



# Elastic Search バックアップ



m:  
<https://pandorafms.com/manual/!776/>  
permanent link:  
[https://pandorafms.com/manual/!776/ja/documentation/pandorafms/technical\\_annexes/16\\_elastic\\_search\\_backup](https://pandorafms.com/manual/!776/ja/documentation/pandorafms/technical_annexes/16_elastic_search_backup)  
2024/06/10 14:34





# Elastic Search バックアップ

[Pandora FMS ドキュメント一覧に戻る](#)

## ElasticSearch のバックアップとリストア (ELK)

スナップショットを使用した ElasticSearch サーバからのデータ移行は比較的高速です。まず、サーバのデータのバックアップが作成され、後で復元するためにリポジトリに保存されます。

### スナップショット

バックアップが行われるマシンは“ソースマシン”と呼ばれ、復元が行われるマシンは“ターゲットマシン”と呼ばれます。

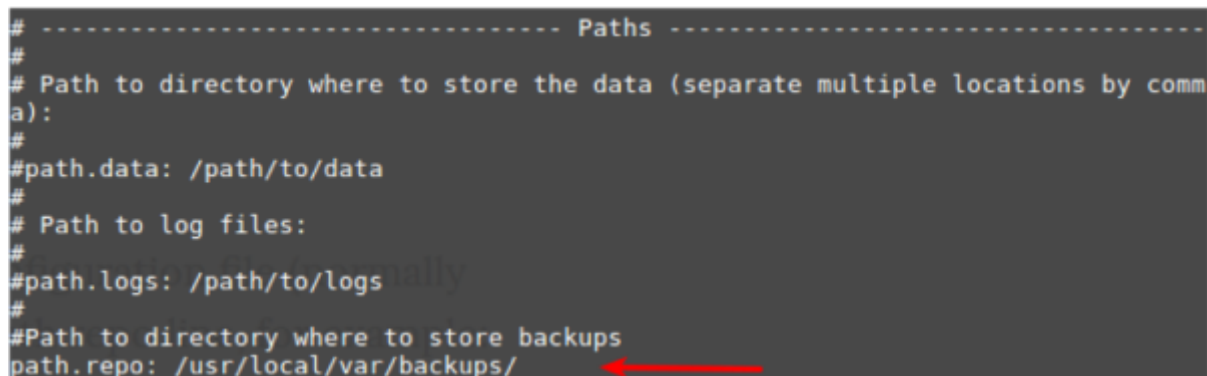
- ソースマシンにて

1) 設定ファイル“elasticsearch.yml”を編集します。

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

次の行を追加します。

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



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

2) 設定ファイルに追記したディレクトリを作成します。

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

3) ディレクトリのパーミッションとユーザを設定します。

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

4) サービスを再起動します。

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

5) 次のコマンドでバックアップを作成します。

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

6) 生成されたバックアップをアーカイブファイルにします。

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

7) リストアを行うターゲットマシンへ、ソースマシンのバックアップファイルをコピーします。

- ターゲットマシンにて

```
scp -P 41122 root@<ip0rigen>:/root/elastic_backup.tar.gz /home/user/backup
```

'scp' コマンドを利用するには、ソースマシンに ssh サーバがインストールされ、ターゲットマシンに ssh クライアントがインストールされている必要があります。

インポートするマシンの Elasticsearch のバージョンがデータのエクスポートをサポートしていることが重要です。上記の例では、ターゲットマシンの Elasticsearch はソースマシンと同じもしくはそれ以上のバージョンである必要があります。そうでなければ、最初に Elasticsearch をアップデートする必要があります。

## バックアップのリストア

- ターゲットマシンにて

1) ソースマシンでバックアップを作成するときに行ったのと同じように、設定ファイルの "elasticsearch.yml" を編集します。

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

次の行を追加します。

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

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

2) 設定ファイルに追記したディレクトリを作成します。

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

3) ディレクトリのパーミッションとユーザを設定します。

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

4) サービスを再起動します。

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

5) ソースマシンからコピーしたバックアップを展開します。

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

6) スナップショットがある場所でリポジトリを作成します。

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

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

7) インデックスを閉じます。

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

アスタリスクは、その名前ですべてのインデックスを示します。

8) バックアップをインポートします。

最初に、バックアップをリポジトリへコピーします。

```
cp <name of the snapshot.dat> my_backup_location/
```

大文字を使わずにファイル名を変更します。

```
mv my_backup_location/<name of snapshot.dat> my_backup_location/snap1
```

以下が重要です。

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

9) 最後に、インデックスを再度開きます。

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

[Pandora FMS ドキュメント一覧に戻る](#)