IBM Process mining sandbox/demo Installation running guide

- Niranjan Talluru

Scope

Sandbox /demo Process mining environment in a single VM/server.

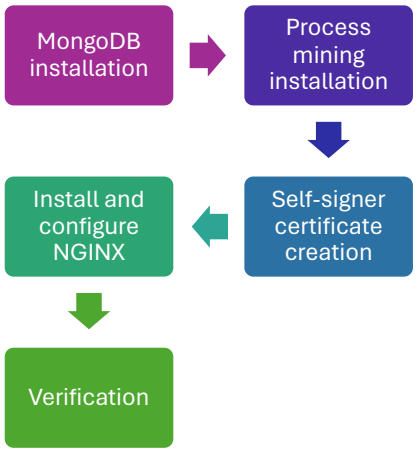
OS : Red Hat Linux 8.x.

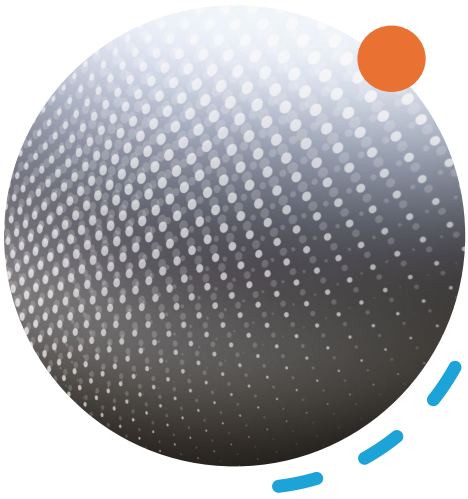
MongoDB (in Same server)

Prerequisites

- OS: Red Hat Linux 8.x
- IBM Process Mining 1.14.3 Server Multiplatform Multilingual (part number M0GXPML)
- DBMS: MongoDB 6.0
- Elevated access to perform installations

Installation Flow





1. MongoDB Installation:

Connect server terminal and execute below commands in sequence.

cd /etc/yum.repos.d
vi mongodb-org-6.0.repo – copy below highlighted script and save the file.

```
[mongodb-org-6.0]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/8/mongodb-org/6.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://pgp.mongodb.com/server-6.0.asc
```

Note: Reference link for the MongoDB script: Click

```
[root@c91314v1 yum.repos.d]# cat mongodb-org-6.0.repo
[mongodb-org-6.0]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/8/mongodb-org/6.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://pgp.mongodb.com/server-6.0.asc
[root@c91314v1 yum.repos.d]#
```

yum install -y mongodb-org
systemctl start mongod
systemctl status mongod

Verification: DB server should be up and Running status as in below.

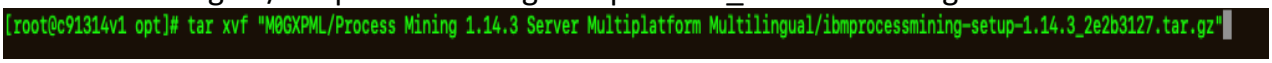
```
[root@c91314v1 yum.repos.d]# systemctl start mongod
[root@c91314v1 yum.repos.d]# systemctl status mongod
● mongod.service - MongoDB Database Server
   Loaded: loaded (/usr/lib/systemd/system/mongod.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2024-03-11 18:20:58 PDT; 13s ago
     Docs: https://docs.mongodb.org/manual
 Main PID: 120589 (mongod)
   Memory: 68.4M
   CGroup: /system.slice/mongod.service
           └─120589 /usr/bin/mongod -f /etc/mongod.conf

Mar 11 18:20:58 c91314v1.fyre.ibm.com systemd[1]: Started MongoDB Database Server.
Mar 11 18:20:58 c91314v1.fyre.ibm.com mongod[120589]: {"t":{"$date":"2024-03-12T01:20:58.851Z"}
```

2. Process Mining installation:

   Execute below commands in server terminal.

   cd /opt
   tar xvf PM1.14.3-apms.tar.gz
   tar xvf "M0GXPML/Process Mining 1.14.3 Server Multiplatform Multilingual/ibmprocessmining-setup-1.14.3_2e2b3127.tar.gz"



3. Self-signer certificate creation:

   Execute below commands in server terminal.

   mkdir /opt/cert
   cd /opt/cert
   vi v3.ext (add below text and save)

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment,
dataEncipherment
subjectAltName = @alt_names
[alt_names]
DNS.1 = pm.processmining
```

   openssl genrsa -des3 -out rootCA.key 2048

   openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem

   openssl req -new -nodes -out server.csr -newkey rsa:2048 -keyout **server.key**

   openssl x509 -req -in **server.csr** -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out **server.crt** -days 500 -sha256 -extfile v3.ext

   cat server.crt **server.key** > **server.pem**

```
[root@c91314v1 cert]# openssl genrsa -des3 -out rootCA.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................+++++
.+++++
e is 65537 (0x010001)
Enter pass phrase for rootCA.key:
Verifying - Enter pass phrase for rootCA.key:
[root@c91314v1 cert]# openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem
Enter pass phrase for rootCA.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:MI
Locality Name (eg, city) [Default City]:Lake Orion
Organization Name (eg, company) [Default Company Ltd]:IBM
Organizational Unit Name (eg, section) []:CSM
Common Name (eg, your name or your server's hostname) []:c91314v1.fyre.ibm.com
Email Address []:
[root@c91314v1 cert]#
```

Reference Link: https://www.ibm.com/docs/en/process-mining/1.14.3?topic=installation-self-certificates

4. Install and configure NGINX server:

Execute below commands in server terminal.

enabled=1
yum install nginx
mkdir /etc/nginx/ssl

cp /opt/cert/**server**.* /etc/nginx/ssl/.
cp /opt/processmining/nginx/processmining.conf /etc/nginx/conf.d/default.conf

vi /etc/nginx/conf.d/default.conf ***(update generated certificate as highlighted)***

```
# dDOS slow-body mitigate attack
#limit_req_zone $binary_remote_addr zone=one:10m rate=30r/m;
#limit_conn_zone $binary_remote_addr zone=addr:10m;

server {
        listen   443 ssl;
        server_name _; #for production environment replace _ with the name of your host
        keepalive_timeout   70;
        server_tokens off;

        ssl on;
        ssl_certificate /etc/nginx/ssl/server.pem;
        ssl_certificate_key /etc/nginx/ssl/server.key;

                ssl_session_timeout 1d;
                ssl_session_cache shared:SSL:50m;
                ssl_session_tickets off;
```

vi /etc/nginx/nginx.conf - Disable http traffic by committing below lines

```
#    server {
#        listen       80 default_server;
#        listen       [::]:80 default_server;
#        server_name  _;
#        root         /usr/share/nginx/html;

       # Load configuration files for the default server block.
#        include /etc/nginx/default.d/*.conf;

#        location / {
#        }

#       error_page 404 /404.html;
#           location = /40x.html {
#        }

#        error_page 500 502 503 504 /50x.html;
#            location = /50x.html {
#        }
#    }
```

chcon -h system_u:object_r:ttpd_config_t /etc/nginx/ssl/**server**.*
service nginx start
setsebool -P httpd_can_network_connect 1

5. Verification:

1. Access application url in browser with DNS / IP address.
   https://<<IPADDRESS>>/index (or) url with dns name
2. Use default credentials as in below to login and verify the application.
   Login process mining
   User Id: maintenance.admin
   Password: pmAdmin$1