Installation et configuration d'OpenSearch

Installation et configuration d'OpenSearch

Pour configurer Pandora FMS avec OpenSearch, voir « Collecte et surveillance des journaux ».

Configuration requise pour le serveur

Il est conseillé de distribuer le serveur Pandora FMS et OpenSearch sur des serveurs indépendants.

- Rocky Linux 8 / RHEL 8 / Ubuntu 22.04 (systèmes d'exploitation recommandés).
- Minimum 4 Go de RAM (test, développement), 8 Go de RAM recommandés pour chaque instance OpenSearch (exigences de base minimales, pour chaque environnement et quantité de données à traiter et/ou stocker, les exigences spécifiques doivent être estimées).
- Désactivez SWAP sur le ou les nœuds où se trouve OpenSearch.
- Minimum 4 cœurs CPU (exigences de base minimales, pour chaque environnement et quantité de données à traiter et/ou stocker, les exigences spécifiques doivent être estimées).
- 50 Go de stockage système.
- 100 Go de stockage OpenSearch (exigences de base minimales, pour chaque environnement et quantité de données à traiter et/ou stocker, les exigences spécifiques doivent être estimées).
- Connectivité du serveur Pandora FMS et de la console Web à l'API OpenSearch (port par défaut `9200/TCP`) et entre les nœuds du cluster (port par défaut `9300/TCP`).

Un environnement à nœud unique doté de ces fonctionnalités peut stocker jusqu'à 1 Go de données par jour et les stocker pendant 30 jours. Dans le cas d'une plus grande résilience des données, d'un plus grand traitement et stockage des données et d'une tolérance aux pannes, la configuration d'un cluster OpenSearch sera nécessaire (avec un minimum de 3 nœuds pour garantir l'intégrité des données). En passant à un environnement cluster, il est également possible de répartir la charge entre les nœuds, doublant (dans le cas de 3 nœuds) la capacité de traitement de l'environnement. Un système d'équilibrage de charge sera nécessaire (Keepalived, par exemple) si vous souhaitez travailler avec les différents nœuds simultanément.

Installation et configuration d'OpenSearch

Documentation officielle d'OpenSearch pour l'installation :

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

Installation

Avant d'exécuter OpenSearch sur votre ordinateur, désactivez la pagination et l'échange de

mémoire sur l'hôte pour améliorer les performances et augmenter le nombre de cartes mémoire disponibles pour OpenSearch. Voir « Paramètres importants » pour plus d'informations :

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
```

Pour Rocky Linux 8, l'installation via le package RPM est recommandée.

Liste des packages : https://opensearch.org/downloads.html

La documentation d'installation officielle :
https://opensearch.org/docs/latest/install-and-configure/install-opensearch/rpm/

Une fois OpenSearch installé, l'accès à OpenSearch doit être vérifié depuis Pandora FMS. Avant d'effectuer ce test vous devez configurer le nœud ou le cluster. Pour cette vérification d'installation, exécutez :

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

Vous devriez obtenir une réponse similaire à :

```
  {
     "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/"
  }
```

Par défaut, l'installation d'OpenSearch active SSL, nom d'utilisateur et mot de passe, ce qui est une bonne pratique ; Il est recommandé de changer le nom d'utilisateur et le mot de passe par défaut.

Configuration du nœud

Vous devez d'abord éditer le fichier de configuration `/etc/opensearch/opensearch.yml` puis le service OpenSearch sera redémarré.

Ce fichier contient la configuration de tous les paramètres du service OpenSearch ; consultez la documentation officielle pour plus d'informations :

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

Configurations minimales nécessaires pour démarrer le service et son utilisation avec Pandora FMS.

- Le numéro de port.

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

- L'emplacement des données et journaux stockés :

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

Il faudra également décommenter et définir les lignes suivantes :

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

- `cluster.name` : Ce sera le nom que recevra le groupe ou le cluster.
- `node.name` : Pour nommer le nœud à l'aide de la variable système `${HOSTNAME}`, il prendra automatiquement le nom de l'hôte.
- Pour `network.host` la valeur `0.0.0.0` permet à OpenSearch d'« écouter » sur toutes les interfaces réseau (NIC) ; Pour utiliser une carte réseau spécifique, entrez une valeur spécifique correspondante.

Si vous travaillez avec un seul nœud, vous devez ajouter la ligne au fichier de configuration pour permettre au nœud unique de démarrer :

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

Si vous travaillez avec un cluster, vous devez compléter le paramètre `discovery.seed_hosts` :

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

Dans les versions les plus récentes d'OpenSearch, la gestion de la mémoire de la machine virtuelle Java® se fait automatiquement et il est recommandé de la laisser gérer de cette manière dans les environnements de production, il n'est donc pas nécessaire de modifier les valeurs de la JVM.

Pour démarrer OpenSearch, exécutez :

```
systemctl start opensearch.service
```

Pour redémarrer, utilisez `restart`, pour arrêter `stop` et `status` pour vérifier l'état.

Si le service ne démarre pas, vérifiez les logs situés dans `/var/log/opensearch/` (dans ce cas, le fichier `pandorafms.log` ou le nom donné au nœud).

N'oubliez pas que pour vérifier l'installation et le fonctionnement d'OpenSearch vous pouvez exécuter :

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

Mise en place d'un cluster OpenSearch

Pour configurer un cluster OpenSearch, vous devez suivre la documentation officielle :

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

Gestion des utilisateurs OpenSearch

Pour changer le mot de passe par défaut de `admin`, une série d'étapes doit être suivie. La première chose est d'exporter la variable pour utiliser le Java® JDK installé par OpenSearch pour utiliser l'un des outils :

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

Ensuite, pour générer le mot de passe haché à placer dans le fichier de configuration d'OpenSearch, le script suivant est utilisé (remplacez `< password >` par le mot de passe à utiliser) :

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

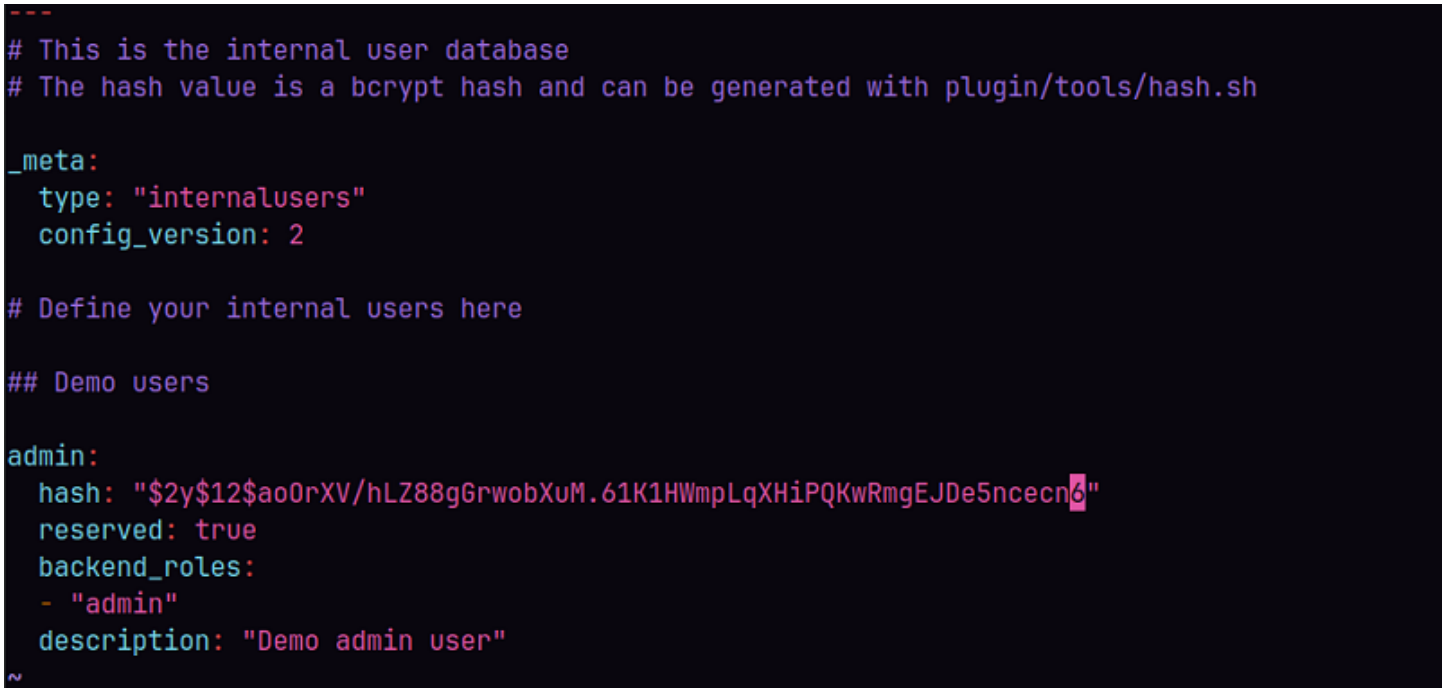
Par exemple:

```
[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
```

Ensuite, vous devez ouvrir le fichier `/etc/opensearch/opensearch-security/internal_users.yml` avec l'éditeur de texte vim ou nano pour modifier le mot de passe du ou des utilisateurs souhaités.

Il est recommandé de laisser uniquement l'utilisateur « admin » pour une utilisation avec Pandora FMS, il n'est pas nécessaire de maintenir un autre utilisateur.

Exemple de fichier :



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

Pour que les modifications soient effectives, les éléments suivants doivent être exécutés :

```
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
```

Un message final `Done with success` devrait être affiché ; pour vérifier le nouveau mot de passe (en suivant l'exemple précédent avec `pandora` utilisé) :

```
❯ 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/"
}
```

Pour plus d'informations sur la gestion des utilisateurs dans OpenSearch :

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

Configuration Pandora FMS avec OpenSearch

Pour configurer Pandora FMS avec OpenSearch voir la rubrique « Collecte et surveillance des journaux ».

Modèles de données et modèles

Avant de mettre en production un environnement, qu'il s'agisse d'un nœud unique ou d'un cluster de données, il est recommandé d'appliquer les configurations correspondantes à ce nœud ou cluster en fonction de son utilisation. Dans le cas des index générés par Pandora FMS, le moyen le plus efficace de le faire est de définir un modèle pour définir la configuration des champs et des données stockées.

Les modèles sont des configurations qui ne sont appliquées qu'au moment de la création de l'index. La modification d'un modèle n'aura aucun impact sur les index existants.

Pour créer un modèle de base, il vous suffit de définir les champs suivants :

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

Grâce à l'interface de Pandora FMS (menú), vous pouvez télécharger ledit modèle :

- PUT _template/<templatename> : dans cet exemple `PUT _template/pandorafms`.

Vous pouvez également consulter les modèles via la même interface Pandora FMS :

- GET _template/<templatename> : dans cet exemple `GET _template/pandorafms`.

Modèles multi-nœuds

Pour définir un modèle multi-nœuds vous devez prendre en compte les informations suivantes :

- Lors de la configuration du modèle (format JSON), vous devez configurer autant de fragments que vous avez de nœuds, cependant pour configurer correctement les réplicas vous devez soustraire 1 au nombre de nœuds dans l'environnement.

Par exemple, dans un environnement Pandora FMS avec 3 nœuds configurés, lorsque vous modifiez les champs `number_of_shards` et `number_of_replicas`, cela devrait ressembler à ceci :

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

Depuis la ligne de commande, vous pouvez lister les modèles d'environnement en exécutant :

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

Vous pouvez également afficher les détails d'un modèle, par exemple créé pour `pandorafms` en exécutant :

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

qui renverra la configuration que vous avez définie au format JSON.

Vous pouvez effectuer ces opérations via l'interface Pandora FMS :

- PUT _template/<template_name> {json_data} : Il permet de saisir les données du modèle à créer.
- GET _template/><template_name> : Il permet de visualiser le modèle créé.

Pour configurer Pandora FMS avec OpenSearch, voir « Collecte et supervision des journaux ».

Retour à l'index de la documentation Pandora FMS