OpenSearch のインストールと設定

OpenSearch のインストールと設定

OpenSearch を使用した Pandora FMS 設定は、「ログの収集と監視」を参照してください。

サーバ要件

Pandora FMS サーバと OpenSearch を独立したサーバに分散することをお勧めします。

- Rocky Linux 8 / RHEL 8 / Ubuntu 22.04 (推奨オペレーティングシステム)
- 最小 4 GB RAM (テスト、開発)OpenSearch インスタンスごとに 8 GB の RAM を推奨 (最小基本要件、各環境および処理または保存されるデータ量に応じて、特定の要件を見積もる必要があります)。
- OpenSearch を動作させるノードでは SWAP を無効にします。
- 最小 4 つの CPU コア (最小基本要件。各環境および処理または保存されるデータ量に応じて、特定の要件を見積もる必要があります)。
- 50 GB システムストレージ。
- 100 GB OpenSearch ストレージ (最小基本要件。各環境および処理または保存されるデータ量に応じて、特定の要件を見積もる必要があります)。
- Pandora FMS サーバおよび Web コンソールから OpenSearch API (デフォルトポート 9200/TCP) およびクラスタノード間の接続 (デフォルトポート 9300/TCP)

これらの機能を備えた単一ノード環境では、1 日あたり最大 1 GB のデータを保存でき、30 日間保存できます。 より優れたデータ復元力、より優れたデータ処理とストレージ、およびフォールトトレランスが必要な場合は、OpenSearch クラスターの構成が必要になります (データの整合性を保証するには、少なくとも 3 つのノードが必要です)。 クラスタ環境に切り替えることでノード間の負荷分散も可能となり、環境の処理能力は2倍（3ノードの場合）となります。 異なるノードを同時に使用する場合、負荷分散システムが必要になります (Keepalived など)。

OpenSearch のインストールと設定

インストールに関する OpenSearch の公式ドキュメント:

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

インストール

マシン上で OpenSearch を実行する前に、パフォーマンスを向上させOpenSearch で使用できるメモリマップの数を増やすために、ホスト上のメモリページングとスワップを無効にする必要があります。 詳細については“Important Settings” を参照してください。

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
```

Rocky Linux 8 の場合は、RPM パッケージでのインストールをお勧めします。

パッケージ一覧: https://opensearch.org/downloads.html

公式インストールドキュメント:
https://opensearch.org/docs/latest/install-and-configure/install-opensearch/rpm/

OpenSearch をインストールしたら、Pandora FMS から OpenSearch へのアクセスを確認する必要があります。 このテストを実行する前に、ノードまたはクラスタを設定する必要があります。 このインストールチェックでは、次のコマンドを実行します。

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

次のような応答が返ります。

```
{
   "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/"
}
```

デフォルトでは OpenSearch のインストールでは SSL ユーザ名、パスワードが有効になっており、これが推奨事項です。 デフォルトのユーザ名とパスワードを変更することをお勧めします。

ノード設定

まず設定ファイル /etc/opensearch/opensearch.yml を編集します。その後、OpenSearch サービスを再起動します

このファイルには OpenSearch サービスのすべてのパラメータ設定が含まれています。 詳細については、公式ドキュメントを参照してください。

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

サービスを開始して Pandora FMS で使用するために必要な最低限の設定。

- ポート番号

```
# ---------------------------------- 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.
```

- データおよびログの保存場所

```
# ---------------------------------- 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
```

次の行のコメントを外して定義することも必要になります。

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

- cluster.name: これは、グループまたはクラスタの名前になります。
- node.name: ${HOSTNAME} システム変数を使用してノードに名前を付けると、ホストの名前が自動的に取得されます。
- network.host の値 0.0.0.0 により OpenSearch はすべてのネットワークインターフェイス (NIC) で待ち受けできます。 特定の NIC を使用するには、対応する特定の値を入力します。

単一ノードを使用する場合は、設定ファイルに次の行を追加して、単一ノードが起動できるように

します。

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

クラスターを使用する場合は、discovery.seed_hosts パラメータを設定する必要があります。

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

OpenSearch の最新バージョンでは Java® 仮想マシンのメモリ管理は自動的に行われ、実稼働環境ではこの方法で管理することをお勧めします。そのため JVM 値を変更する必要はありません。

OpenSearch を開始するには、次のように実行します。

```
systemctl start opensearch.service
```

再起動には restart、停止には stop、状態を確認するには status を使用します。

サービスが開始しない場合は、/var/log/opensearch/ にあるログ (この場合はファイル pandorafms.log または ノードに指定された名前) を確認してください。

OpenSearch のインストールと動作の確認は、次のコマンドで行なえます。

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

OpenSearch クラスタのセットアップ

OpenSearch クラスタを設定するには、公式ドキュメントに従ってください。

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

OpenSearch ユーザ管理

デフォルトのパスワードを admin から変更するには、一連の手順に従う必要があります。 まず OpenSearch によってインストールされた Java® JDK を使用していずれかのツールを使用できるように変数をエクスポートします。

```

```

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

次に、ハッシュ化されたパスワードを生成して OpenSearch 設定ファイルに配置するために、次のスクリプトを使用します (< password > を使用するパスワードに置き換えます)。

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

例:

```
[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
```

次に、テキストエディタ vim または nano でファイル /etc/opensearch/opensearch-security/internal_users.yml を開き、必要なユーザのパスワードを変更します。

Pandora FMS で使用するために admin ユーザのみを残すことをお勧めします。他のユーザを維持する必要はありません。

ファイル例:

```
---
# 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"
~
```

変更を有効にするには、以下を実行する必要があります。

```
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
```

最後のメッセージ Done with success が表示されます。 新しいパスワードを確認するには (pandora を使用した前の例に従って) 次のようにします:

```
❯ 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/"
}
```

OpenSearch でのユーザ管理の詳細については、以下を参照してください。

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

OpenSearch を使用する Pandora FMS 設定

OpenSearch を使用するように Pandora FMS を設定するには、“ ログ収集と監視 ”を参照してください。

データモデルとテンプレート

本番環境に設定する前に、それが単一ノードであってもデータクラスタであっても、その用途に基

づいてこのノードまたはクラスタに対応する設定を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、最も効果的な方法は、フィールドと保存されたデータの設定を定義する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、次のフィールドを定義するだけで済みます。

```
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"
         }
      }
    }
}
}
'
```

Pandora FMS (メニュー) インターフェイスを通じて、上記のテンプレートをアップロードできます。

- PUT _template/<templatename>: この例では、 PUT _template/pandorafms です。

Pandora FMS インターフェイス自体を通じてテンプレートを確認することもできます。

- GET _template/<templatename>: この例では、 GET _template/pandorafms です。

複数ノードテンプレート

複数ノードテンプレートを定義するには、次の情報を考慮してください。

- テンプレート (JSON 形式) を設定する場合、存在するノードと同じ数のシャードを設定する必要があります。ただし、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 を減算します

たとえば、3 つのノードが設定された Pandora FMS 環境で、number_of_shards フィールドと number_of_replicas フィールドを変更すると、次のようになります。

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

コマンドラインから次のコマンドを実行して、環境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"
```

次のコマンドを実行すると、たとえば pandorafms 用に作成されたテンプレートの詳細を確認することもできます。

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

これにより、定義した設定が JSON 形式で返されます。

これらの操作は、Pandora FMS インターフェイスを通じて実行できます。

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

OpenSearch を使うように Pandora FMS を設定するには、“ ログ収集と監視 ”を参照してください。

Pandora FMS ドキュメント一覧に戻る