ログの監視と収集

ログの監視と収集

Pandora FMS ドキュメント一覧に戻る

概要

Pandora FMS におけるログ監視には、以下の 2つの異なる手法があります。

1. モジュールベース: 非同期監視としの Pandora でログを表現します。ユーザにより事前設定された条件を満たすデータを検出した場合にアラートを関連付けることができます。 ログのモジュール表現では、以下を行うことができます：
    1. ログの中で正規表現にマッチする数を数えるモジュールの作成
    2. ログメッセージの行および内容を取得
2. 複合表示ベース: キャプチャしたい複数の発生元のログからすべての情報を 1つのコンソールで表示し、ログが処理されたタイムスタンプを使用して情報を順番に整理できます。

バージョン 7.0NG 712 からは、Pandora FMS に、ログ情報を保存するための Elasticsearch が組み込まれているため、パフォーマンスが大幅に向上しています。

動作の仕組み

処理は単純です。

- ソフトウエアエージェントで分析されたログ (eventlog またはテキストファイル) は、Pandora サーバへ転送されます。エージェントから送信される XML に (RAW) データとして含まれます。
- Pandora FMS データサーバは、エージェントから XML を受け取ります。そこには、監視とログの両方の情報が含まれています。
- データサーバが XML データを処理する時に、ログ情報を識別し、報告されたエージェントに関する情報やログのソースをプライマリデータベースに保存し、ログの保存には情報を自動的に ElasticSearch に送信します。
- Pandora FMS はデータを Elasticsearch インデックスに保存し、各 Pandora FMS インスタンスの日次インデックスを生成します。
- Pandora FMS サーバには、システム管理者が定義した間隔(デフォルトでは90日)でインデックスを削除するメンテナンスタスクがあります。

サーバの必要条件

Pandora FMS サーバと Elasticsearch は別々のサーバに展開することをお勧めします。

- Rocky Linux 8 または RHEL 8
- 最低 4GB のメモリ、ただし ElasticSearch インスタンスでは6GB のメモリを推奨します。
- Elastic が動作するサーバでの SWAP の無効化。
- 最低 2 CPUコア。
- 最低 20GB のシステムディスク空き領域。
- 最低 50GB の ElasticSearch データディスク空き領域(保存されるデータの量に応じて、異なる場合があります) Elasticsearch のディスク使用量は非常に多いため、読み取りと書き込みの速度が速いほど、環境のパフォーマンスが向上します
- Pandora FMS サーバからElasticsearch API (デフォルトポートは 9200/TCP) への接続性。

上記の最低条件のシングルノード環境では、毎日最大 1 GB のデータを保存し、デフォルトで 8日間保存できます。

より高いデータ復元力とフォールトトレランスが必要な場合は、Elasticsearch クラスターを構成する必要があります(データの整合性を保証するために最低 3つのノード)。 クラスタ環境に移行する場合、ノード間で負荷を分散し、環境の処理能力を 2倍(3ノードの場合)にすることもできます。 *異なるノード*で同時に処理したい場合は負荷分散システムが必要になります

Elasticsearch のインストールと設定

Elasticsearch の公式ドキュメントは以下にあります。

- https://www.elastic.co/guide/en/elasticsearch/reference/current/install-elasticsearch.html

インストール

Rocky Linux 8 の場合RPM パッケージを使用してインストールすることをお勧めします。これはElasticsearch データベースのインストールに必要なものすべてを含んだ単一のパッケージです。

ダウンロードには、https://www.elastic.co/downloads/elasticsearch へ行き、Linux x86_64 (

AMD® または Intel® 64 ビットプロセッサ) を選択します。

パッケージをダウンロードしたら、Elasticsearch をインストールするサーバにアップロードし、そのディレクトリに移動して、必要な権限を持ったユーザで次のように実行します。

```
dnf install ./downloaded_packet.rpm
```

次のような出力が表示されます。

```
[root@rocky8-node1 ~]# rpm -i elasticsearch-8.2.0-x86_64.rpm
warning: elasticsearch-8.2.0-x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID d88e42b4: NOKEY
Creating elasticsearch group... OK
Creating elasticsearch user... OK
-------------------------- Security autoconfiguration information ------------------------------

Authentication and authorization are enabled.
TLS for the transport and HTTP layers is enabled and configured.

The generated password for the elastic built-in superuser is : w5N8Vs-VwSyLqljisU8t

If this node should join an existing cluster, you can reconfigure this with
'/usr/share/elasticsearch/bin/elasticsearch-reconfigure-node --enrollment-token <token-here>'
after creating an enrollment token on your existing cluster.

You can complete the following actions at any time:

Reset the password of the elastic built-in superuser with
'/usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic'.

Generate an enrollment token for Kibana instances with
 '/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana'.

Generate an enrollment token for Elasticsearch nodes with
'/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s node'.

-------------------------------------------------------------------------------------------------
### NOT starting on installation, please execute the following statements to configure
    elasticsearch service to start automatically
 using systemd
 sudo systemctl daemon-reload
 sudo systemctl enable elasticsearch.service
### You can start elasticsearch service by executing
 sudo systemctl start elasticsearch.service
[/usr/lib/tmpfiles.d/elasticsearch.conf:1]
Line references path below legacy directory /var/run/, updating /var/run/elasticsearch →
 /run/elasticsearch; please update the tmpfiles.d/ drop-in file accordingly.
[root@rocky8-node1 ~]#
```

サービスが正しくインストールされたことを確認するには、次のコマンドを実行します。

```
systemctl status elasticsearch.service
```

次のような出力が表示されます。

Elasticsearch サービスが無効になっていることに注意してください。

ノードの設定

最初に、設定ファイル
/etc/elasticsearch/elasticsearch.yml を編集
し、Elasticsearch サービスを起動する必要があります。

このファイルには□Elasticsearch 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://www.elastic.co/guide/en/elasticsearch/reference/current/settings.html

次に、サービスを開始するために必要最小限の設定と、Pandora FMS での使用について説明します。

- ポート番号、データの場所、イベントログファイルの場所を設定します:

```
 # ---------------------------------- Network -----------------------------------
-
 # Set a custom port for HTTP:
 http.port: 9200
 # ---------------------------------- Paths -------------------------------------
-
 # Path to directory where to store the data (separate multiple locations by a
comma):
 path.data: /var/lib/elastic
 # Path to log files:
 path.logs: /var/log/elastic
```

- xpack を設定します:

```
xpack.security.enabled: false
xpack.security.enrollment.enabled: false
```

```
#---------------------- BEGIN SECURITY AUTO CONFIGURATION -----------------------
#
# The following settings, TLS certificates, and keys have been automatically
# generated to configure Elasticsearch security features on 12-05-2022 07:46:39
#
# --------------------------------------------------------------------------------

# Enable security features
xpack.security.enabled: false

xpack.security.enrollment.enabled: false
```

- この行をコメントアウトします。

```
#http.host: [_local_]
#transport.host: [_local_]
```

また、以下の行の *コメントを外し*、次のように定義する必要があります。

```
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です。

node.name

システムの環境変数 ${HOSTNAME} を使っているので、ホスト名が自動的に利用されます。

network.host

network.host に 0.0.0.0 を指定すると Elasticsearch は全ネットワークインタフェース(NIC)で待ち受けます。*特定の NIC を指定する場合は、特定の値を指定します。*

クラスターを使用する場合は、discovery.seed_hosts を設定する必要があります(詳細については、 Elasticsearch サーバのクラスターの構成 を参照してください):

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

または(フォーマット例):

```
 discovery.seed_hosts:
  - 192.168.1.10:9300
  - 192.168.1.11
  - seeds.mydomain.com
```

Elasticsearch 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るため、本番環境ではこれを利用することをお勧めします。したがって、Elasticsearch の JVM の値を変更する必要はありません。

完了したら、以下を実行します:

```
systemctl start elasticsearch.service
```

Elasticsearch が起動するまでしばらくお待ちください。ステータスを照会するコマンドは次のとおりです。

```
systemctl status elasticsearch.service
```

次のような出力が見られます。

```
[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)
```

サービスの開始に失敗した場合は、/var/log/elastic/ にあるログ(この場合はファイル pandorafms.log *または ノードに付けられた名前*)を確認してください。

Elasticsearch のインストールをテストするには、ターミナルウィンドウで次のコマンドを実行します。

```
curl -q http://{IP}:9200/
```

{IP} をインストールされている Elasticsearch の IP アドレスまたは URL に置き換えます。

次のような応答が得られます。

```
{
  "name" : "3743885b95f9",
```

```
  "cluster_name" : "docker-cluster",
  "cluster_uuid" : "7oJV9hXqRwOIZVPBRbWIYw",
  "version" : {
    "number" : "7.6.2",
    "build_flavor" : "default",
    "build_type" : "docker",
    "build_hash" : "ef48eb35cf30adf4db14086e8aabd07ef6fb113f",
    "build_date" : "2020-03-26T06:34:37.794943Z",
    "build_snapshot" : false,
    "lucene_version" : "8.4.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

本番環境に向けては、Elasticsearch のベストプラクティスを参照することをお勧めします。

- https://www.elastic.co/guide/en/elasticsearch/reference/current/system-config.html#dev-vs-prod

Elasticsearch クラスタ設定

- 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。

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。

データモデルとテンプレート

本番環境に導入する前に、用途に応じて、単一ノードまたはデータクラスターのいずれかの環境に応じて対応する設定をあらかじめ実施することをお勧めします。 Pandora FMS によって生成されるインデックスの場合、それを行う最も簡単な方法は、フィールドと保存するデータの設定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、フィールドを定義するだけです。

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

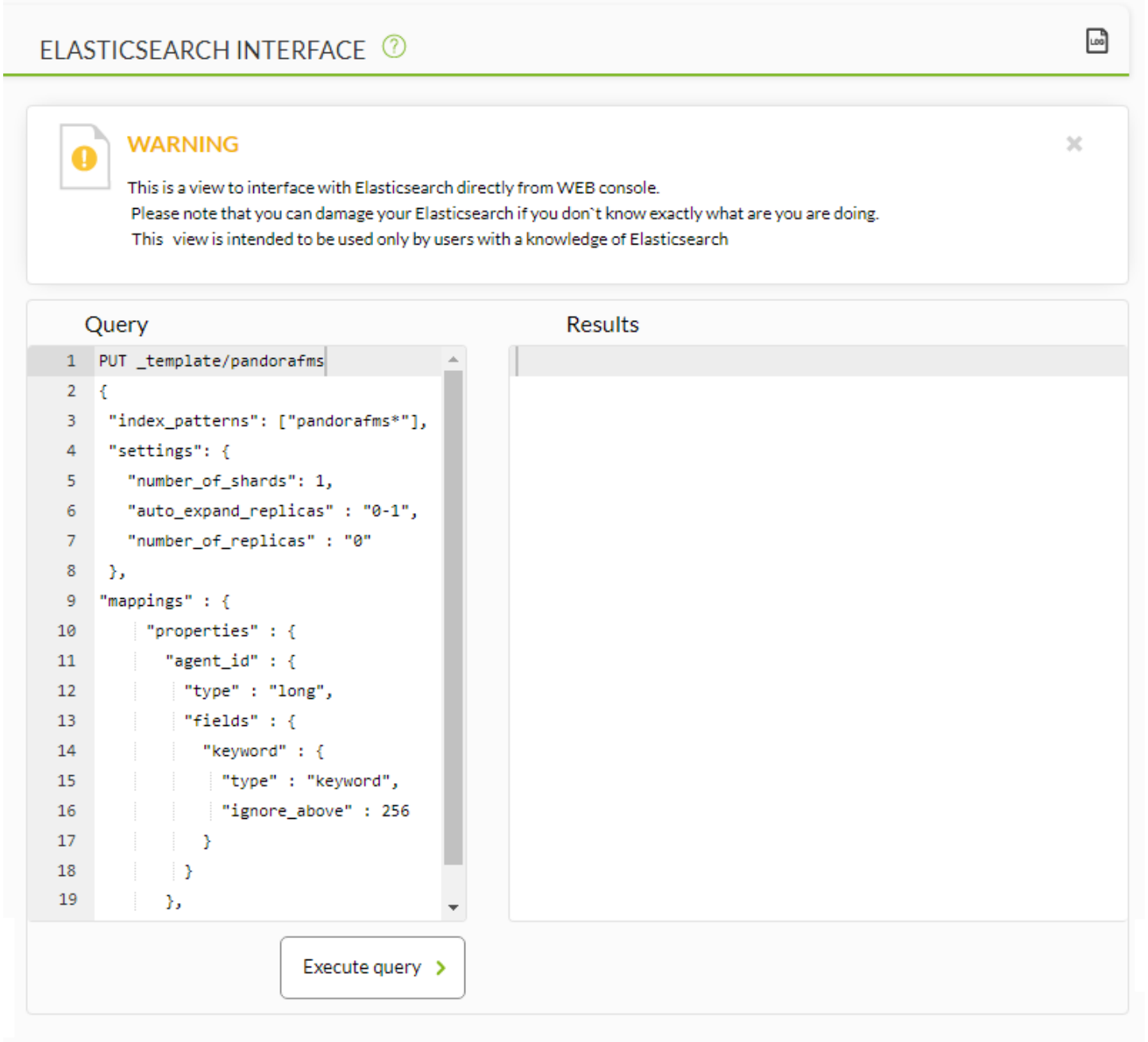
```
        "type" : "long",
        "fields" : {
          "keyword" : {
            "type" : "keyword",
            "ignore_above" : 256
          }
        }
      },
      "group_name" : {
        "type" : "text",
        "fields" : {
          "keyword" : {
            "type" : "keyword",
            "ignore_above" : 256
          }
        }
      },
      "logcontent" : {
        "type" : "text",
        "fields" : {
          "keyword" : {
            "type" : "keyword",
            "ignore_above" : 256
          }
        }
      },
      "source_id" : {
        "type" : "text",
        "fields" : {
          "keyword" : {
            "type" : "keyword",
            "ignore_above" : 256
          }
        }
      },
      "suid" : {
        "type" : "text",
        "fields" : {
          "keyword" : {
            "type" : "keyword",
            "ignore_above" : 256
          }
        }
      },
      "type" : {
        "type" : "text",
        "fields" : {
          "keyword" : {
            "type" : "keyword",
            "ignore_above" : 256
          }
        }
```

```
        },
        "utimestamp" : {
          "type" : "long"
        }
      }
    }
  }
}
```

Pandora FMS の Elasticsearch インターフェース(管理ツール(Admin tools) → Elasticsearch インターフェース(Elasticsearch Interface))を介して、ネイティブの Elasticsearch コマンドを使用し、テンプレートをアップロードできます。

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

- PUT _template/<template_name>: この例では PUT `_template/pandorafms`



同じ Pandora FMS インターフェースを介してテンプレートを参照することもできます。

- GET _template/<template_name>: この例では GET _template/pandorafms

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

マルチノードテンプレート

マルチノードテンプレートを定義するには、考慮しなければならないことがいくつかあります。

- テンプレート(JSON)の設定を行うときは、ノードと同じ数の検索を設定する ことを考慮に入れる必要がありますが、正しく設定するには、環境に実際に存在する レプリカの数から 1を引く 必要があります。

例えば、3つのノードを設定した Elasticsearch を Pandora FMS 環境で使用する場合、number_of_search および 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、以下で説明され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、以下を実行すると pandorafms 用に作成したテンプレートを表示できます。

```
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

推奨事項

Elasticsearch のログローテーション

重要: Elasticsearch のログが肥大化しないように、/etc/logrotate.d でログローテーションのエントリーを作成することをお勧めします。

```
cat > /etc/logrotate.d/elastic <<EOF
/var/log/elastic/elaticsearch.log {
       weekly
       missingok
       size 300000
       rotate 3
       maxage 90
       compress
       notifempty
       copytruncate
}
EOF
```

インデックスの削除

ElasticSearch サーバに対して curl でアクセスすることにより、いつでもインデックスの一覧と大きさを確認することができます。

```
curl -q http://elastic:9200/_cat/indices?
```

ここで、elastic はサーバの IP です。

インデックスを削除するには、DELETE コマンドを実行します。

```
curl -q -XDELETE http://elastic:9200/{index-name}
```

ここで elastic はサーバの IP で、"{index-name}" は上のコマンドの出力ファイルです。これにより、削除されたインデックスによって使用されていたスペースが解放されます。

Pandora FMS Syslog サーバ

E バージョン NG 717 以上

このコンポーネントにより、Pandora はマシンの Syslog を分析できます。Syslog のコンテンツを分析し、ElasticSearch サーバに格納することができます。

SyslogServer の主な利点としては、ログの統合を補完することにあります。Linux および UNIX 環境

の SYSLOG 出力をもとにしてSyslogServer では、1つの共通ポイント(Pandora FMS コンソールのログビューア)で、発信元ごとに個別のログを参照したり、検索したりすることができます。

Syslog のインストールは、クライアントとサーバの両方に次のコマンドで行います。

```
yum install rsyslog
```

対象のコンピューターに Syslog をインストールしたら、設定ファイル /etc/rsyslog.conf を編集して TCP および UDP 接続を有効にする必要があることに注意してください。

```
 (...)

 # Provides UDP syslog reception
 $ModLoad imudp
 $UDPServerRun 514

 # Provides TCP syslog reception
 $ModLoad imtcp
 $InputTCPServerRun 514

 (...)
```

調整を行ったらrsyslog サービスを再起動します。

サービスが再起動したら、ポート 514 が開いているか確認します。

```
netstat -ltnp
```

rsyslog 設定に関する詳細は、公式サイト を参照してください。

Syslog サーバにログを送信するようにクライアントを設定します。そのためには、/etc/rsyslog.conf にあるクライアント rsyslog 設定ファイルにて、リモートホストの設定をする行を見つけて有効にします。

```
.* @@remote-host:514
```

ログ送信により、クライアント名を持つコンテナエージェントが生成されるため、エージェントの重複を回避するために、クライアントのホスト名と一致する“ 別名 ”を持つエージェントを作成することをお勧めします。

この機能を有効化するには、pandora_server.conf で以下の設定を有効にするだけです。

```
 # Enable (1) or disable (0) the Pandora FMS Syslog Server
```

```
#  (PANDORA FMS ENTERPRISE ONLY).
syslogserver 1

# Full path to syslog's output file (PANDORA FMS ENTERPRISE ONLY).
syslog_file /var/log/messages

# Number of threads for the Syslog Server
#  (PANDORA FMS ENTERPRISE ONLY).
syslog_threads 2

# Maximum number of lines queued by the Syslog Server's
#   producer on each run (PANDORA FMS ENTERPRISE ONLY).
syslog_max 65535
```

syslogserver

ローカルの SYSLOG 分析**エンジンの**有効化(1)**または**無効化(0)**を**設定**します**。

syslog_file

SYSLOG **ファイルの**場所**です**。

syslog_threads

SyslogServer **のデータ**処理**に**使う最大**スレッド**数**です**。

syslog_max

SyslogServer **が**処理**する**最大**ウインドウサイズです**。一度**の**実行**で**処理**する**最大**の** SYSLOG **エントリー**数**です**。

これは SyslogServer **の**最大処理**ウィンドウであり、**一度**に**処理**される** SYSLOG **エントリの**最大数**になります**。

ElasticSearch **サーバを**有効化**し**設定**する**必要**があります**。
使用方法**については、**前述**の**内容**を**確認**してください**。

ログが Pandora FMS **サーバに**送信**されるように、デバイス**
の設定**を**変更**する**必要**があります**。

Elasticsearch システムへのマイグレーション

バージョン 712 **またはそれ**以前。最新**のバージョンにアッ**
プグレードする必要**があります**。詳細**については、**Pandora

FMS アップグレード を参照してください。

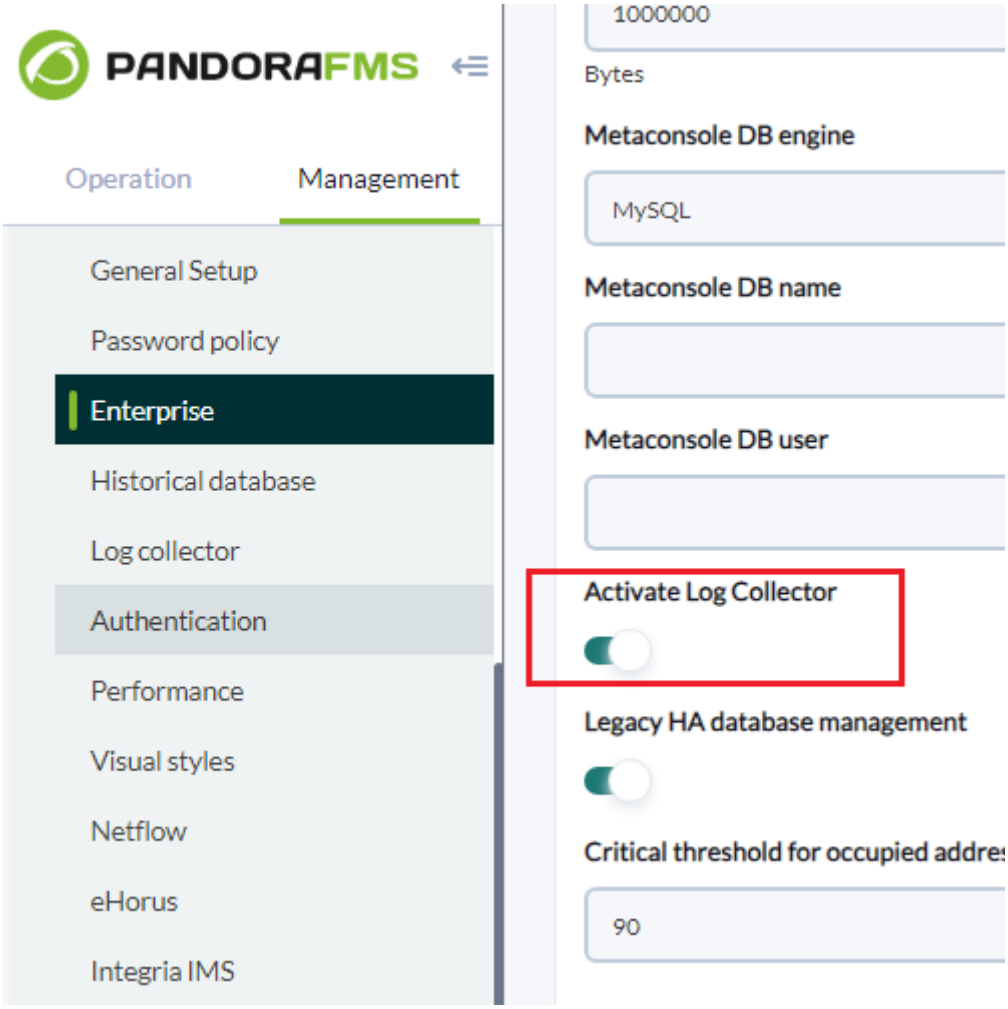
ログの新たなストレージシステムを設定後、以前から Pandora に保存されているデータを新たなシステムへマイグレートできます。

新たなシステムへマイグレートするには/usr/share/pandora_server/util/ 以下にある次のスクリプトを実行します。

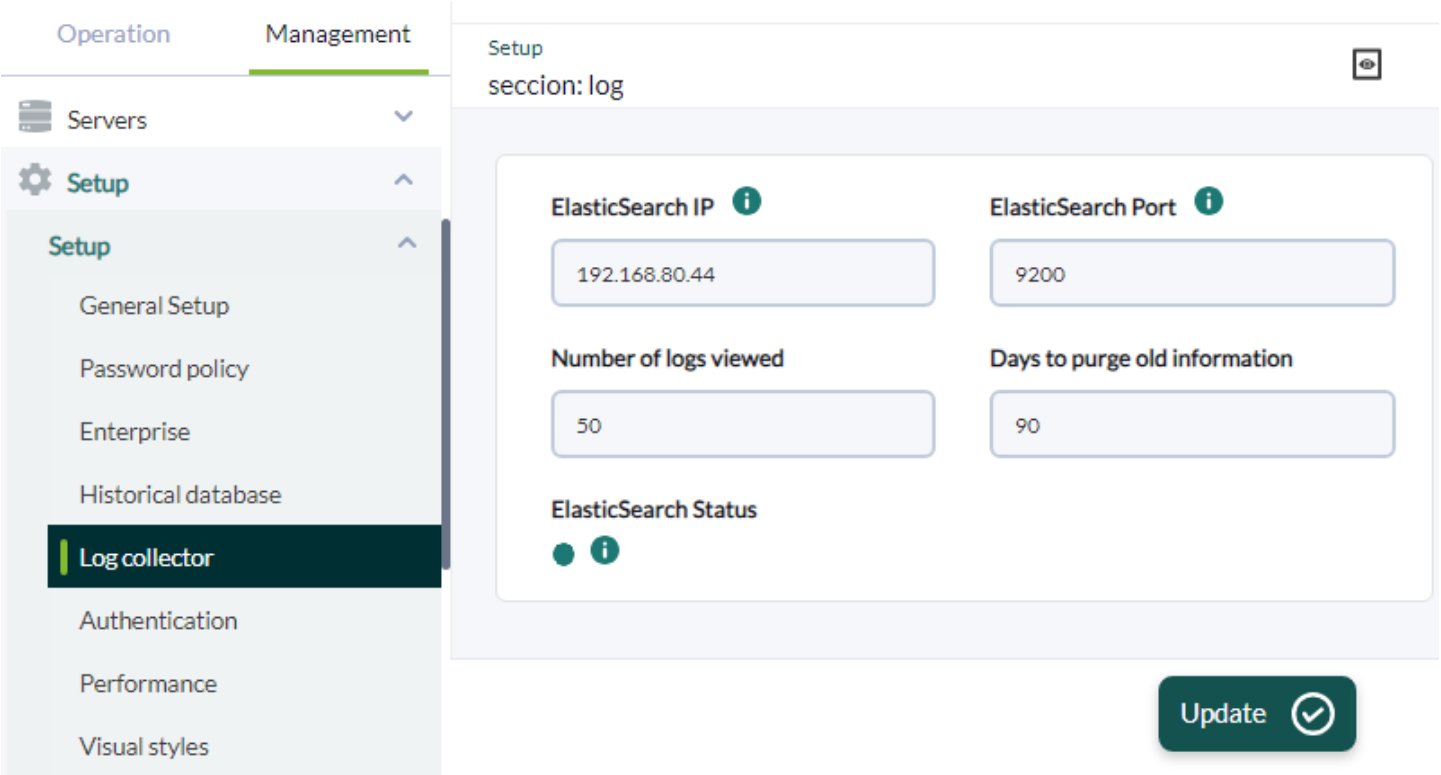
```
 # 7.0NG 712 より前のログデータを、7.0NG 712 以降にマイグレート
 /usr/share/pandora_server/util/pandora_migrate_logs.pl
/etc/pandora/pandora_server.conf
```

コンソールの設定

ログの表示を有効化するには、次の設定を有効化する必要があります。(セットアップ(Setup) → セットアップ(Setup) → Enterprise)



セットアップ(Setup) → セットアップ(Setup) → ログ収集(Log Collector) タブで、ログビューワの動作を設定できます。

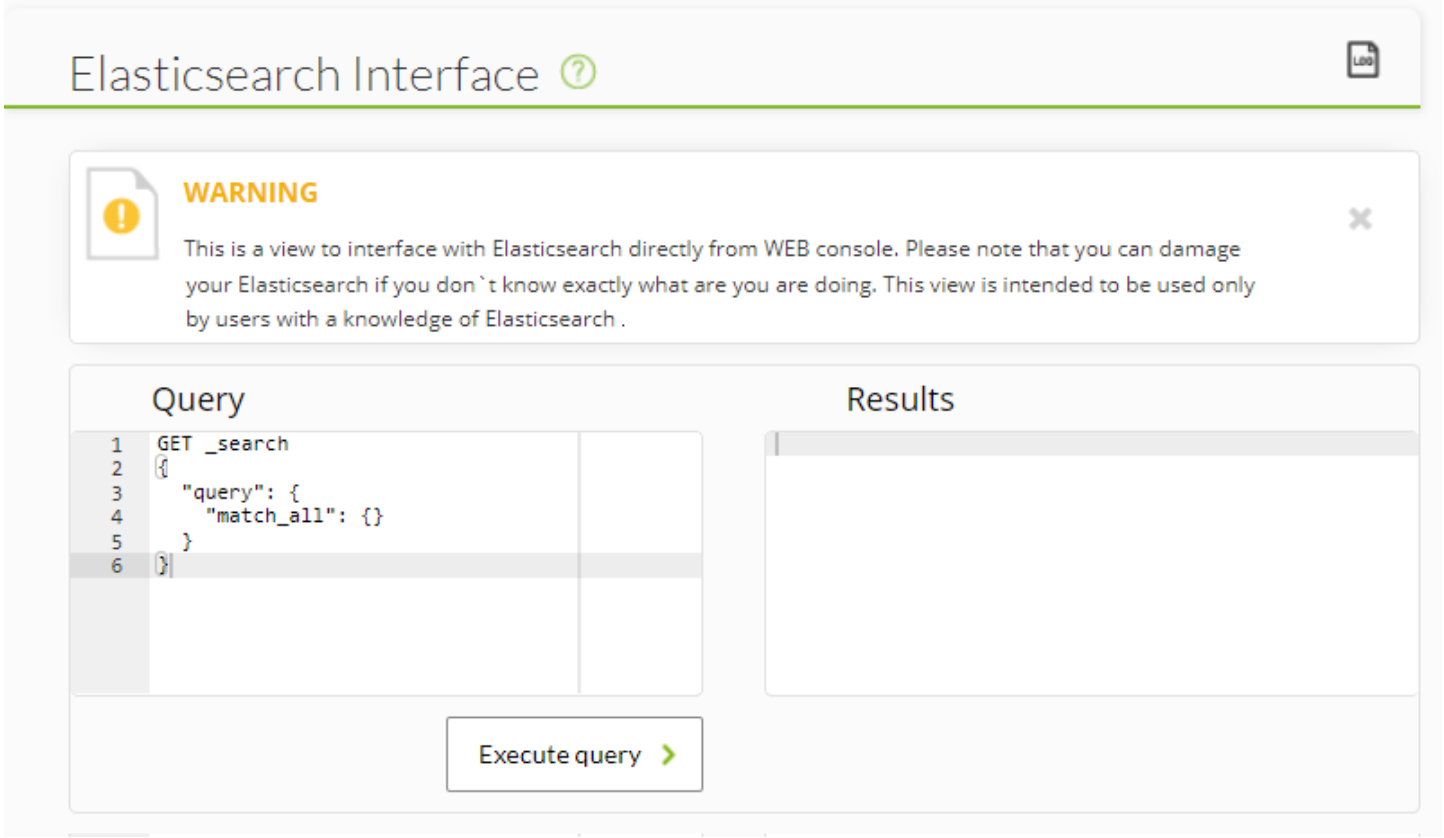


この画面では以下の設定ができます。

- Elasticsearch サーバの IP または FQDN アドレス
- Elasticsearch サービスのポート
- 表示されるログの数(Number of logs being shown):コンソール応答の高速化のため、レコードの動的読み込みが追加されています。これを利用するには、ページの一番下へスクロールします。すると、次のレコードが読み込まれます。これらのグループのサイズは、グループあたりのレコード数としてこのフィールドに設定できます。
- 削除する日数(Days to purge): システムのサイズを保持するために、ログ情報を保存する最大日数を定義できます。それを超えるとPandora FMS のクリーニング処理により自動的に削除されます。

Elasticsearch インタフェース

Eバージョン NG 747 以上



デフォルトの設定では、Pandora は 1日あたりのインデックスを生成します。これは、何かを検索する際のフラグメント化の役割を持ちます。検索時に Elastic がフラグメントの場所を認識できるようにします。

この検索をデフォルトで最適化するには、Elastics が検索ごとにインデックスを生成し、Elastics ノードと同じ数の検索を環境内で設定する必要があります。

これらの検索とレプリカは、Pandora が自動的に生成するインデックスの作成時に設定されるため、この設定を変更するには、テンプレートを使用する必要があります。

データバックアップとリストア

データスナップショット(インデックス)は、Elastichsearchの最近のバージョンにおいてデータをバックアップするために使用するメカニズムです。 これらのスナップショットを使用して、ハードウェア障害後にデータを回復したり、ノード間でデータを転送したり、ノードからめったに使用されないインデックスを削除したりすることもできます(*後者には追加の構成が必要です*)。

これらのスナップショットは、データを段階的にバックアップすることで機能します。つまり、バックアップされていない新しいデータのみをコピーし、作成済みのバックアップの信頼性と Elasticsearch の異なるバージョン間の互換性を確保します。

Elasticsearch で、これらすべての機能を保証する方法はリポジトリを使用することです。

リポジトリは独自のものでも、サードパーティ(AWS S3®、Google Cloud Storage®、Microsoft Azure®)で作成することもできます。いずれの場合も、Pandora FMS と組み合わせて使用する 1つまたは複数のノードの外に物理的に配置する必要があります。 これらのスナップショットについては、ユーザ自身の責任の元での管理となります。

詳細については、Elasticsearch の公式ドキュメントを参照してください。

- https://www.elastic.co/guide/en/elasticsearch/reference/current/snapshot-restore.html

リポジトリの作成

ネットワークファイルシステム(NFS)またはその他の共有ファイルシステムは、環境内で Elasticsearch リポジトリとノードをホストするマシンから利用可能である必要があります。

複数のサーバ間でのディレクトリの共有: このNFS を使用して Elasticsearch リポジトリを提供することは控えてください。 システムの各コンポーネントを適切に責任はユーザにあります。

対象の NFS をインストールして設定したら、Elastisearch ノードにディレクトリを作成してマウントします。たとえば、次のように呼び出すことができます。

```
/mnt/pandorafms/elk_repo
```

ユーザー elasticsearch に権限を付与します。

```
chown elasticsearch:  /mnt/pandorafms/elk_repo
```

Elasticsearch 設定ファイルでこのパスをノード(すべてのノード)のリポジトリパスとして宣言する必要があります。

```
path:
  repo:
   - /mnt/pandorafms/elk_repo
```

ノードを設定したら、(すべてのノードで) elasticsearch サービスを再起動する必要があります。

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

Pandora FMS の Elasticsearch インターフェース とは別に、curl コマンドを使用して、情報を取得したり、Elastisearch ノードに要求を伝達したりすることもできます。 リポジトリを作成するには、1つまたは複数のノード(すべてのノード)でローカルに次のコマンドを実行します。

```
curl -X PUT "localhost:9200/_snapshot/backup_repo?pretty" -H 'Content-Type:
application/json' -d'
{
 "type": "fs",
 "settings": {
   "location": "/mnt/pandorafms/elk_repo/"
 }
}
'
```

9200 以外のポートを利用する場合は、その値を置き換えます。

ノードから次のようなメッセージが得られます。

```
"acknowledged" : true
```

これは、リポジトリが作成されたことを示します。 リポジトリのステータスを確認するには次のようにします。

```
curl -X POST "localhost:9200/_snapshot/my_unverified_backup/_verify?pretty"
```

my_unverified_backup を確認するリポジトリの名前に置き換えます。 すべてが正常に行われた場合、リポジトリが設定されているノードのリストが表示されます。

データベースのスナップショット生成

スナップショットを手動で取得するには、スナップショット作成 API を使用します。 スナップショット名は、一意の名前をつけるために、date math の使用をサポートしています。

```
PUT _snapshot/my_repository/<my_snapshot_{now/d}>
```

my_repository をリポジトリの名前に置き換え、my_snapshot をスナップショットの名前に置き換えます。 curl を使用する場合は、エスケープ文字を使用する必要があるため、上記のコマンドは次のようになります。

```
PUT _snapshot/my_repository/%3Cmy_snapshot_%7Bnow%2Fd%7D%3E
```

サイズによっては、スナップショットの取得に時間がかかる場合があります。 デフォルトでは、スナップショット作成 API は、バックグラウンドで実行されるスナップショットプロセスのみを実行します。 スナップショットが終了するまでクライアントが待つようにするには、クエリパラメータ wait_for_completion を true に設定します。

```
PUT _snapshot/my_repository/my_snapshot?wait_for_completion=true
```

snapshot_today という名前のスナップショットを実行するには、ノードの 1つで以下のように実

行します。

```
curl -X PUT
"localhost:9200/_snapshot/backup_repo/snapshot_today?wait_for_completion=true&pr
etty"
```

9200 以外のポートを利用する場合は、該当部分を置き換えます。

パラメータ wait_for_completion=true を使用すると、プロセスが終了するまで呼び出し処理が待ちのままになります(データベースのサイズによっては時間がかかる場合があります)。

完了するとすぐに、処理の概要情報が JSON 形式で返されます。これは次のようになります。

```
curl -X PUT "localhost:9200/_snapshot/backup_repo/snapshot_today?
wait_for_completion=true&pretty"
{
  "snapshot" : {
    "snapshot" : "snapshot_today",
    "uuid" : "7OpWobAlR3GCirpjREdisg",
    "repository" : "backup_repo",
    "version_id" : 8010199,
    "version" : "8.1.1",
    "indices" : [
      "pandorafms-a047762063ed11ecae4e000c29f05369-2022.04.18",
      "pandorafms-eea618e1825411eb8d587ee88f349bd9-2022.02.18",
      "pandorafms-3b32000b825911eb917ee22e0c51316e-2022.04.11",

      "pandorafms-9139d75dfe6111eb9baeb6e1fdfecee6-2022.03.08"
    ],
    "data_streams" : [
      "ilm-history-5",
      ".logs-deprecation.elasticsearch-default"
    ],
    "include_global_state" : true,
    "state" : "SUCCESS",
    "start_time" : "2022-05-12T17:07:08.642Z",
    "start_time_in_millis" : 1652375228642,
    "end_time" : "2022-05-12T17:10:29.848Z",
    "end_time_in_millis" : 1652375429848,
    "duration_in_millis" : 201206,
    "failures" : [ ],
    "shards" : {
      "total" : 445,
      "failed" : 0,
      "successful" : 445
    },
    "feature_states" : [
      {
        "feature_name" : "geoip",
        "indices" : [
          ".geoip_databases"
        ]
      },
      {
        "feature_name" : "tasks",
        "indices" : [
          ".tasks"
        ]
      },
      {
        "feature_name" : "kibana",
        "indices" : [
          ".kibana_task_manager_7.12.0_001",
          ".apm-custom-link",
          ".kibana_task_manager_8.1.1_001",
          ".apm-agent-configuration",
          ".kibana_8.1.1_001",
          ".kibana_7.12.0_001"
        ]
      }
    ]
  }
}
```

含めるインデックスやメタデータなど、スナップショットの実行で特定のオプションを定義することもできます。詳細については、次を参照してください。

- https://www.elastic.co/guide/en/elasticsearch/reference/current/create-snapshot-api.html

例:

```
curl -X PUT
"localhost:9200/_snapshot/backup_repo/snapshot_2?wait_for_completion=true&pretty
" -H 'Content-Type: application/json' -d'
{
 "indices": "pandorafms*",
 "metadata": {
   "taken_by": "PandoraFMS admin user",
   "taken_because": "backup before upgrading"
 }
}
'
```

スナップショットの一覧

保存されているすべてのスナップショットの一覧を取得するには、次のコマンドを実行します。

```
curl -X GET "localhost:9200/_snapshot/backup_repo/*?pretty"
```

ここで、backup_repo はリポジトリ ID であり、* はすべてを表します Elasticsearch のスナップショット検索フィルターの詳細については、次の Web サイトをご覧ください。

- https://www.elastic.co/guide/en/elasticsearch/reference/current/get-snapshot-api.html

スナップショットの削除

スナップショットを削除するには、上記のコマンドにてその名前を取得してから、ノードの 1つで実行します。

```
curl -X DELETE "localhost:9200/_snapshot/backup_repo/snapshot_today?pretty"
```

データベーススナップショットのリストア

スナップショットからインデックスを復元するには、他の技術的な考慮事項とは別に、インデックスを閉じる必要があります。 詳細については、次のリンクを参照してください。

- https://www.elastic.co/guide/en/elasticsearch/reference/current/snapshot

s-restore-snapshot.html#restore-snapshot-considerations

インデックスを復元するには、次の 2つの方法のいずれかを使用する必要があります。

1. 復元する前に、元のインデックスを削除
2. 復元するインデックスの名前を変更

両方の場合を、リポジトリ名に backup_repo、スナップショット名に snapshot_today を例として使用して以下に示します。

- 削除およびリストア:

競合を回避する最も簡単な方法は、既存のインデックスまたはデータストリームを*復元する前に*削除することです。

インデックスまたはデータストリームが誤って再作成されないように、復元操作が完了するまですべてのインデックスを一時的に停止することをお勧めします。

インデックスの削除方法:

```
curl -X DELETE "localhost:9200/my-index?pretty"
```

インデックスのリストア方法:

```
curl -X POST
"localhost:9200/_snapshot/backup_repo/snapshot_today/_restore?pretty" -H
'Content-Type: application/json' -d'
{
 "indices": "my-index,logs-my_app-default"
}
'
```

- リストアの際にリネーム

  この操作をする際は十分なストレージスペースがあることを確認してください。

この方法では、すでに保存されている情報と同じものを扱います。一部のシナリオでは、この処理が役立つ場合があります。たとえば、次のような場合です。

- データ取得が正常に実行されたことを確認する必要がある。 各インデックスとその名前が変更されたコピーで、同じ情報が含まれ、同じ検索結果が返されることを確認する。
- サードパーティによって実行されたデータ監査を検証する。

```
curl -X POST
"localhost:9200/_snapshot/backup_repo/snapshot_today/_restore?pretty" -H
'Content-Type: application/json' -d'
{
 "indices": "my-index,logs-my_app-default"
  "rename_pattern": "(.+)",
  "rename_replacement": "restored-$1"
}
'
```

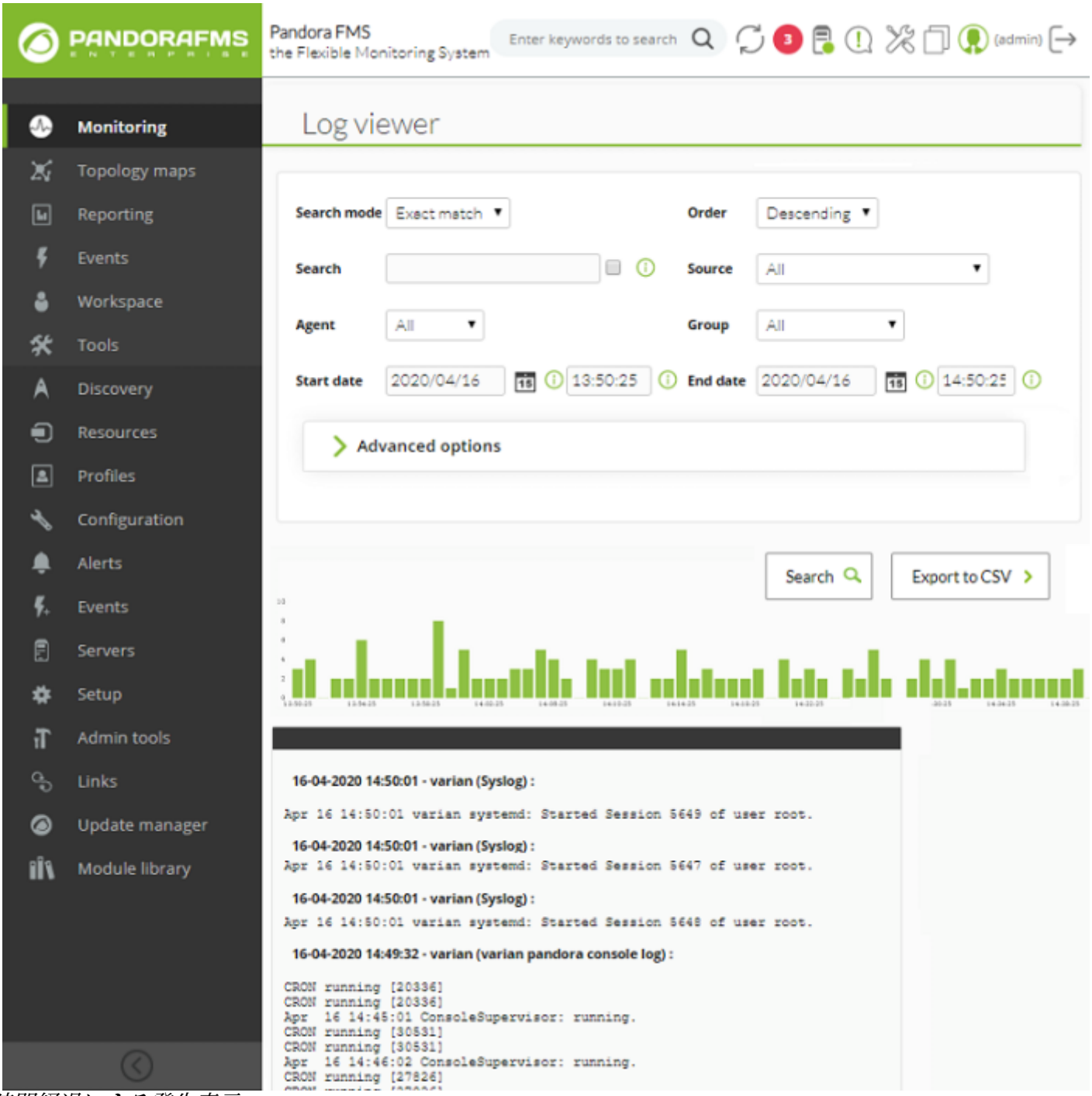
ノードの完全リストア

すべてのインデックスを含むノード全体を復元する場合は、復元を実行する前にインデックスサービスを停止することをお勧めします。このトピックの詳細については、次を参照してください。

- https://www.elastic.co/guide/en/elasticsearch/reference/current/snapshots-restore-snapshot.html#restore-entire-cluster

表示と検索

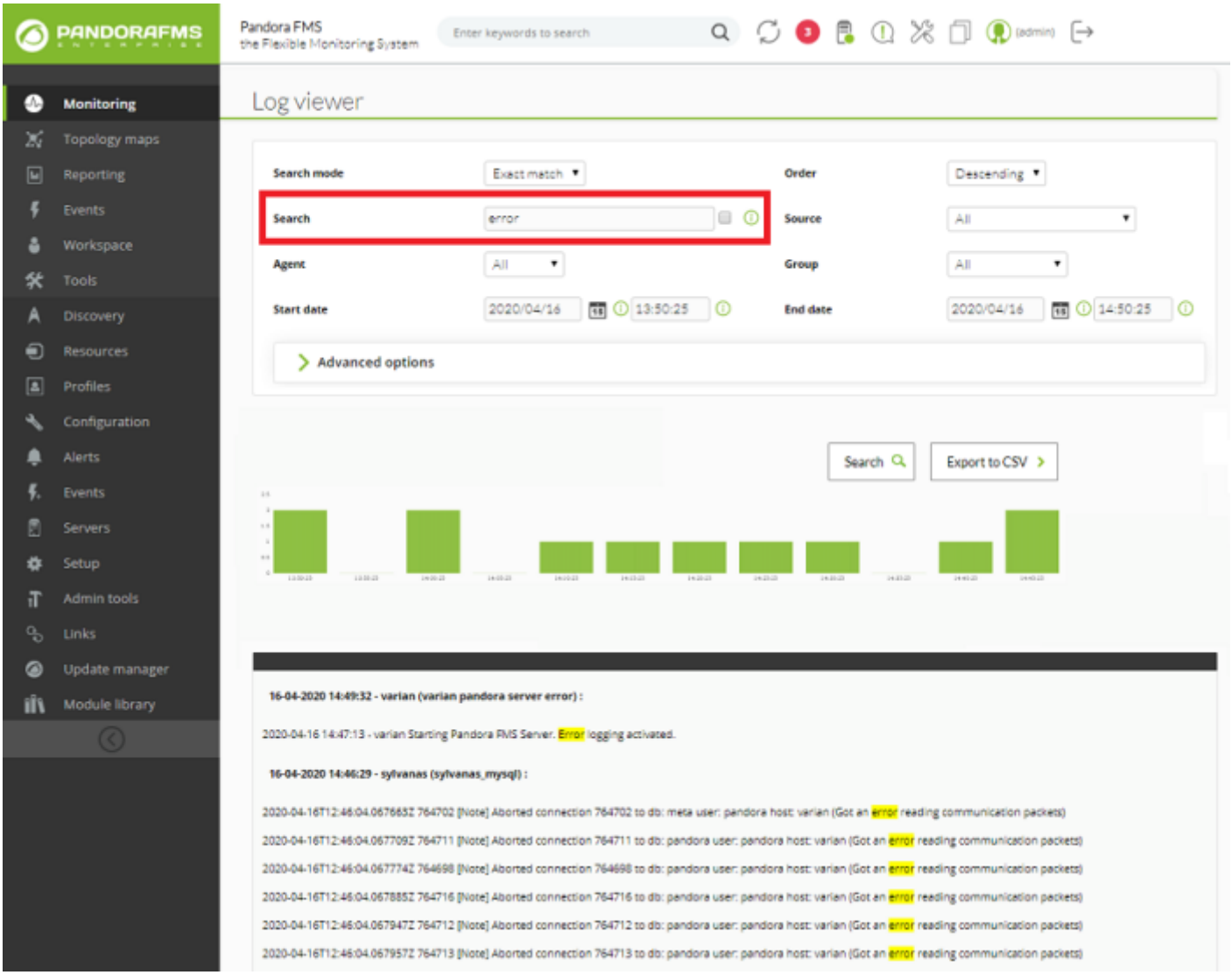
ログ収集のツールに関して、私たちは主に 2つのことに興味があります。日時やデータソース、キーワードによるフィルタリングをしての情報の検索と、時間単位ごとに発生する情報の参照(ログビューワ)です。この例では、直近 1時間のすべてのデータソースからのログメッセージを見てみます。Search, Start date **および** End date **を見てください。**



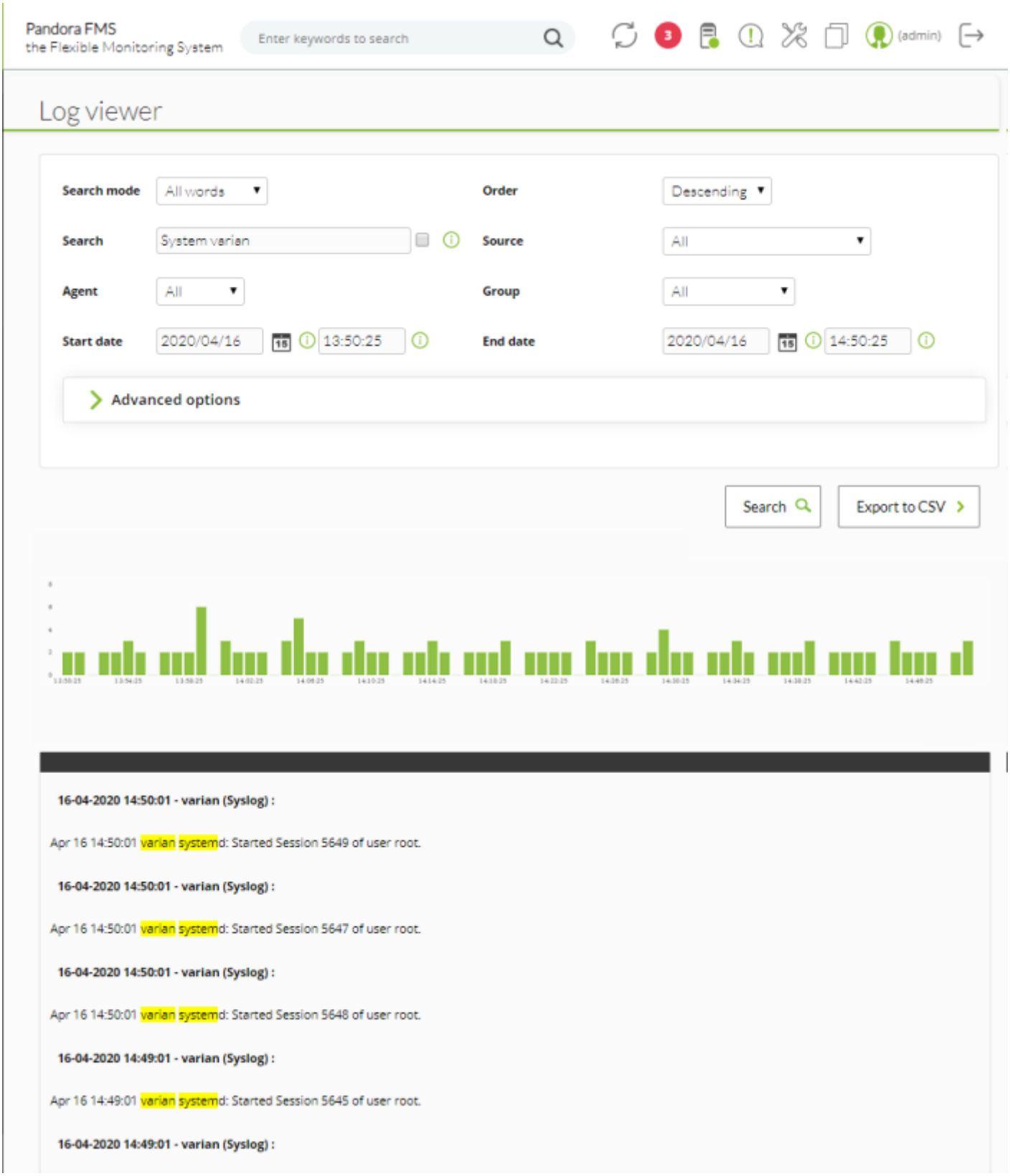
時間経過による発生表示

最も重要で便利なフィールドは、検索 テキストボックスに入力する検索文字列と、使用可能な 3つの 検索モード です。

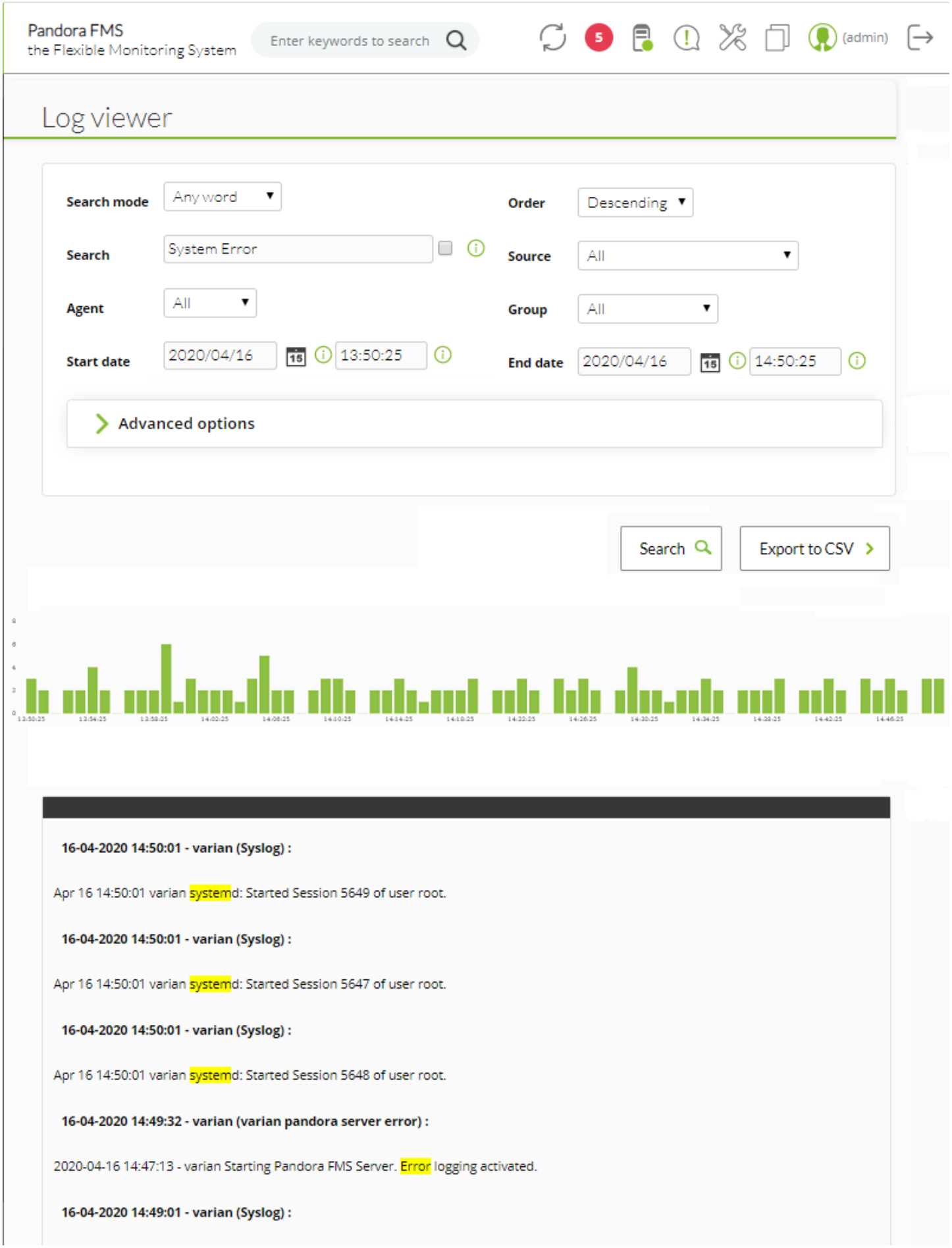
完全一致 文字検索で、*log* は完全マッチします。



全単語 単一の *ログ*の行の順序に関係なく、指定された単語(各単語はスペースで区切られることに注意してください)を *すべて*含むかを検索します



任意の単語 順番は関係なく、指定した単語の いくつか が含んでいるかを検索します。



フィルタされたコンテンツのコンテキストを表示するオプションがチェックされている場合、結果は、検索に関連する他のログ行に関する情報を含む状況の概要になります。

表示と高度な検索

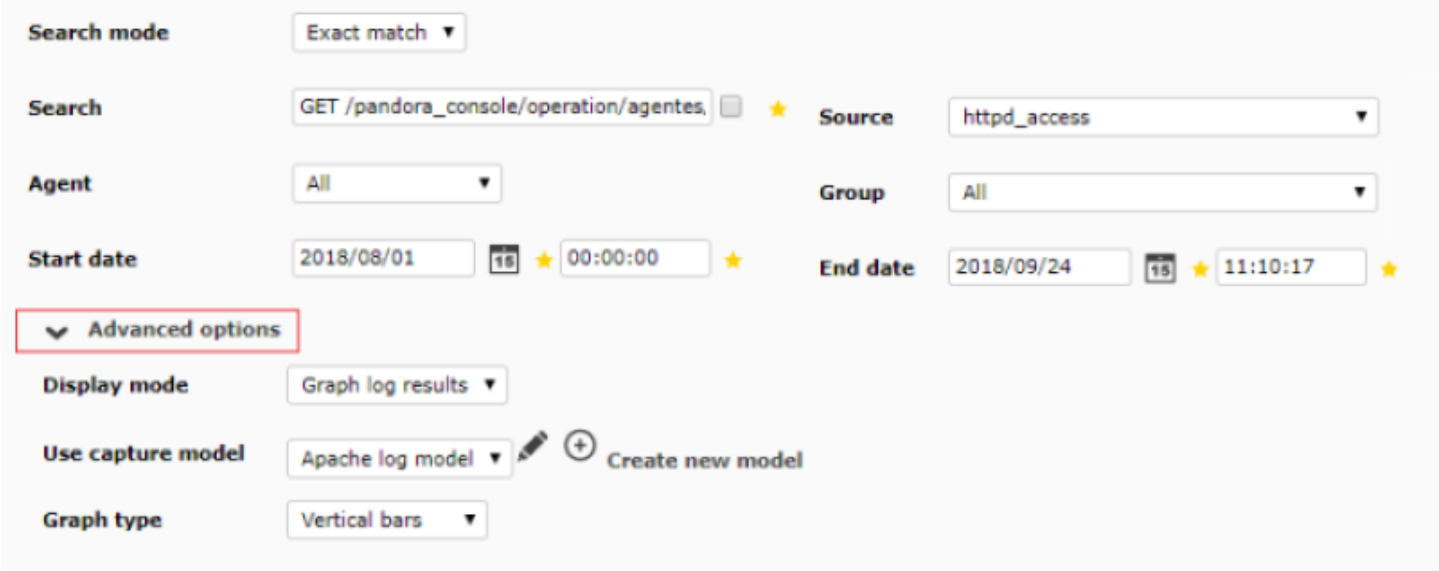
Eバージョン NG 727 以上

この機能により、ログエントリをグラフに変換し、 データキャプチャテンプレート に従って情報を整理できます。

これらのデータキャプチャテンプレートは基本的に正規表現と識別子であり、データソースを分析してグラフとして表示できます。

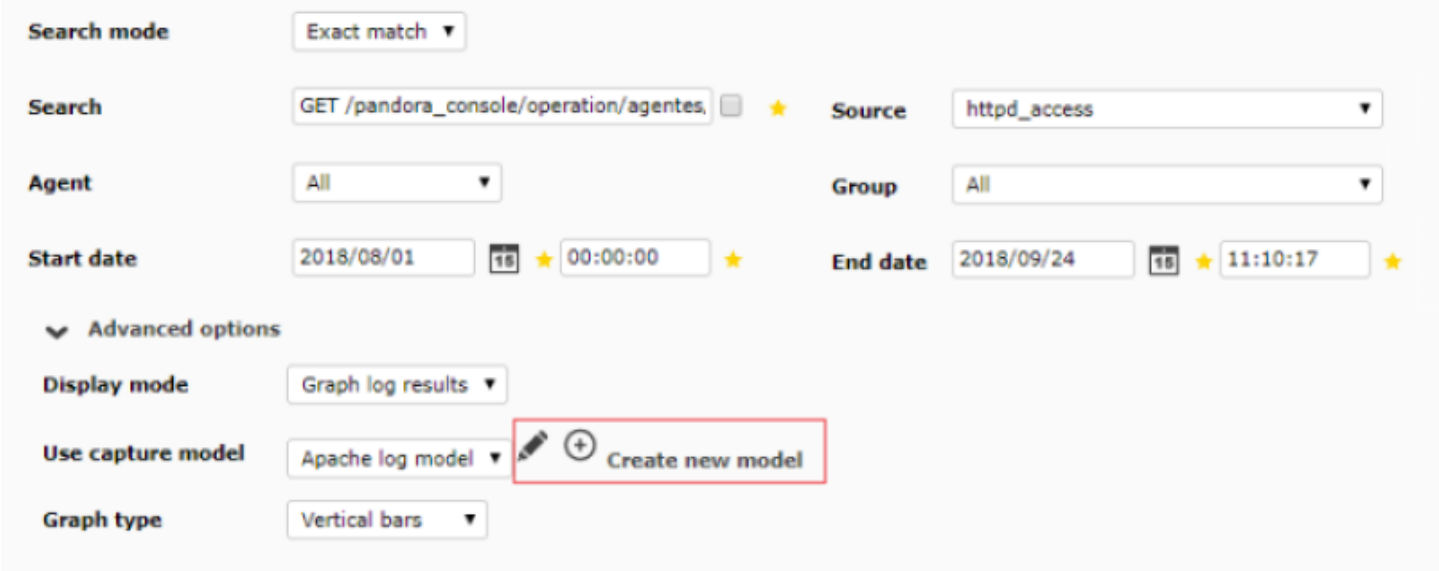
高度なオプションへアクセスするには、*高度なオプション(Advanced options)* をクリックします。表示形式を選択できるフォームが表示されます。

- ログエントリーの表示 (プレーンテキスト)
- ロググラフの表示

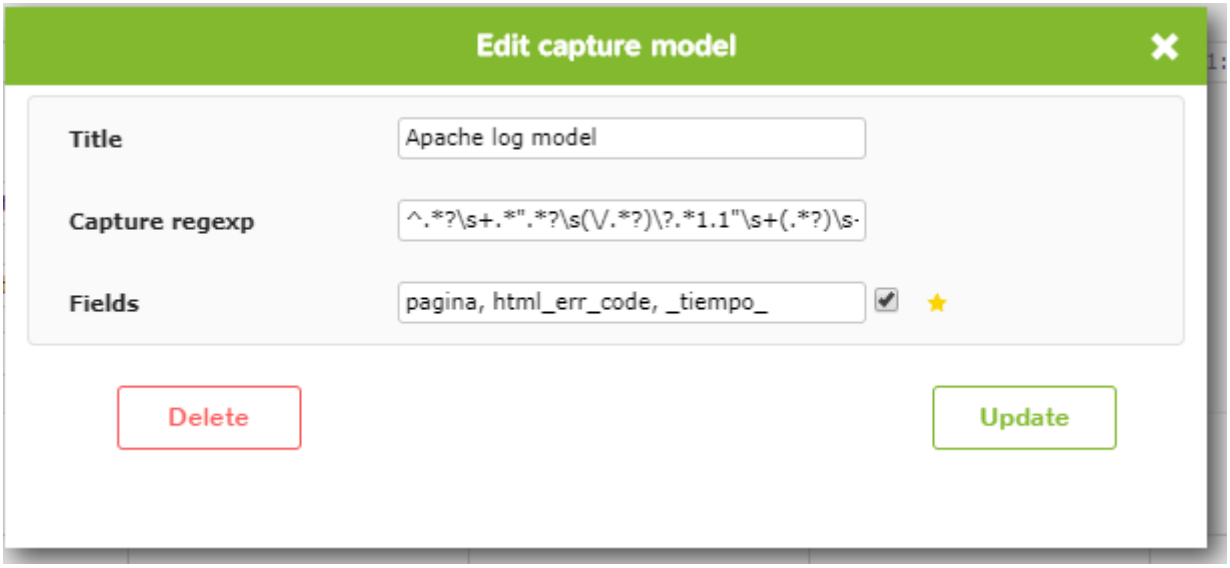


ロググラフ表示 オプションでは、キャプチャテンプレートを選択できます。

Apache log model テンプレートは、デフォルトで、標準形式の Apache ログ (access_log) をパースし、時間応答比較グラフの取得、訪問サイトと応答コードによるソートができます。



編集ボタン を押すと、選択したキャプチャテンプレートを編集できます。作成ボタン では、新たなキャプチャテンプレートを追加できます。



このフォームでは、以下を選択できます。

キャプチャ正規表現(Capture regexp)

データをキャプチャするための正規表現です。取得する各フィールドは、カッコでくくります。*(キャプチャする内容)* フィールド(Fields)

正規表現を介してキャプチャされる順番です。 結果は、アンダースコアの間に書かれていない名前のキーフィールドの連結によってソートされます。

```
key, _value_
```

```
key,key2,_value_
```

```
key1,_value_,key2
```

注意: value フィールドが指定されていない場合、自動的に一致する正規表現の数になります。

注意 2: 1つだけ *value* カラムが指定されている場合は、累積値(デフォルトではパフォーマンス)を表すか、チェックボックスをオンにして平均を表すかを選択できます。

例

以下のフォーマットのログからエントリを取得するとします。

```
 Sep 19 12:05:01 nova systemd: Starting Session 6132 of user root.
 Sep 19 12:05:01 nova systemd: Starting Session 6131 of user root.
```

ユーザのログイン数をカウントするには、次のようにします。

正規表現:

```
Starting Session \d+ of user (.*?)\.
```

フィールド:

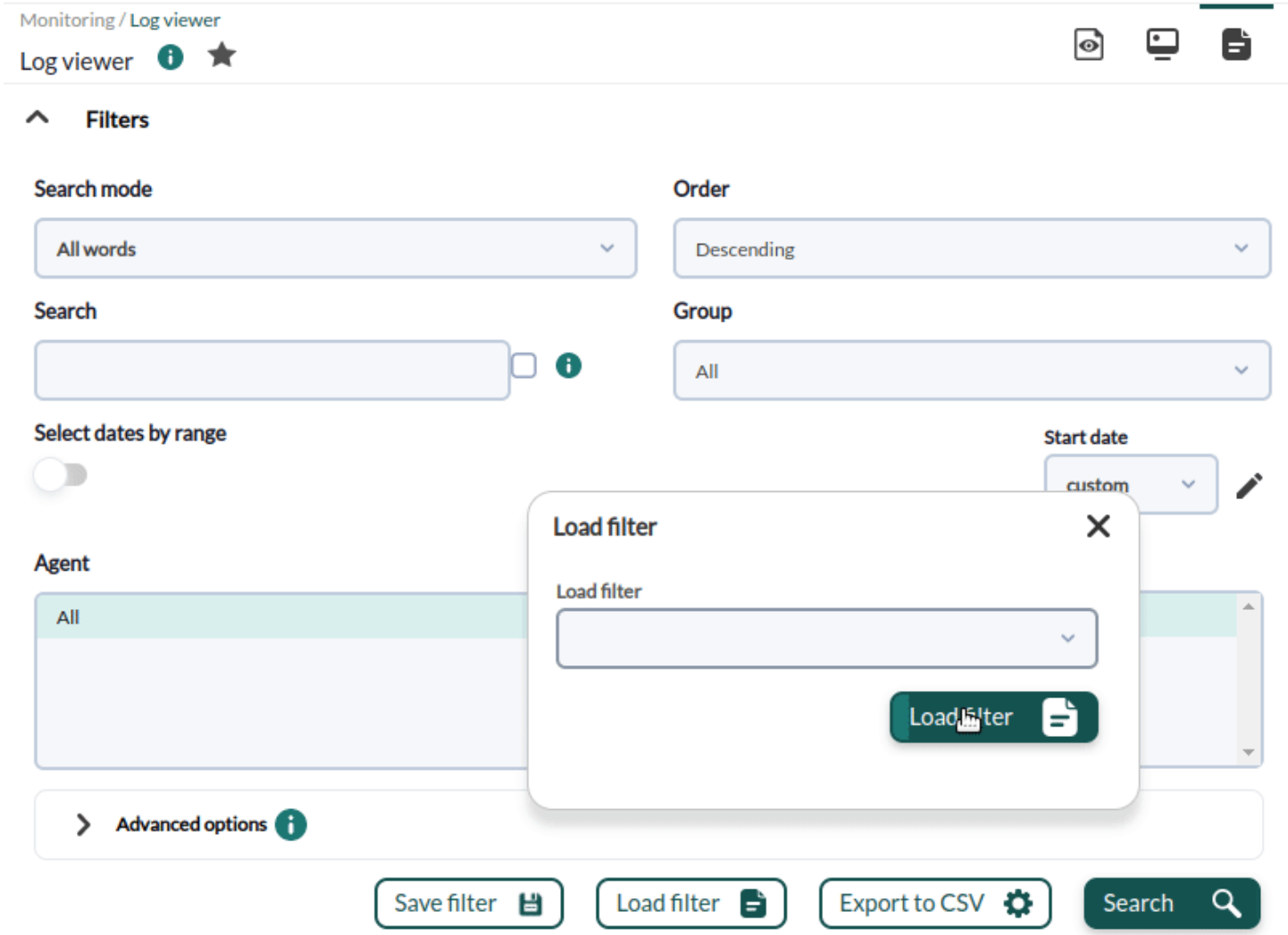
```
username
```

このキャプチャテンプレートは、選択した時間間隔におけるユーザのログイン数を返します。

頻繁に使用するフィルタ

バージョン 771 以降

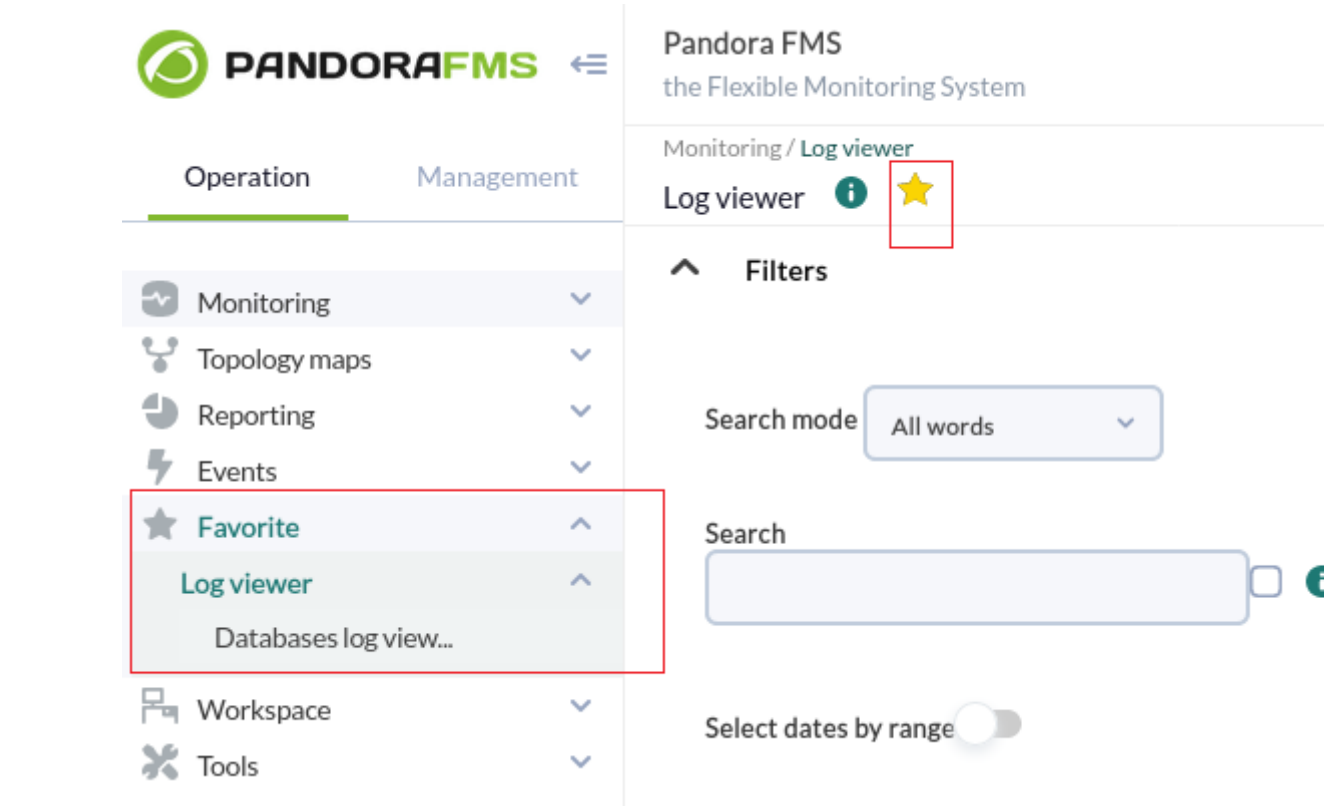
このオプションを使用すると、頻繁に使用するフィルタ設定を保存し、そのフィルタの一覧を作成できます。 すべてのフィルタ値を設定したら、フィルターの保存(Save filter) をクリックし、名前を割り当てて、保存(Save) をクリックします。 いつでも、保存されたフィルタをドロップダウンリストから選択し、フィルタの読み込み(Load filter) ボタンを使用してこれらの設定を読み込むことができます。



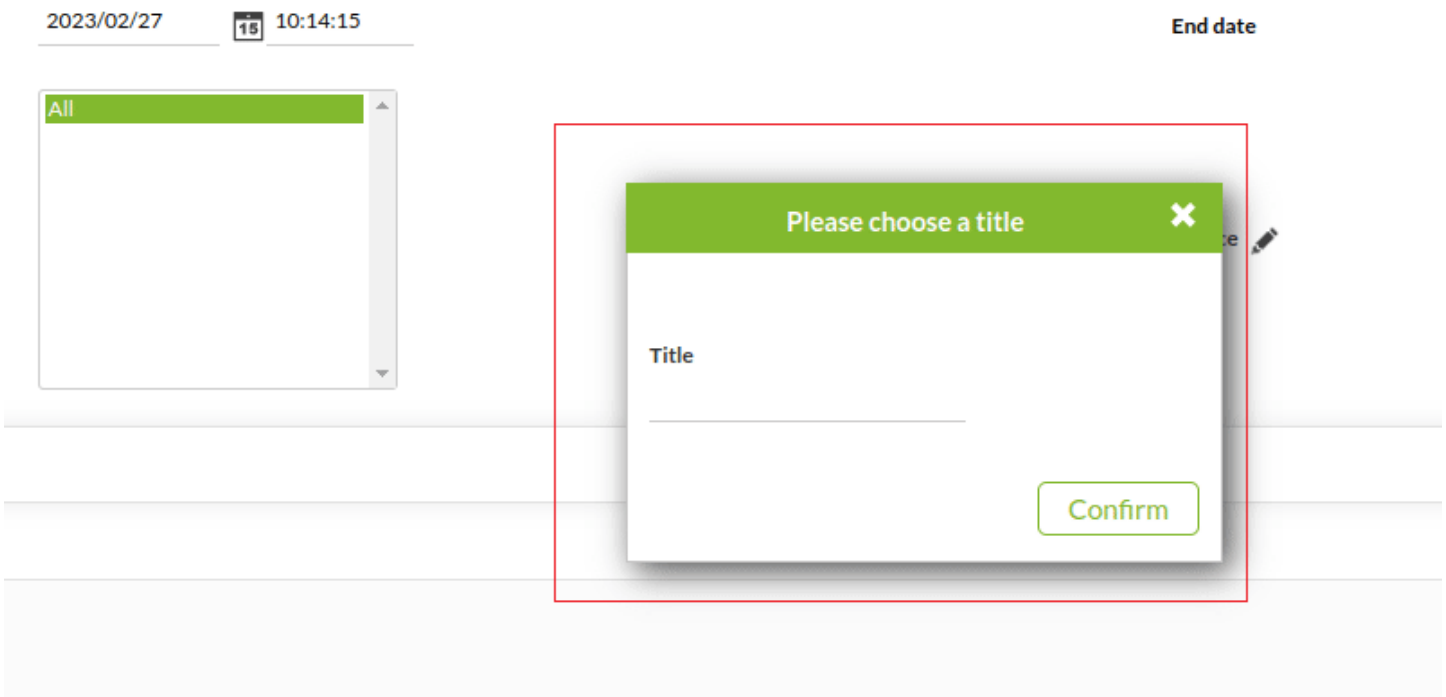
お気に入り要素として保存されたフィルタ

バージョン NG 770 以降

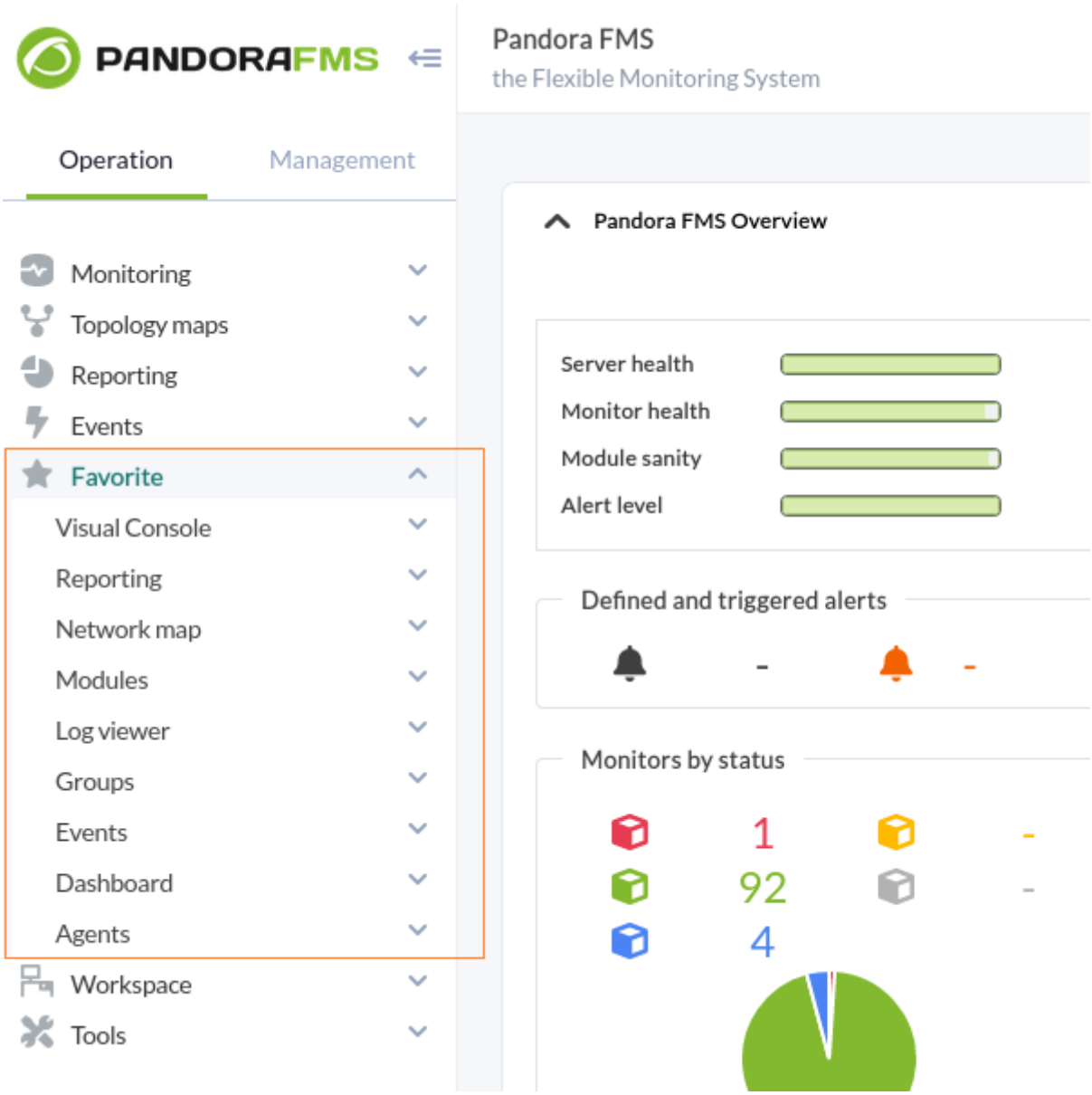
お気に入り システムを使用すると、タイトルの星アイコンをクリックして、フィルタ設定を含む ログビューア へのショートカットを保存できます。



設定したフィルタリング条件をお気に入りとして保存するための名前を求められます。



ログビューワ フィルタ設定は、お気に入り(Favorite) (操作(Operation) メニュー) の対応するセクションに保存されます。



エージェント設定

ログ収集は、Windows および Unux (LInux®, MacOS X®, Solaris®, HP-UX®, AIX®, BSD® など) エージェント双方で実行されます。Windows エージェントの場合、イベントビューワモジュールで同様のフィルタを用いることにより、Windows イベントビューワから情報を取得することもできます。

Windows と Unix でのログ情報収集の例をみてみます。

Windows の場合

バージョン 750 以降、このアクションは、詳細オプションを有効化することにより、エージェントプラグインを介して実行できます。

以下に示すタイプの処理を実行できるようになります。

Logchannel module

```
module_begin
module_name MyEvent
module_type log
module_logchannel
module_source <logChannel>
module_eventtype <event_type/level>
module_eventcode <event_id>
module_pattern <text substring to match>
module_description <description>
module_end
```

Logevent module

```
module_begin
module_name Eventlog_System
module_type log
module_logevent
module_source System
module_end
```

Regexp module

```
module_begin
module_name PandoraAgent_log
module_type log
module_regexp C:\archivos de programa\pandora_agent\pandora_agent.log
module_description This module will return all lines from the specified logfile
module_pattern .*
module_end
```

ログタイプモジュールの詳細説明については、次の章で確認できます。特定のディレクティブ

```
module_type log
```

この種のタグ module_type log**を 定義すると、データベースには保存されませんが、ログコレクターに送信されていることを示します。このタイプのデータを持つモジュールは、有効になっている場合はコレクターに送信され、有効になっていない場合は情報が破棄されます。**

注意: **この書式は、バージョン 5.0 以上で有効です**Enterprise **版をアップデートした状態にしているか確認してください。**

Unix システム

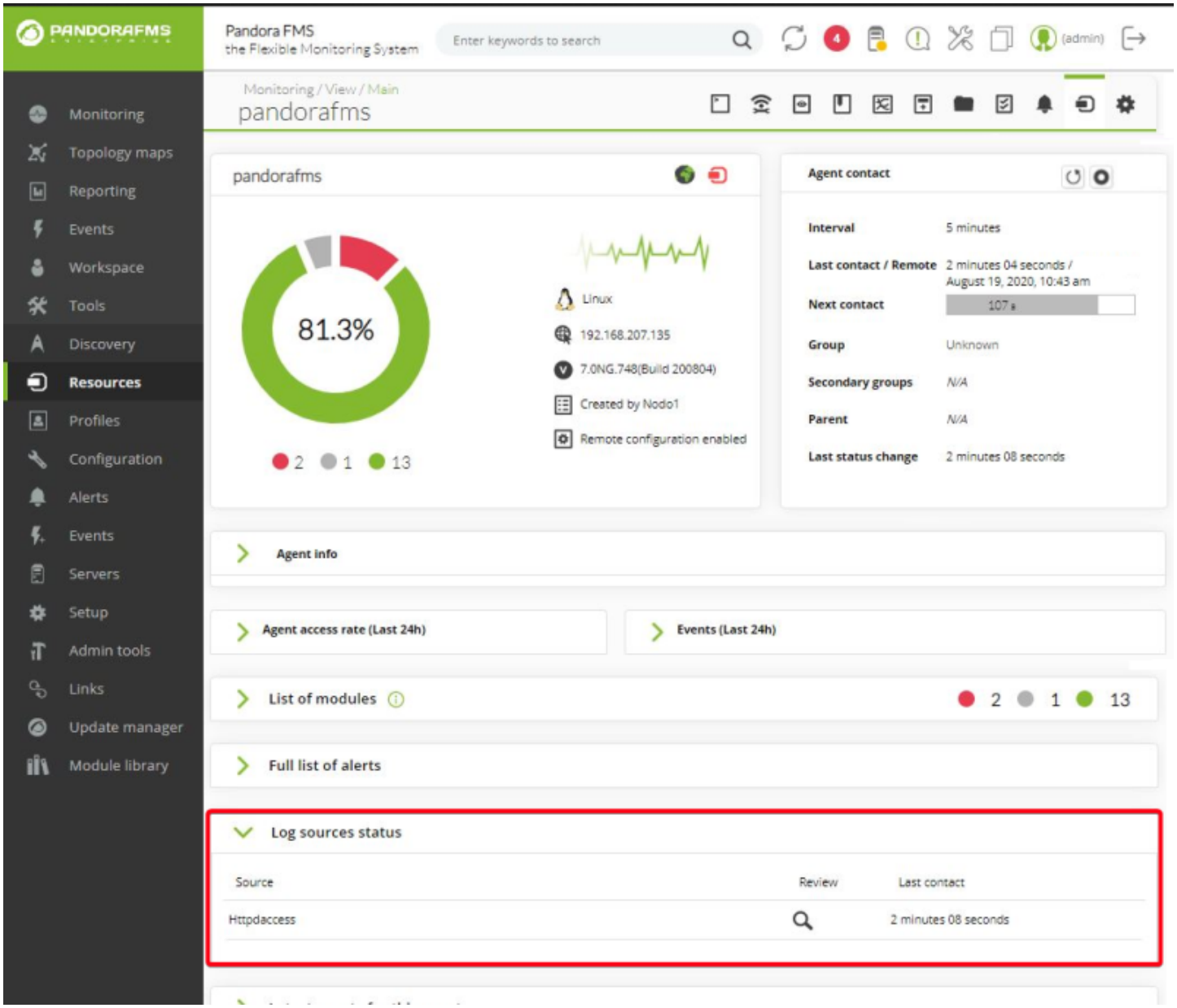
エージェントバージョン 5.0 では、次の書式を使います。

```
module_plugin grep_log_module /var/log/messages Syslog \.\*
```

ログパースプラグイン(grep_log)と同じように grep_log_module プラグインは、処理した情報をログファイルのソースとして “syslog” という名前でログ収集に送信します。どういったパターンの行を送信するかまたはしないかは、\.* といった 正規表現を利用します(この例では全て)。

エージェント表示でのログソース

Pandora FMS バージョン 749 以降、ログソース状態 と呼ばれるボックスがエージェント表示に追加され、そのエージェントによる最後のログ更新の日付が表示されます。虫眼鏡のアイコンをクリックすると、そのログにフィルタしたログビューワ表示にリダイレクトされます。



Pandora FMS ドキュメント一覧に戻る