Elasticsearch Backup and Restore

Elasticsearch Backup and Restore

From NG 774 version, Pandora FMS incorporates OpenSearch for *log* monitoring, this topic is only valid for version 773 or previous versions.

Data migration from an Elasticsearch server using snapshots is relatively quick. First, the server data is backed up and then stored in a repository for later restoration.

Create backup copy

The machine to be backed up is called the “source machine” and the machine to be restored is called the “target machine”.

- On the source machine

Modify the configuration file `elasticsearch.yml`:

```
vi /etc/elasticsearch/elasticsearch.yml
```

Add the following line:

```
path.repo: /usr/local/var/backups/
```

Create the directory previously added to the configuration file:

```
mkdir -p /usr/local/var/backups/
```

Grant reading and writing permissions to directory and user:

```
chmod 700 /usr/local/var/backups
chown elasticsearch:elasticsearch /usr/local/var/backups
```

Restart the service:

```
/etc/init.d/elasticsearch restart
```

Back up:

```
curl -XPUT http://localhost:9200/_snapshot/my_backup -d '{"type": "fs",
"settings": {"compress": "true", "location": "/usr/local/var/backups/"}}}'
```

Compress the backup:

```
cd /usr/local/var/
tar -zcvf elastic_backup.tar.gz backups/
```

Copy the compressed backup of the source machine from the target machine.

```
scp -P 41122 root@<dir_ip_origin>:/root/elastic_backup.tar.gz /home/user/backup
```

- To use the scp command, an SSH server must be installed on the source machine and at least one SSH client must be installed on the target machine.
- It is important for the version of Elasticsearch on the target machine to support the data export, i.e. in this case the source machine must have the same version or a higher one. If not, first upgrade Elasticsearch on the target machine.

Restore Backup

- On the target machine

Modify the configuration file `elasticsearch.yml` in the same way as in create backup on the source machine:

```
vi /etc/elasticsearch/elasticsearch.yml
```

Add the following line:

```
path.repo: /usr/local/var/backups/
```

Create the directory previously added to the configuration file:

```
mkdir -p /usr/local/var/backups/
```

Grant reading and writing permissions to the directory:

```
chmod 700 /usr/local/var/backups
chown elasticsearch:elasticsearch /usr/local/var/backups
```

Restart the service:

```
/etc/init.d/elasticsearch restart
```

Unzip the backup imported from the source machine:

```
tar -xzvf /home/user/backup/elastic_backup.tar.gz -C /usr/local/var/backups
```

Create the repositories where the snapshots are located:

```
curl -X PUT "localhost:9200/_snapshot/my_backup" -H 'Content-Type:
application/json' -d'

{
  "type": "fs",
  "settings": {
    "location": "/usr/local/var/backups"
  }
}
'
```

Close the indexes:

```
curl -XPOST http://localhost:9200/< indexes_names >-*/_close
```

The asterisk shows all indexes starting with that name, `< indexes_names >`.

Import the backup, first copy the backup to the repository:

```
cp <name_snapshot.dat> my_backup_location/
```

Rename the file without capital letters:

```
mv my_backup_location/<name_snapshot.dat> my_backup_location/snap1
```

Finally, it is imported:

```
curl -X POST
"localhost:9200/_snapshot/my_backup/snap1/_restore?wait_for_completion=true"
```

Finally, reopen the indexes:

```
curl -XPOST http://localhost:9200/< indexes_names >-*/_open
```

Back to Pandora FMS Documentation Index