Alibaba Cloud Elasticsearch

Cloud Monitor

Document Version20190716

目次

1 ES CloudMonitor アラーム

Elasticsearch は、インスタンスのモニタリングをサポートし、テキストメッセージによるアラートを送信できます。 必要に応じて、アラートのしきい値を設定できます。

重要

モニタリングアラートを設定することを推奨します。

- クラスターのステータス (クラスターのステータスインジケーターが、緑色または赤色かどうか)
- ノードディスク使用率 (%) (アラートのしきい値は 75%未満にする必要があります。80%を超えることはできません)
- ノードのヒープメモリ使用率 (%) (アラートのしきい値は 85%未満にする必要があります。90%を超えることはできません)

その他の要件

- ノードの CPU 使用率 (%) (アラートのしきい値は 95%を超えることはできません)
- ノードの load_1m (基準値は、CPU コア数の 80%)
- クラスタークエリ QPS (カウント/秒) (基準値は、実際のテスト結果)
- クラスター書き込み QPS (カウント/秒) (基準値は、実際のテスト結果)

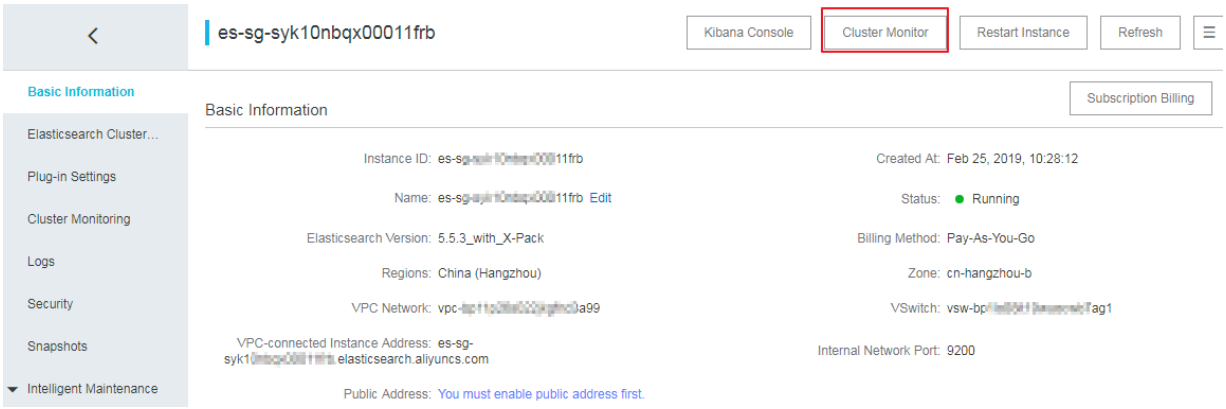
使用方法

入力モード

- Elasticsearch コンソール
- CloudMonitor の [Elasticsearch] タブページ

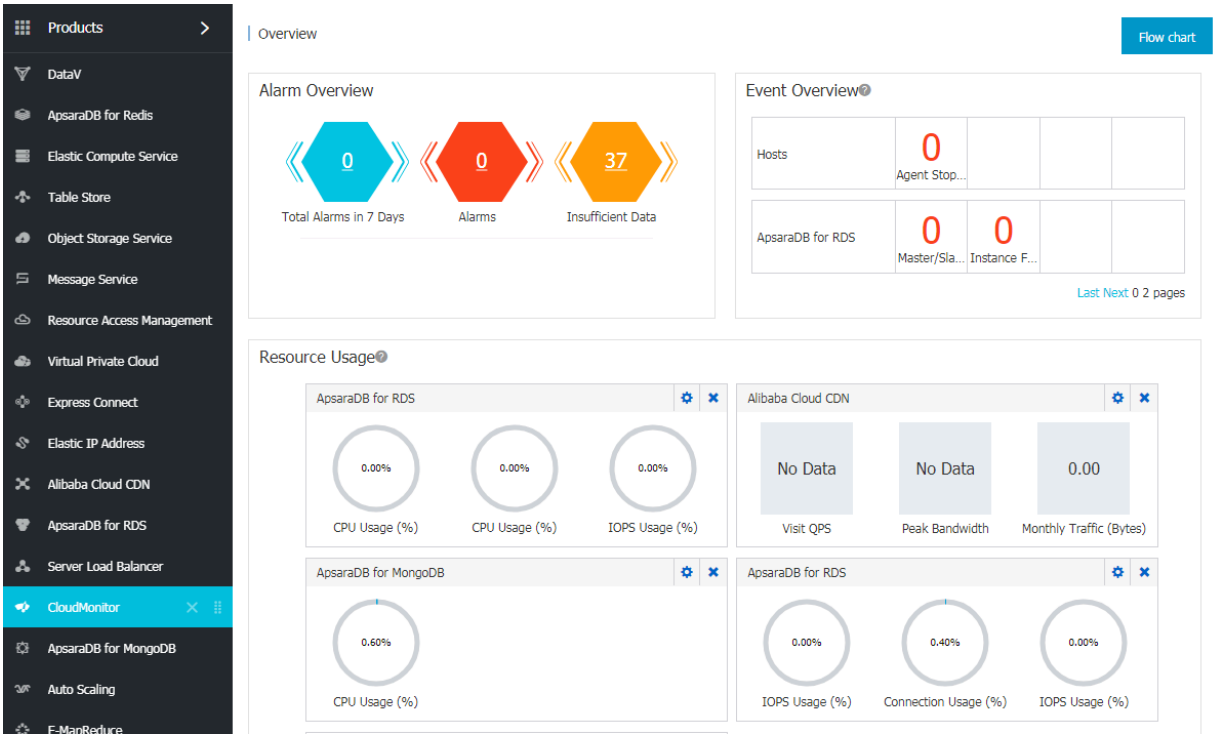
Elasticsearch コンソール

ES コンソールにログインし、ES インスタンスの [基本情報] ページに移動します。 [クラスターモニタリング] をクリックして、ES Cloud Monitor モジュールに移動します。



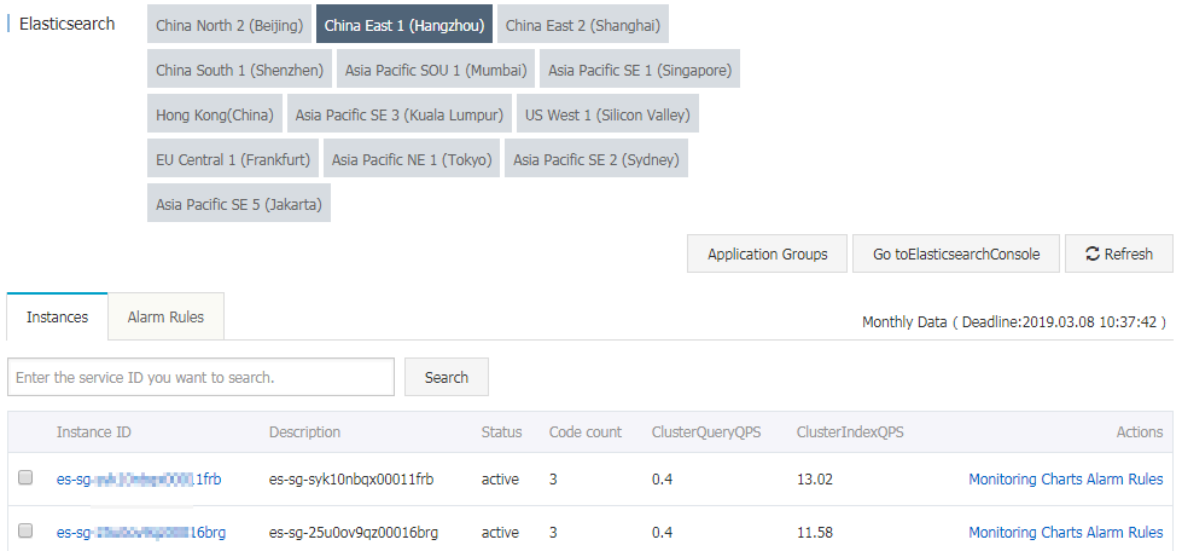
CloudMonitor の [Elasticsearch] タブ

アカウントを使用して Alibaba Cloud コンソールにログインし、プロダクトナビゲーターで [Cloud Monitor] を選択します。[クラウドサービスモニタリング] メニューから [Elasticsearch] を選択します。



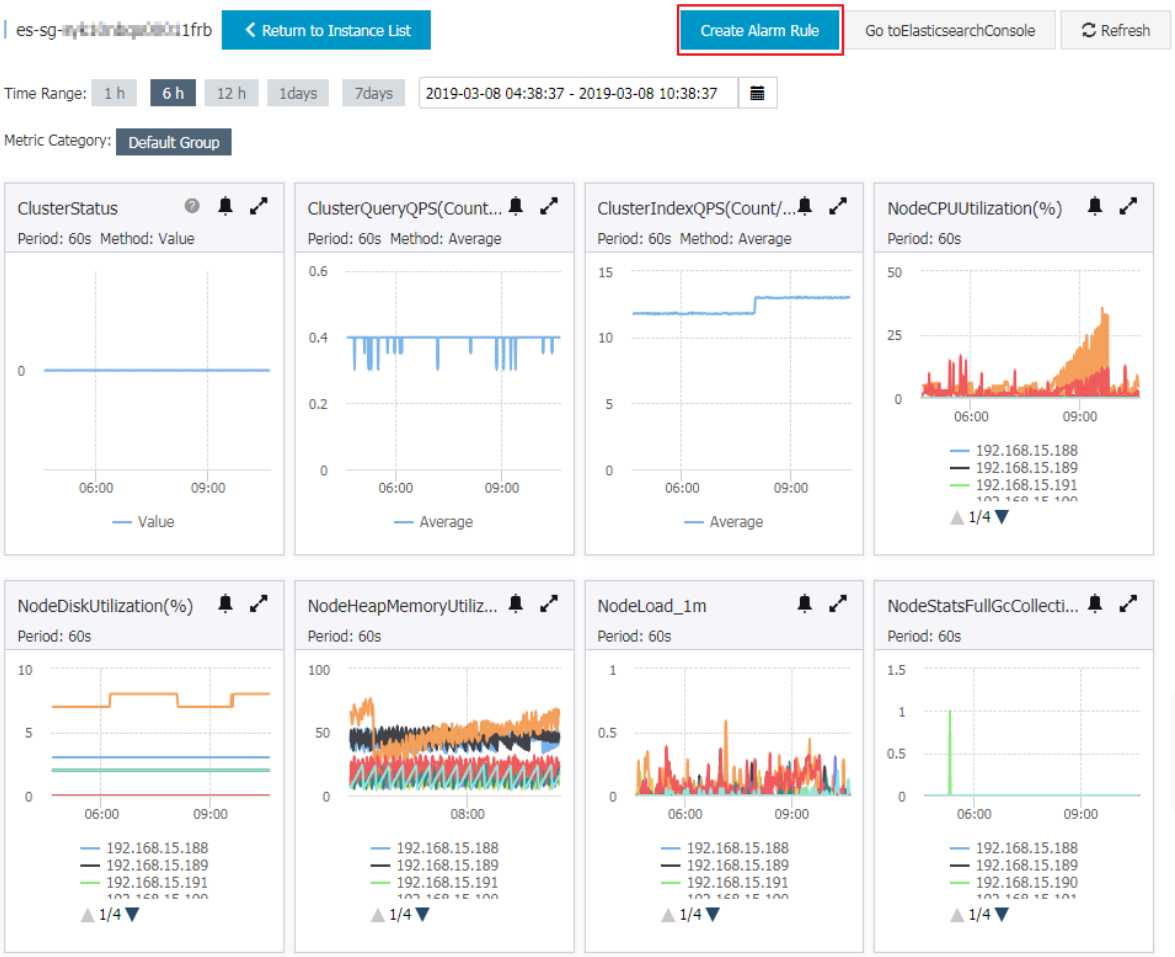
モニタリングインデックスの設定

1. 確認するリージョンを選択し、ES インスタンス ID をクリックします。



2. インデックスの詳細ページで、アラートポリシーを作成します。

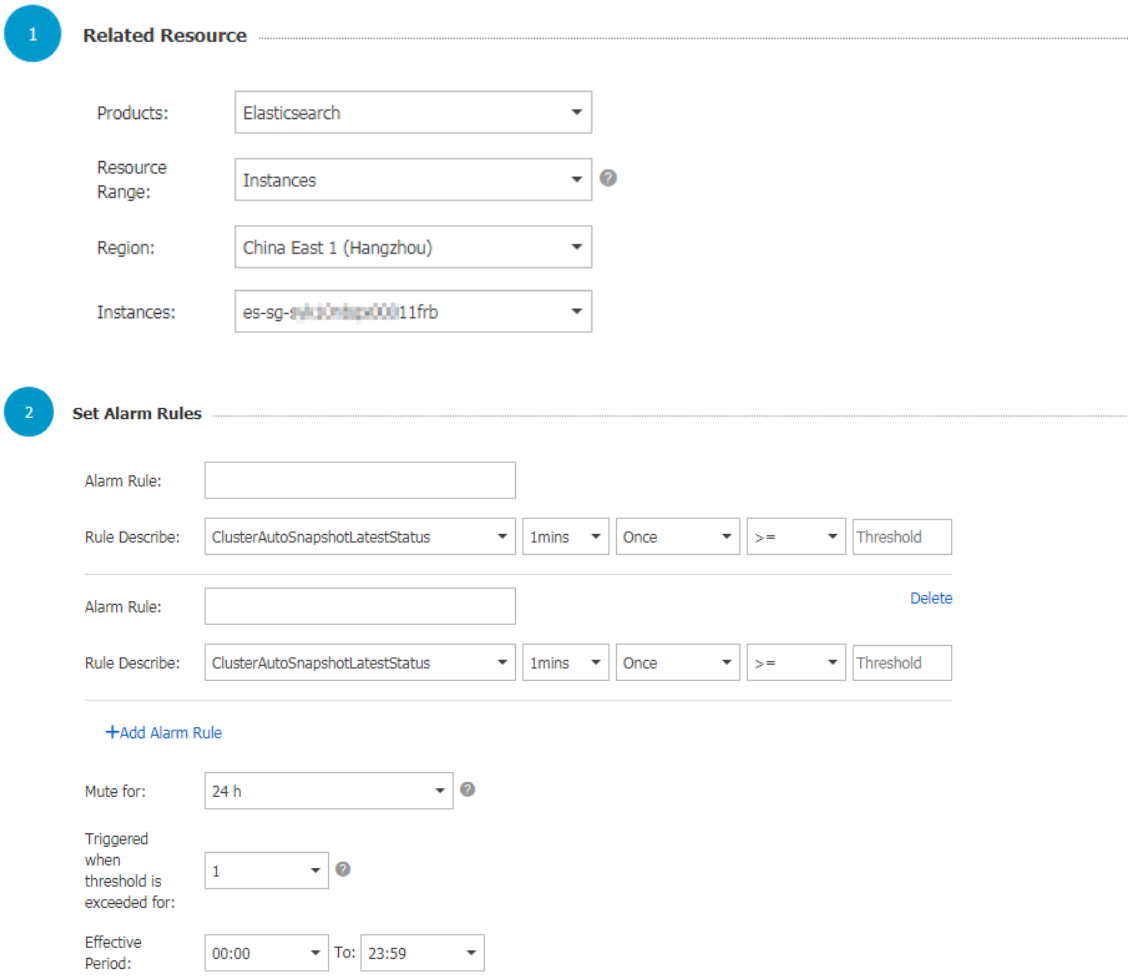
   このページでは、過去のクラスターモニタリング統計を確認できます。 過去 1 か月のモニタリング統計が保存されています。 アラートポリシーを作成すると、このインスタンスのアラートモニタリングを設定できます。



3. ポリシーの名前と説明を入力します。

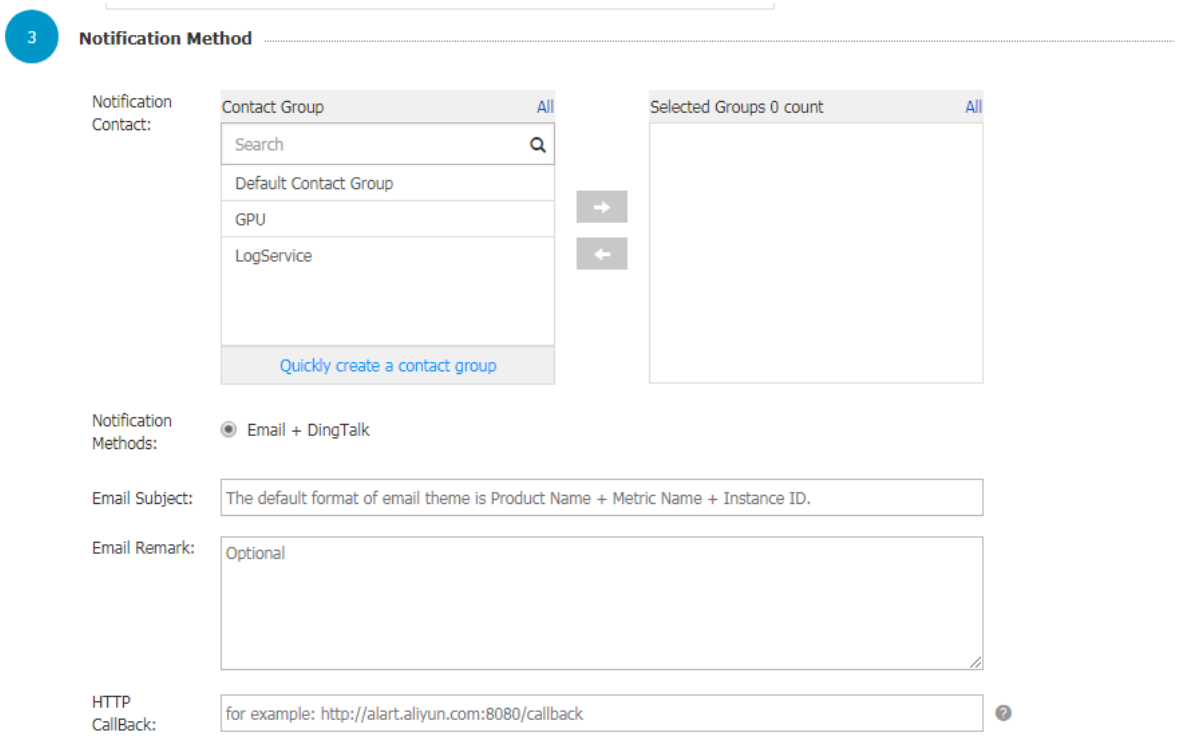
   次の例では、ディスク使用率、クラスターのステータス、およびノードのヒープメモリ使用率に関するモニタリングが設定されています。

   - クラスターのステータスである、緑、黄、赤は、それぞれ ０．０、１．０、２．０ に対応します。 クラスターステータスのアラートインデックスの設定値を設定します。
   - チャネルのサイレント時間内に、１つのインデックスで１回のみアラートがトリガーされます。

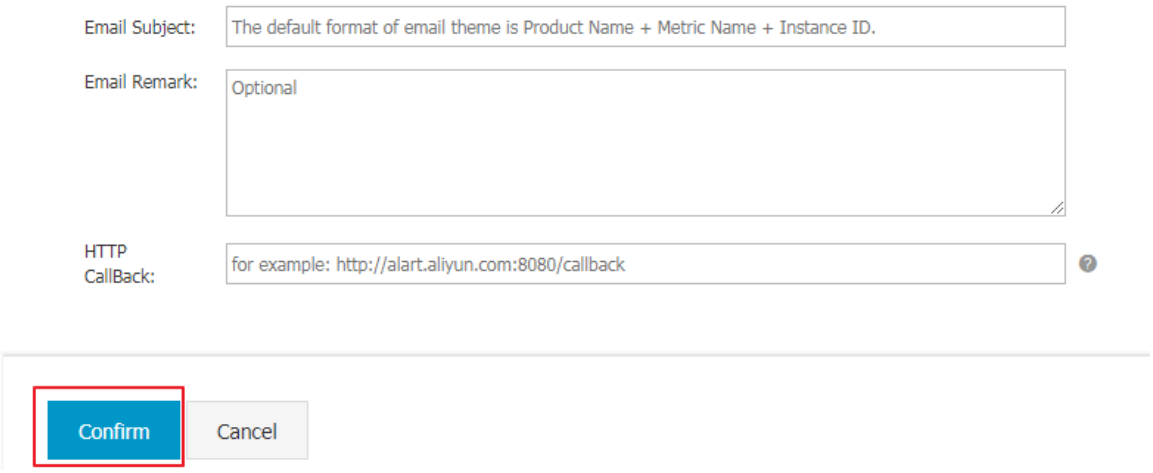


4. アラート連絡先グループを選択します。

   連絡先グループを作成するには、[送信先グループの作成] をクリックします。



5. [確認] をクリックしてアラート設定を保存します。



注：

Elasticsearch のモニタリングデータは、インスタンスが正常に実行されてから 5 分後に収集されます。 その後、モニタリング統計情報が表示されます。

2 XPack Watcher

概要

モニタリングとアラームのサービスとして Watcher を Elasticsearch に追加すると、特定の条件が満たされたときにアクションをトリガーできます。 たとえば、ログインデックスに ERROR が含まれている場合、メールでアラームが自動送信されます。

機能

Watcher は、Trigger、Input、Condition、Action など、複数の機能をサポートしています。

Trigger

Trigger は、ウォッチを実行する日時を決定します。 ウォッチを設定するには、Trigger が必要です。 Watcher は複数のタイプのスケジュールトリガーを提供します。 詳細は、『Schedule Trigger』をご参照ください。

Inputs

inputs を使用して、Watcher でモニタリングするインデックスをフィルタリングできます。 詳細は、『Inputs』をご参照ください。

Conditions

condition は、actions を実行するかどうかを決定します。

Actions

特定の条件が満たされると actions が実行されます。

設定

Elasticsearch のウォッチは、パブリックネットワークを介して通信できません。 VPC ネットワーク経由でのみインスタンスの内部エンドポイントにアクセスできます。 Watcher を使用するには、パブリックネットワークと Elasticsearch インスタンスの両方にアクセスできる ECS インスタンスを作成する必要があります。 ECS インスタンスは、アクションを実行するためのプロキシとして動作します。

次の例は、Webhook アクションの設定方法を示します。 この例では、DingTalk Chatbot を使用しています。

1. ECSインスタンスの購入

   ECSインスタンスを購入します。 ECS インスタンスがインターネットにアクセスできることを確認します。

   > 注：
   >
   > - ECS インスタンスと Elasticsearch インスタンスは同じ VPC ネットワークを共有する必要があります。
   > - ECS インスタンスはパブリックネットワークにアクセスできる必要があります。

2. セキュリティグループの設定

   ECS コンソールの [インスタンス] ページに移動し、ターゲットインスタンスの右側にある [詳細] をクリックし、[セキュリティグループの設定]を選択し、[セキュリティグループリスト] ページでセキュリティグループルールを追加します。

   - ルールの方向 を [受信] に設定します。
   - 許可ポリシーのデフォルトアクションである [許可] を使用します。
   - カスタムプロトコルを [Custom TCP] に設定します。
   - デフォルトのプライオリティ設定を使用します。
   - 必要に応じてポート範囲を設定します。 この例では、Nginx にポート 8080 を使用します。
   - 許可タイプを CIDR に設定します。
   - Elasticsearch インスタンスのすべてのノードの IP アドレスを許可オブジェクトとして追加します。

   > 注：
   > Elasticsearch インスタンスの IP アドレスリストの取得
   >
   > 購入した Elasticsearch インスタンスの Kibana コンソールにログインし、[Monitoring]、[Nodes] の順にクリックすると、Elasticsearch インスタンスのすべてのノードの IP アドレスが表示されます。

3. Nginx プロキシの設定

   a. Nginx 設定ファイルを変更します。 次の例では、Nginx 設定ファイルでサーバーを設定する方法を示します。

   ```
   server
    {
       listen   8080 ;# Listening   port
       server_nam  e   localhost ;# Domain   name
   ```

```
    index   index . html   index . htm   index . php ;
    root  / usr / local / webserver / nginx / html ;# Website
directory
      location  ~ . *\.( php | php5 )? $
   {
     # fastcgi_pa  ss   unix :/ tmp / php - cgi . sock ;
      fastcgi_pa  ss   127 . 0 . 0 . 1 : 9000 ;
      fastcgi_in  dex   index . php ;
      include   fastcgi . conf ;
   }
    location  ~ . *\.( gif | jpg | jpeg | png | bmp | swf | ico
)$
   {
      expires   30d ;
 #  access_log   off ;
   }
    location  / {
      proxy_pass   Paste   the   Webhook   address   of   the
DingTalk   Chatbot   here .
   }
    location  ~ . *\.( js | css )? $
   {
      expires   15d ;
  #  access_log   off ;
    }
    access_log   off ;
  }
}
```

b. Nginx 設定ファイルを設定したら、設定ファイルを再ロードし、Nginx を再起動します。

```
/ usr / local / webserver / nginx / sbin / nginx  - s   reload  #
 Reload   the   configurat  ion   file
/ usr / local / webserver / nginx / sbin / nginx  - s   reopen  #
 Restart   Nginx
```

注：

DingTalk Chatbot の Webhook アドレスの取得

DingTalk アラーム受信グループを作成します。右上隅の [Group Settings] をクリックし、[ChatBot] を選択し、Webhook ロボットを追加してから、ロボットの Webhook アドレスを取得します。

4. アラームの設定

a. Elasticsearch インスタンスの Kibana コンソールにログインし、左側の [Dev Tools] タブをクリックします。次の例では、log_error_watch という Watcher を作成して、ログインデックスに ERROR が含まれているかどうかを 10 秒ごとに確認する方法を示します。エラーログエントリが検出されると、アラームがトリガーされます。

```
 PUT   _xpack / watcher / watch / log_error_  watch
{
  " trigger ":  2
    " schedule ": {
      " interval ": " 10s "
    }
```

```
  },
  " inputs ": [
    " search ": {
      " request ": {
        " indices ": [" logs "],
        " body ": {
          " query ": {
            " match ": {
              " message ": " error "
            }
          }
        }
      }
    }
  },
  " condition ": {
    " compare ": {
      " ctx . payload . hits . total ": {
        " gt ":  0
      }
    }
  },
  " actions " : {
  " test_issue " : {
    " webhook " : {
      " method " : " POST ",
      " url " : " http ://  The   private   IP   address   of
 your   ECS   instance : 8080 ",
      " body " : "{\" msgtype \": \" text \", \" text \": { \"
 content \": \" An   error   log   entry   has   been   detected
 .  Handle   the   issue   immediatel  y .\"}}"
    }
  }
}
}
```

注：

actions の URL は、Elasticsearch インスタンスと同じリージョンと VPC を共有する ECS インスタンスの内部 IP アドレスでなければなりません。 この例の以降の手順に従って作成されたセキュリティグループに ECS インスタンスが追加されている必要があります。 そうしないと、ECS インスタンスは Elasticsearch インスタンスと通信できません。

b. Watcher を削除するには、次のコマンドを実行します。

```
DELETE   _xpack / watcher / watch / log_error_  watch
```

よくある質問

- **URI のハンドラーが見つかりません**

  次のエラーメッセージは、Elasticsearch インスタンスの Watcher 機能が有効になっていないことを示しています。 Elasticsearch コンソールの [インスタンス管理] ページに移動

し、[詳細設定] > [YML ファイル] を選択し、`xpack . watcher . enabled : true` を追加します。

No handler found for uri [/_xpack/watcher/watch/log_error_watch_2] and method [PUT]

注：

`. watcher - history` インデックスは、定期的に消去されません。不要になった `. watcher - history` インデックスは、手動で消去する必要があります。インデックスを削除する API 操作を呼び出すよう、ECS インスタンスでタスクをスケジュールすることができます。

3 ログモニタリング

Elasticsearch は、オープンソースの Elasticsearch v5.5.3 と X-Pack Business Edition を提供し、データ分析やデータ検索などのシナリオに対応します。 エンタープライズレベルの権利管理、セキュリティモニタリングアラート、自動レポート生成など、さまざまな機能がオープンソースの Elasticsearch に基づいて作成されています。

モニタリングログの設定

ログ収集

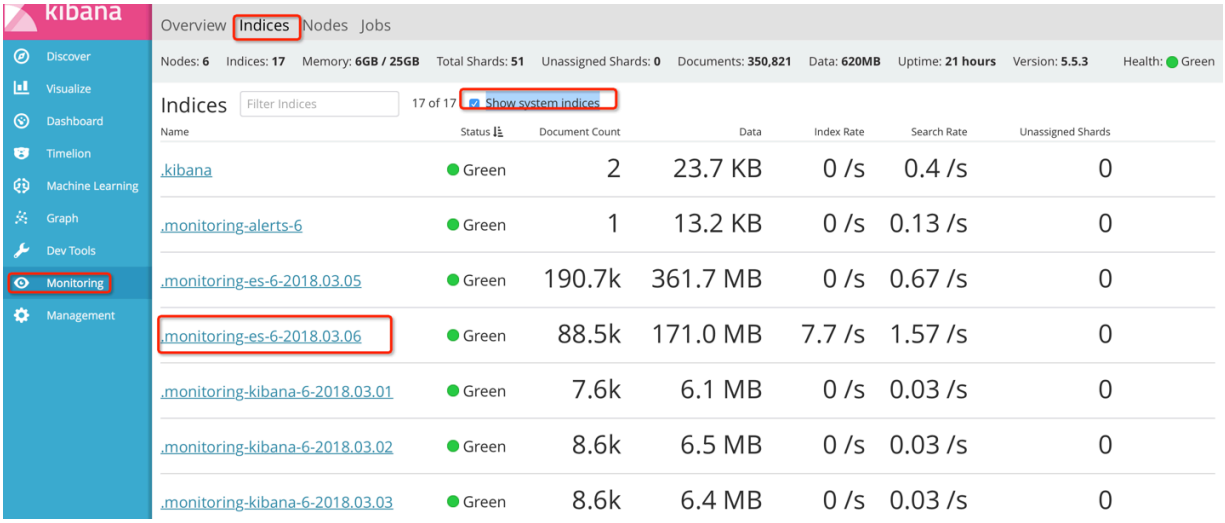
デフォルトでは、X-Pack はクライアントをモニタリングし、購入したインスタンスの `.monitoring-*` という接頭辞が付いたインデックスに、収集したクラスター情報を 10 秒ごとに送信します。

インデックス `.monitoring-es-6-*` と `.monitoring-kibana-6-*` が利用可能で、毎日作成されます。 収集された情報は `.monitoring-es-6-` という接頭辞のインデックスに保存され、現在の日付が末尾に付けられます。

`.monitoring-es-6-*` インデックスは、比較的大きなディスク容量を占有します。 クラスターのステータス、クラスター統計、ノード統計、インデックス統計などの情報を保存します。

システムインデックスの表示

Kibana ページで [Show system indices] を選択すると、インデックスが占有する容量が表示されます。



ログ保存

デフォルトでは、過去 7 日間のモニタリング対象のインデックスが保存されます。 これらの .monitoring-es-6-* インデックスは、ES インスタンスの容量を占有します。 インデックスサイズは、クラスター内のインデックス数 (システムインデックスを含む) とノード数によって異なります。 インデックスがインスタンス容量の大半を占有しないようにするには、次の方法を使用します。

1. 次の API を使用して、インデックス保持日数を設定する

```
PUT _cluster/settings
{"persistent": {"xpack.monitoring.history.duration":"1d"}}
# The number of days shall be configured according to your requirements. The indexes shall be retained at least one day.
```

2. モニタリング対象のインデックスを指定する

   API でモニタリングする必要のあるインデックスを指定することで、.monitoring-es-6-* インデックスが占有するディスク容量を削減できます。 次の例では、システムインデックスはモニタリングされません。

```
PUT _cluster/settings
{"persistent": {"xpack.monitoring.collection.indices":"*,-.*"}}
# The disabled index information is not displayed in the Monitoring module of Kibana. For example, you cannot see the disabled index information in the index list or on the index monitoring page. In this situation, the index list obtained through _cat/indices is different from the index list displayed in the Monitoring module of Kibana.
```

注:

実際には、両方の方法を使用してディスク容量を節約できます。