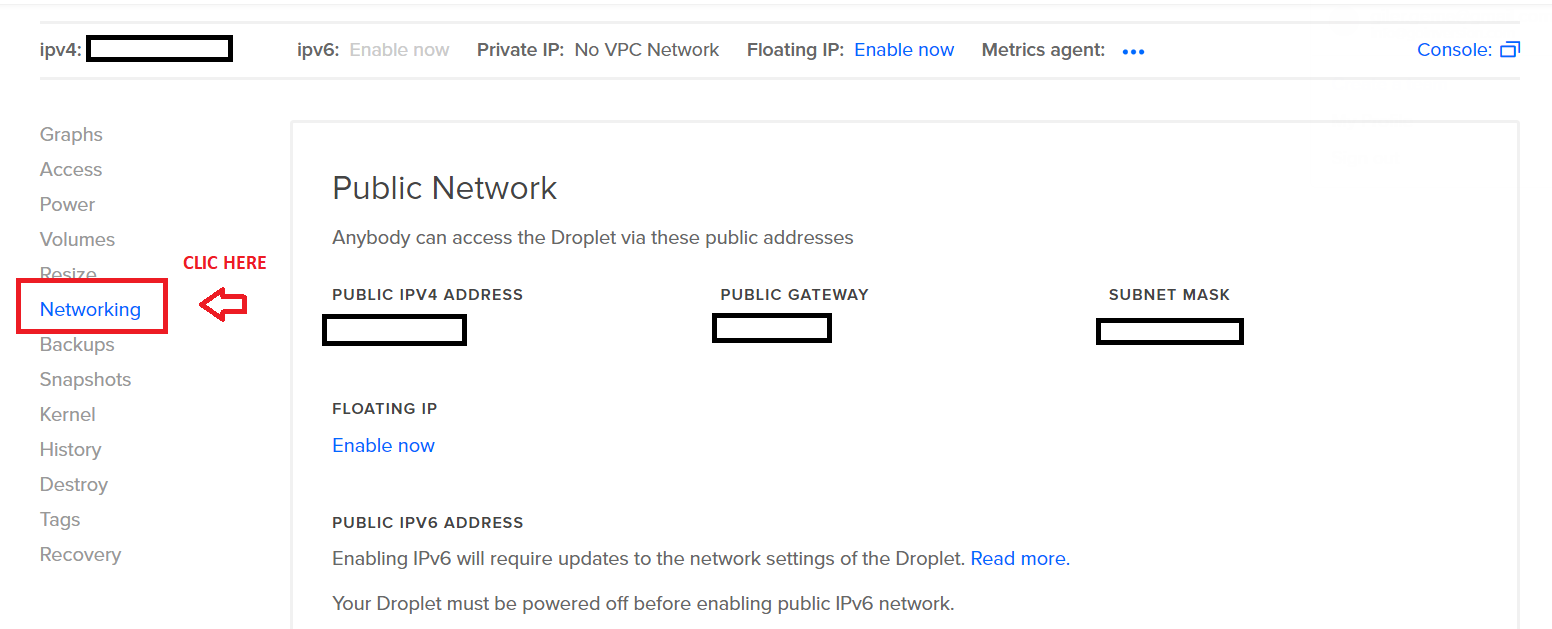
1. **Reiniciamos Mongo**

$ systemctl restart mongod

1. **Agregamos Seguridad por parte del servidor Digital Ocean de la siguiente manera:**

Creamos unas reglas del firewall de la siguiente manera:

Ingresamos al Droplet y damos clic en Networking:



Tenemos un apartado de Firewalls le damos a crear reglas firewall e ingresamos las reglas que necesites para tu servidor, en este caso se agregaron las básicas y en los espacios en blanco de la imagen deberían ir las IP permitidas para poder acceder a tu server y como tal a la base de datos por el puerto anteriormente configurado:

