PANDORAFMS

Sauvegarde et restauration d'Elasticsearch

Sauvegarde et restauration d'Elasticsearch

À partir de la version NG 774, Pandora FMS incorpore OpenSearch pour la supervision des *logs*, cette rubrique n'est valable que pour la version 773 ou les versions antérieures.

La migration des données d'un serveur Elasticsearch via *snapshots* est relativement rapide. Les données du serveur sont d'abord sauvegardées, puis stockées dans un référentiel en vue d'une restauration ultérieure.

Créer une copie de sauvegarde

La machine sur laquelle la *sauvegarde* sera effectuée est appelée « machine source » et la machine sur laquelle la restauration sera effectuée est appelée « machine cible ».

- Sur la machine d'origine

Modifier le fichier de configuration `elasticsearch.yml` :

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

Ajoutez la ligne suivante :

```

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

Créez le répertoire ajouté au fichier de configuration ci-dessus :

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

Accordez les droits de lecture et d'écriture au répertoire et à l'utilisateur :

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

Redémarrez le service :

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

Crééz la sauvegarde :

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

Compressez la sauvegarde :

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

Sur la machine cible, copiez la sauvegarde compressée de la machine source.

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

- Pour utiliser la commande scp, un serveur SSH doit être installé sur la machine source et au moins un client SSH doit être installé sur la machine cible.
- Il est important que la version d'Elasticsearch sur la machine cible soit compatible avec l'exportation de données, c'est-à-dire que dans ce cas la machine source doit avoir la même version ou une version supérieure. Si ce n'est pas le cas, vous devez d'abord mettre à jour Elasticsearch sur la machine cible.

Restaurer la sauvegarde

- Sur la machine cible

Modifiez le fichier de configuration `elasticsearch.yml` de la même manière que sur créer la sauvegarde sur la machine source :

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

Ajoutez la ligne suivante :

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

Créez le répertoire ajouté ci-dessus au fichier de configuration :

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

Accordez les droits de lecture et d'écriture au répertoire :

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

Redémarrez le service :

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

Décompressez le fichier *backup* importé de la machine source :

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

Créez les référentiels dans lesquels les *snapshots* :

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

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

Fermez les index :

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

L'astérisque indique tous les index commençant par ce nom, `< indexes_names >`.

Importez la sauvegarde, d'abord copiez la sauvegarde dans le référentiel :

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

Renommez le fichier sans majuscules :

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

Enfin, importez-le :

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

Enfin, rouvrez les index :

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

Retour à l'index de la documentation de Pandora FMS