Instalación y configuración de OpenSearch

Instalación y configuración de OpenSearch

Para configurar Pandora FMS con OpenSearch consulte "Recolección y monitorización de logs".

Requisitos para el servidor

Es recomendable distribuir a Pandora FMS server y OpenSearch en servidores independientes.

- Rocky Linux 8 / RHEL 8 / Ubuntu 22.04 (sistemas operativos recomendados).
- Mínimo 4 GB RAM (*testing*, *dev*), recomendado 8 GB de RAM por cada instancia de OpenSearch (requisitos mínimos base, para cada entorno y cantidad de datos a procesar y/o almacenar se deberá estimar los requisitos concretos).
- Desactivar SWAP en el nodo o nodos donde esté OpenSearch.
- Mínimo 4 *cores* de CPU (requisitos mínimos base, para cada entorno y cantidad de datos a procesar y/o almacenar se deberá estimar los requisitos concretos).
- 50 GB almacenamiento sistema.
- 100 GB almacenamiento OpenSearch (requisitos mínimos base, para cada entorno y cantidad de datos a procesar y/o almacenar se deberá estimar los requisitos concretos).
- Conectividad desde el Servidor y Consola web de Pandora FMS a la API de OpenSearch (por defecto puerto `9200/TCP`) y entre nodos de *cluster* (por defecto puerto `9300/TCP`).

Con un entorno de un solo nodo con estas características se pueden almacenar hasta 1 GB de datos diarios y almacenarlos durante 30 días. En el caso de requerir una mayor resiliencia de datos, mayor procesamiento y almacenamiento de datos y tolerancia a fallos, será necesario la configuración de un *cluster* de OpenSearch (con un mínimo 3 nodos para garantizar integridad de datos). Al pasar a un entorno de *cluster* también es posible distribuir la carga entre los nodos, duplicando (en el caso de 3 nodos) la capacidad de procesamiento del entorno. Será necesario un sistema de balanceo de carga (Keepalived, por ejemplo) si se quiere trabajar con los diferentes nodos de forma simultánea.

Instalación y configuración de OpenSearch

Documentación oficial de OpenSearch para su instalación:

https://opensearch.org/docs/latest/install-and-configure/install-opensearch/index/

Instalación

Antes de ejecutar OpenSearch en su máquina se debe desactivar la paginación de memoria y

swap en el *host* para mejorar el rendimiento y aumentar el número de mapas de memoria disponibles para OpenSearch. Consulte “Configuraciones importantes” para obtener más información:

https://opensearch.org/docs/latest/install-and-configure/install-opensearch/index/#important-settings

```
 # Disable memory paging and swapping.
sudo swapoff -a

# Edit the sysctl config file that defines the host's max map count.
sudo vi /etc/sysctl.conf

# Set max map count to the recommended value of 262144.
vm.max_map_count=262144

# Reload the kernel parameters.
sudo sysctl -p
```

Para Rocky Linux 8 se recomienda la instalación por medio de paquete RPM.

Listado de paquetes: https://opensearch.org/downloads.html

Documentación oficial de instalación:
https://opensearch.org/docs/latest/install-and-configure/install-opensearch/rpm/

Una vez instalado OpenSearch, desde Pandora FMS se debe comprobar el acceso a OpenSearch. Antes de realizar esta prueba se debe configurar el nodo o clúster. Para dicha comprobación de instalación se debe ejecutar:

```
curl -X GET https://<ip_opoensearch_box>:9200 -u 'admin:admin' --insecure
```

Se debería obtener una respuesta similar a:

```
{
   "name" : "hostname",
   "cluster_name" : "opensearch",
   "cluster_uuid" : "6XNc9m2gTUSIoKDqJit0PA",
   "version" : {
      "distribution" : "opensearch",
      "number" : <version>,
      "build_type" : <build-type>,
      "build_hash" : <build-hash>,
      "build_date" : <build-date>,
      "build_snapshot" : false,
      "lucene_version" : <lucene-version>,
      "minimum_wire_compatibility_version" : "7.10.0",
      "minimum_index_compatibility_version" : "7.0.0"
   },
```

```
    "tagline" : "The OpenSearch Project: https://opensearch.org/"
 }
```

Por defecto, la instalación de OpenSearch habilita SSL, usuario y contraseña lo cual es una buena práctica; se recomienda cambiar el usuario y la contraseña que vienen por defecto.

Configuración de nodo

Primero se debe editar el fichero de configuración `/etc/opensearch/opensearch.yml` y después se reiniciará el servicio OpenSearch.

Este fichero contiene la configuración de todos los parámetros del servicio de OpenSearch; consulte la documentación oficial para más información:

https://opensearch.org/docs/latest/install-and-configure/configuration/

Configuraciones mínimas necesarias para iniciar el servicio y su uso con Pandora FMS.

- Número de puerto.

```
# ---------------------------------- Network
# Set the bind address to a specific IP (IPv4 or IPv6):
network.host: 0.0.0.0
# Set a custom port for HTTP:
http.port: 9200
# For more information, consult the network module documentation.
```

- Ubicación de los datos almacenados y *logs*:

```
# ---------------------------------- Paths
# Path to directory where to store the data (separate multiple locations by
comma):
path.data: /var/lib/opensearch
# Path to log files:
path.logs: /var/log/opensearch
```

También será necesario *descomentar* y definir las siguientes líneas:

```
cluster.name: pandorafms
node.name: ${HOSTNAME}
network.host: 0.0.0.0
```

- `cluster.name`: Será el nombre que recibirá el grupo o *cluster*.
- `node.name`: Para nombrar el nodo utilizando la variable de sistema `${HOSTNAME}`, este tomará automáticamente el nombre del anfitrión.
- Para `network.host` el valor `0.0.0.0` permite que OpenSearch “escuche” en todas las interfaces de

red (NIC); *para utilizar una NIC específica coloque un valor específico correspondiente*.

Si se trabaja con un único nodo se debe añadir al fichero de configuración la linea para que permita el inicio de *single node*:

```
discovery.type: single-node
```

En caso de trabajar con un *cluster* necesita completar el parámetro `discovery.seed_hosts`:

```
discover.seed_hosts : ["ip:port", "ip", "ip"]
```

En las versiones más recientes de OpenSearch la gestión de la memoria la máquina virtual Java® se hace de forma automática y se recomienda dejar que se gestione de esta forma en entornos de producción, por lo que es innecesario modificar los valores de la JVM.

Para iniciar OpenSearch se debe ejecutar:

```
systemctl start opensearch.service
```

Para reiniciar use `restart`, para detener `stop` y `status` para consultar el estado.

Si el servicio no se inicia, revise los *logs* ubicados en `/var/log/opensearch/` (en este caso el fichero `pandorafms.log` o el nombre dado al nodo).

Recuerde que para comprobar la instalación y funcionamiento de OpenSearch se puede ejecutar:

```
curl -X GET https://<node-ip> -u 'admin:admin' --insecure
```

Configuración de un clúster OpenSearch

Para la configuración de un *cluster* de OpenSearch se debe seguir la documentación oficial:

https://opensearch.org/blog/optimize-opensearch-index-shard-size/

Gestión de usuarios OpenSearch

Para cambiar la contraseña por defecto de `admin` se deben seguir una serie de pasos. Lo primero

es exportar la variable para usar el JDK de Java® instalado por OpenSearch para usar cualquiera de las herramientas:

```
export OPENSEARCH_JAVA_HOME=/usr/share/opensearch/jdk
```

Luego para generar la contraseña con *hash* a colocar en el fichero de configuración de OpenSearch se utiliza el siguiente *script* (sustituya `< password >` por la contraseña a utilizar):

```
/usr/share/opensearch/plugins/opensearch-security/tools/hash.sh -p <password>
```

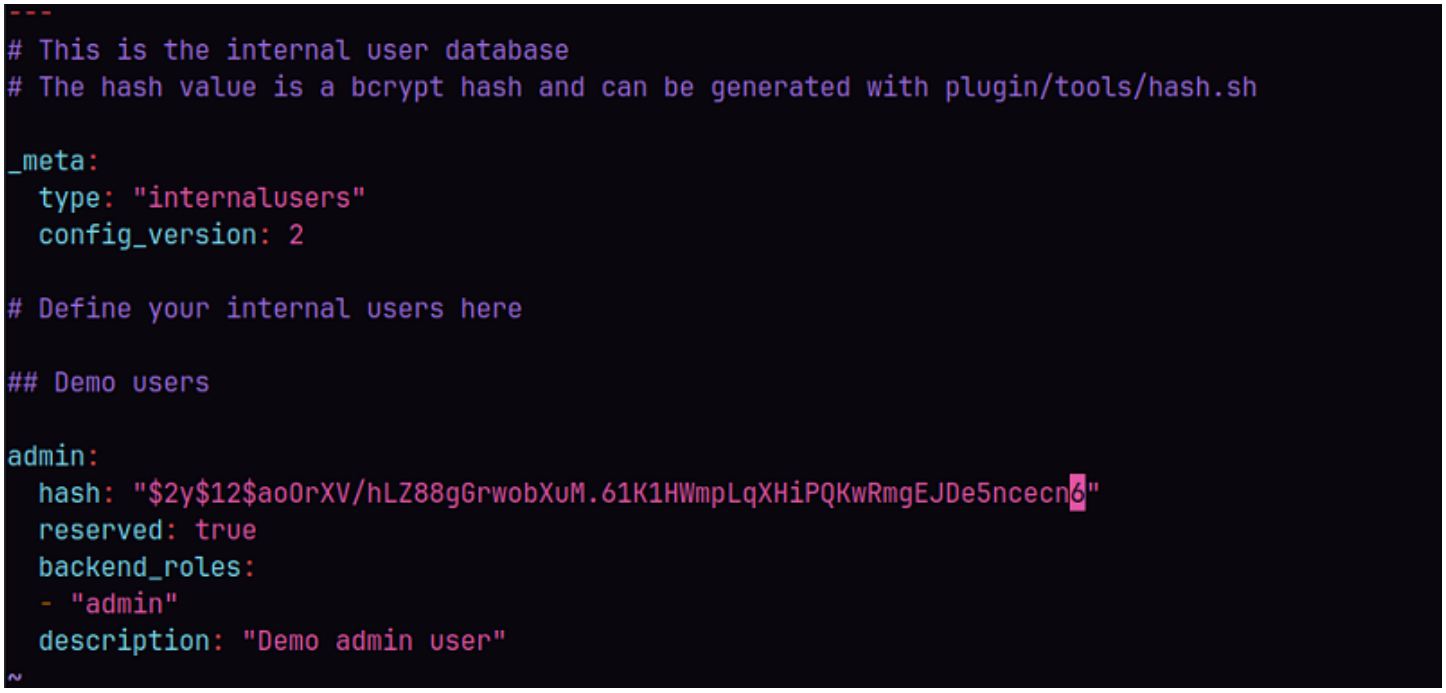
Por ejemplo:

```
[root@test ~]# /usr/share/opensearch/plugins/opensearch-security/tools/hash.sh -p pandora
************************************************************************
** This tool will be deprecated in the next major release of OpenSearch **
** https://github.com/opensearch-project/security/issues/1755           **
************************************************************************
$2y$12$aoOrXV/hLZ88gGrwobXuM.61K1HWmpLqXHiPQKwRmgEJDe5ncecn6
```

Luego se debe abrir el fichero `/etc/opensearch/opensearch-security/internal_users.yml` con el editor de texto vim o nano para modificar la contraseña del usuario o usuarios requeridos.

Se recomienda dejar solamente el usuario `admin` para el uso con Pandora FMS, es innecesario mantener a cualquier otro usuario.

Fichero de ejemplo:



```
---
# This is the internal user database
# The hash value is a bcrypt hash and can be generated with plugin/tools/hash.sh

_meta:
  type: "internalusers"
  config_version: 2

# Define your internal users here

## Demo users

admin:
  hash: "$2y$12$aoOrXV/hLZ88gGrwobXuM.61K1HWmpLqXHiPQKwRmgEJDe5ncecn6"
  reserved: true
  backend_roles:
  - "admin"
  description: "Demo admin user"
~
```

Para hacer efectivos los cambios debe ejecutarse:

```
cd /usr/share/opensearch/plugins/opensearch-security/tools
```

```
OPENSEARCH_JAVA_HOME=/usr/share/opensearch/jdk ./securityadmin.sh -cd
/etc/opensearch/opensearch-security/ -cacert /etc/opensearch/root-ca.pem -cert
/etc/opensearch/kirk.pem -key /etc/opensearch/kirk-key.pem -icl -nhnv-t
internalusers   -icl   -nhnv   -cacert /etc/opensearch/root-ca.pem   -cert
/etc/opensearch/kirk.pem   -key /etc/opensearch/kirk-key.pem
```

Se debe visualizar un mensaje final `Done with success`; para comprobar la nueva contraseña (siguiendo el ejemplo anterior con `pandora` utilizada):

```
❯ curl https://10.235.50.104:9200 -ku 'admin:pandora'
{
  "name" : "node-1",
  "cluster_name" : "my-application",
  "cluster_uuid" : "3MDB9QFtS5OBPhK9AWn6Yg",
  "version" : {
    "distribution" : "opensearch",
    "number" : "2.11.0",
    "build_type" : "rpm",
    "build_hash" : "4dcad6dd1fd45b6bd91f041a041829c8687278fa",
    "build_date" : "2023-10-13T02:56:26.505314582Z",
    "build_snapshot" : false,
    "lucene_version" : "9.7.0",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
```

Para más información de gestión de usuarios en OpenSearch:

- https://opensearch.org/docs/latest/security/configuration/yaml/
- https://opensearch.org/docs/latest/security/access-control/users-roles/#create-users

Configuración de Pandora FMS con OpenSearch

Para configurar Pandora FMS con OpenSearch consulte el tema "Recolección y monitorización de logs".

Modelos de datos y plantillas

Antes de poner en producción un entorno, bien sea de un solo nodo o un clúster de datos, se recomienda aplicar las configuraciones correspondientes a este nodo o clúster en función a su utilización. En el caso de los índices generados por Pandora FMS la forma más efectiva de hacerlos es definiendo una plantilla (*template*) para definir la configuración de los campos y los datos almacenados.

Las *templates* son configuraciones que solo se aplican en el momento de la creación del índice. Cambiar un *template* no tendrá ningún impacto en los índices ya existentes.

Para crear un *template* básico, solo debe definir los siguientes campos:

```
curl -X PUT -ku 'admin:admin' https://<node_ip>:9200/_index_template/pandorafms
-H 'Content-Type: application/json' -d'
{
 "index_patterns": [
   "pandorafms*"
 ],
 "template": {
   "aliases": {
     "pandorafms_logs": {}
   },
   "settings": {
     "number_of_shards": 1,
     "auto_expand_replicas" : "0-1",
     "number_of_replicas": "0"
   },
"mappings" : {
    "properties" : {
      "agent_id" : {
        "type" : "long"
      },
      "group_id" : {
        "type" : "long"
      },
      "group_name" : {
        "type" : "text"
      },
      "logcontent" : {
        "type" : "text"
      },
      "source_id" : {
        "type" : "text"
      },
      "suid" : {
        "type" : "text"
      },
      "type" : {
        "type" : "text"
      },
      "utimestamp" : {
        "type" : "long"
      },
      "@timestamp": {
         "type": "date"
       }
    }
  }
}
}
'
```

A través de la interfaz de Pandora FMS (menú) podrá subir dicho *template*:

- PUT _template/<nombredeltemplate>: en este ejemplo `PUT _template/pandorafms` .

También podrá consultar los *templates* por la misma interfaz de Pandora FMS:

- GET _template/<nombredeltemplate>: en este ejemplo `GET _template/pandorafms` .

Templates multinodo

Para definir un *template* multinodo debe tener en cuenta la siguiente información:

- Cuando realice la configuración del *template* (formato JSON), necesita configurar tantos *shards* como nodos tenga, sin embargo para configurar correctamente las réplicas debe restar 1 al número de nodos del entorno.

Por ejemplo, en un entorno de Pandora FMS con 3 nodos configurados, cuando modifique los campos `number_of_shards` y `number_of_replicas` deberá quedar de la siguiente manera:

```
{
 "index_patterns": ["pandorafms*"],
 "settings": {
   "number_of_shards": 3,
   "auto_expand_replicas" : "0-1",
   "number_of_replicas" : "2"
 },
```

Desde la línea de comando puede listar los *templates* del entorno ejecutando:

```
curl -X GET "localhost:9200/_cat/templates/*?v=true&s=name&pretty"
```

También puede ver los detalles de un *template*, por ejemplo, creado para `pandorafms` ,ejecutando:

```
curl -X GET "localhost:9200/_template/pandorafms*?pretty"
```

el cual devolverá en formato JSON la configuración que tenga definida.

Puede realizar estas operaciones a través de la interfaz de Pandora FMS:

- PUT _template/<nombre_del_template> {json_data}: permite introducir los datos del *template* a crear.
- GET _template/><nombre_del_template>: permite visualizar el *template* creado.

Para configurar Pandora FMS con OpenSearch consulte “Recolección y monitorización de logs”.

Volver al índice de documentación de Pandora FMS