Elasticsearch クラスタ設定

Elasticsearch クラスタ設定

Pandora FMS ドキュメント一覧に戻る

前提条件

- まず最初に 各ノードでインストールと設定手順 を行う必要があります。
- Elasticsearch クラスターの最小サイズは 3ノードであり、*quorum* システムを利用してデータの整合性を保証するには、常に奇数で増やす必要があります。
- 3つのノードすべての間で通信が可能であり、各ノード間でポート 9200 および 9300 へアクセスできることを確認してください。

これらのポート番号を介した接続を許可するように、各ノードのファイアウォールの設定を忘れないでください。

設定

全ノードの Elasticsearch サービスを停止します。

```
systemctl stop elasticsearch.service
```

設定ファイル `/etc/elasticsearch/elasticsearch.yml` の以下の行を編集します。

```
#discovery.seed_hosts: ["host1", "host2"]
#cluster.initial_master_nodes: ["host1", "host2"]
```

該当行を ***コメントアウト*** し、各ノードの IP アドレスまたは URL を追加します。

```
discovery.seed_hosts: ["host1", "host2", "host3"]
cluster.initial_master_nodes: ["host1", "host2", "host3"]
```

IP アドレスでの例:

```
discovery.seed_hosts: ["172.42.42.101", "172.42.42.102", "172.42.42.103"]
cluster.initial_master_nodes: ["172.42.42.101", "172.42.42.102",
"172.42.42.103"]
```

`cluster.initial_master_nodes` の行は設定ファイル内で 1回のみ定義されていることを確認してください。場合によっては、同じ行が同じファイルの異なる 2つの場所に表示されます。

ノードは初回に単独で(スタンドアロンで)開始されたため、サービスを開始する前にデータフォルダーの内容(デフォルトでは /var/lib/elasticsearch/)を削除する必要があります。 次のコマンドを実行します。

```
rm -rf /var/lib/elasticsearch/*
```

次に、すべてのノードでサービスを開始します。 次のコマンドで開始し、実行されていることを確認します。

```
systemctl start elasticsearch.service && systemctl status elasticsearch.service
```

次のような出力を得られます。

```
[root@rocky8-node1 ~]# systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; disabled; vendor preset: disabled)
   Active: active (running) since Thu 2022-05-12 08:23:05 UTC; 49s ago
     Docs: https://www.elastic.co
 Main PID: 3334 (java)
    Tasks: 67 (limit: 11401)
   Memory: 1.3G
   CGroup: /system.slice/elasticsearch.service
           ├─3334 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60
           └─3619 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

May 12 08:22:53 rocky8-node1 systemd[1]: Starting Elasticsearch...
May 12 08:23:05 rocky8-node1 systemd[1]: Started Elasticsearch.
lines 1-13/13 (END)
```

サービスが開始されたら、3つのノードがクラスターに正しく参加していることを確認する必要があります。任意のノードで次のコマンドを実行すると、同じ応答が返されます。

```
curl -XGET http://127.0.0.1:9200/_cat/nodes
```

```
[root@rocky8-node1 ~]# curl -XGET http://127.0.0.1:9200/_cat/nodes
172.42.42.102 46 89 3 0.16 0.23 0.17 cdfhilmrstw - rocky8-node2
172.42.42.103 39 90 3 0.48 0.17 0.12 cdfhilmrstw * rocky8-node3
172.42.42.101 15 93 0 0.00 0.00 0.00 cdfhilmrstw - rocky8-node1
[root@rocky8-node1 ~]#
```

ノードがポート 9200 および 9300 を介して通信する必要があることに加えて、Pandora FMS サーバおよび Pandora FMS Web コンソールからポート 9200 へアクセスできる必要があることを常に考慮してファイアウォールの設定を再度確認してください。ここまでの設定により、Pandora FMS ログストレージエンジンとして使用される Elasticsearch クラスターの準備が完了です。

データモジュールとテンプレート

単一ノードまたはデータクラスターのいずれかを本番環境に導入する前に、用途に応じて、対応する設定をこのノードまたはクラスターに適用することをお勧めします。 Pandora FMS によって生成されたインデックスの場合、それを行う最も簡単な方法は、フィールドと保存されたデータの構成を定義するためのテンプレートを定義することです。

テンプレートは、インデックスの作成時にのみ適用される設定です。 テンプレートを変更しても、既存のインデックスには影響しません。

- 基本テンプレート を作成するには、ノードのデータモデルとテンプレート の手順に従います。
- マルチノードテンプレート を定義するには、次の情報を考慮する必要があります。
    - テンプレート(JSON 形式)を設定する場合、ノードと同じ数の検索を設定する必要がありますが、レプリカを正しく設定するには、環境内のノードの数から 1を引く必要があります。

たとえば、3つのノードで構成された Elasticsearch を使用する Pandora FMS 環境では、number_of_search フィールドと number_of_replicas フィールドを次のように変更します。

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

これは非常に基本的な定義です。Elasticsearch 環境のサイズを正しく定義するには、この記事で説明している要素を考慮に入れることをお勧めします。

- https://www.elastic.co/blog/how-many-shards-should-i-have-in-my-elasticsearch-cluster

コマンドラインから、以下を実行して環境のテンプレートを一覧表示できます。

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

テンプレートの詳細を表示することもできます。たとえば、pandorafms 用に作成したテンプレートは次のようにして表示できます。

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

定義した設定を JSON 形式で返します。

これらの操作は、ネイティブの Elasticsearch コマンドを使用して Pandora FMS の Elasticsearch インターフェースから実行できます。

- PUT _template/<template_name> {json_data}: 作成するテンプレートのデータを入力できます。
- GET _template/><template_name>: 作成したテンプレートを表示できます。

Elasticsearch Interface

WARNING

This is a view to interface with Elasticsearch directly from WEB console. Please note that you can damage your Elasticsearch if you don`t know exactly what are you are doing. This view is intended to be used only by users with a knowledge of Elasticsearch .

Query

```
1  GET _template/pandorafms
```

Results


```
{
  "pandorafms": {
    "order": 0,
    "index_patterns": [
      "pandorafms*"
    ],
    "settings": {
      "index": {
        "number_of_shards": "1",
        "auto_expand_replicas": "0-1",
        "number_of_replicas": "0"
      }
    },
    "mappings": {
      "properties": {
        "agent_id": {
          "type": "long",
          "fields": {
            "keyword": {
              "ignore_above": 256,
              "type": "keyword"
            }
          }
        },
        "group_id": {
          "type": "long",
          "fields": {
            "keyword": {
              "ignore_above": 256,
              "type": "keyword"
            }
          }
        },
        "group_name": {
          "type": "text",
          "fields": {
            "keyword": {
              "ignore_above": 256,
              "type": "keyword"
            }
          }
        },
        "utimestamp": {
          "type": "long"
        },
        "source_id": {
          "type": "text",
          "fields": {
            "keyword": {
              "ignore_above": 256,
              "type": "keyword"
            }
          }
        },
        "suid": {
          "type": "text",
          "fields": {
```


Execute query

Pandora FMS ドキュメント一覧に戻る