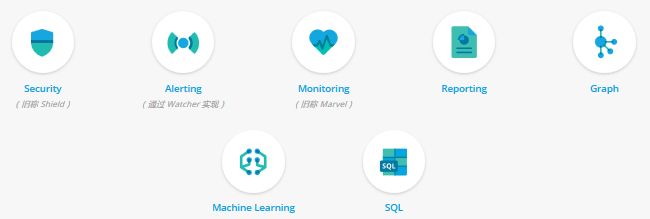
**X-Pack**

# 简介

X-Pack 是一个 Elastic Stack 的扩展组件包，将 security, alerting, monitoring, reporting, and graph 功能打在一个易于安装的包中。X-Pack组件被设计成无缝地协同工作，但是您可以很容易地启用或禁用您想要使用的特性。部分组件是收费的。

对于Elasticsearch 5.0.0以前的版本,你需要一个一个安装 Shield, Watcher, and Marvel 这些被统一打在X-Pack包中的插件。还需要选对这些插件的版本。使用x-pack就只需要选择和Elasticsearch版本一致的即可。

当前6.2.4版本中包含的功能组件：



Security：为ES stack 提供安全防护。

Alerting：提供告警能力，让你实时获知集群的异常状态

Monitoring：提供ES stack的监控能力，一目了然掌握集群的健康状况，及故障诊断。

Reporting：能够为任何 Kibana 可视化或仪表板快速生成报告。您可以即需即取报告、预约报告、根据特定条件触发报告，并自动将报告分享给指定的人员。

Graph：提供分析数据间关系的功能。

Machine Learning：提供机器学习能力。

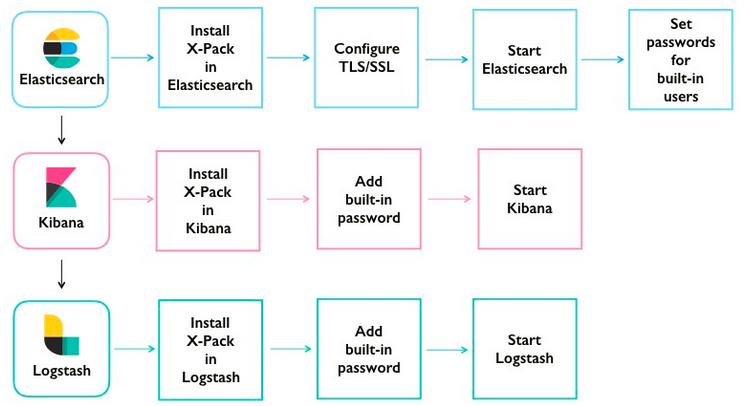
SQL：6.3.0版本新推出的SQL查询能力，让我们可以通过写SQL来进行查询。当前还是一个beta版本。

# 安装&配置

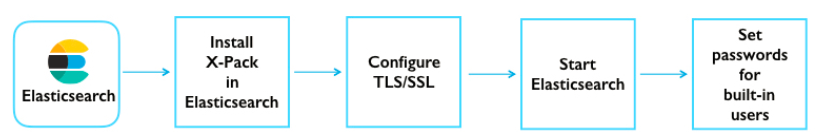
## 安装步骤

前置条件：先得安装elasticsearch、kibana。如果想在Logstash中也使用x-pack，先安装logstash。

安装流程：



### 在elasticsearch上安装x-pack



1. 安装 x-pack

如果你的机器能访问外网，可以直接用如下命令进行安装：

Linux：bin/elasticsearch-plugin install x-pack

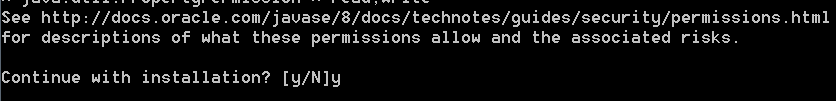
Windows：bin/elasticsearch-plugin.bat install x-pack

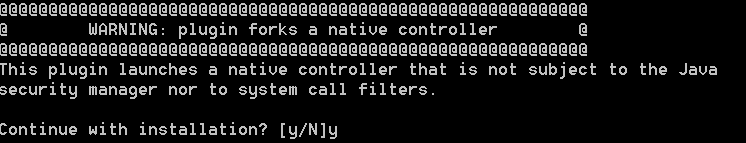
如果不能访问外网，则将x-pack的包下载下来，在安装命令中用 file指定安装包文件

下载地址：<https://artifacts.elastic.co/downloads/packs/x-pack/x-pack-6.2.4.zip> kibana和logstash的插件也在这个包中。

安装命令：bin/elasticsearch-plugin install file:///path/to/file/x-pack-6.2.4.zip

安装过程中，会向你确认向 x-pack 附加权限。可在安装命令上带--batch 选项自动授权。





安装完成后会在es中自动创建如下索引（这要求你的es中的允许自动创建索引打开，action.auto\_create\_index in elasticsearch.yml）

action.auto\_create\_index: .security,.monitoring\*,.watches,.triggered\_watches,.watcher-history\*,.ml\*

x-pack工作过程中的数据也会存到集群中。

1. 配置加密传输（TSL/SSL）

这个特性是收费的。

需要在各个节点上创建证书，并启用TSL

1. 启动/重启elasticsearch

bin/elasticsearch

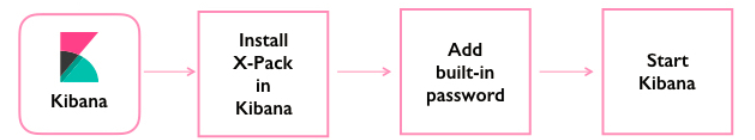
1. 为内建的初始用户 elastic kibana logstash 设置密码

bin/x-pack/setup-passwords interactive

交互式的为三个用户设置密码

### 在 kibana 上安装 x-pack

流程：



步骤命令：

1. 安装 x-pack

如果你的机器能访问外网，可以直接用如下命令进行安装：

Linux：bin/kibana-plugin install x-pack

Windows：bin/kibana-plugin.bat install x-pack

如果不能访问外网，则将x-pack的包下载下来。

安装命令：bin/kibana-plugin install file:///path/to/file/x-pack-6.2.4.zip

The Kibana server needs to be able to write to files in the optimize directory. If you’re using sudo or su, run the plugin installation as the built-in kibana user. For example:

sudo -u kibana bin/kibana-plugin install x-pack

1. 在kibana的配置文件 kibana.yml中配置内建用户kibana的密码

elasticsearch.username: "kibana"

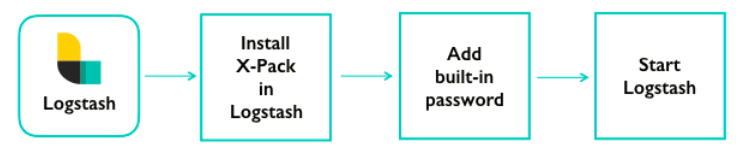
elasticsearch.password: "kibanapassword"

1. 启动/重启kibana
2. 以有kibana\_user角色的用户登录 http://localhost:5601

### 在 logstash 上安装 x-pack

在logstash上安装 x-pack是可选的。如果你想安装，流程如下。如果不安装，为了让logstash能访问elasticsearch索引数据，只需在配置文件logstash.yml中配置访问es的用户密码（下图的步骤2）

流程：



步骤命令：

1. 安装 x-pack

如果你的机器能访问外网，可以直接用如下命令进行安装：

Linux：bin/logstash-plugin install x-pack

Windows：bin/logstash-plugin.bat install x-pack

如果不能访问外网，则将x-pack的包下载下来。

安装命令：bin/logstash-plugin install file:///path/to/file/x-pack-6.2.4.zip

1. 在logstash的配置文件 logstash.yml中配置内建用户logstash\_system的密码

xpack.monitoring.elasticsearch.username: logstash\_system

xpack.monitoring.elasticsearch.password: logstashpassword

1. 启动/重启logstash

## 启用/禁用x-pack中的特性

By default, all X-Pack features are enabled. You can enable or disable specific X-Pack features in the elasticsearch.yml, kibana.yml, and logstash.yml configuration files.

| **Setting** | **Description** |
| --- | --- |
| xpack.graph.enabled | Set to false to disable X-Pack graph features. |
| xpack.ml.enabled | Set to false to disable X-Pack machine learning features. |
| xpack.monitoring.enabled | Set to false to disable X-Pack monitoring features. |
| xpack.reporting.enabled | Set to false to disable X-Pack reporting features. |
| xpack.security.enabled | Set to false to disable X-Pack security features. |
| xpack.watcher.enabled | Set to false to disable Watcher. |

| **X-Pack Feature** | **Elasticsearch Settings** | **Kibana Settings** | **Logstash Settings** |
| --- | --- | --- | --- |
| APM UI | No | [Yes](https://www.elastic.co/guide/en/kibana/6.2/apm-settings-kb.html) | No |
| Development Tools | No | [Yes](https://www.elastic.co/guide/en/kibana/6.2/dev-settings-kb.html) | No |
| Graph | No | [Yes](https://www.elastic.co/guide/en/kibana/6.2/graph-settings-kb.html) | No |
| Machine learning | [Yes](https://www.elastic.co/guide/en/elasticsearch/reference/6.2/ml-settings.html) | [Yes](https://www.elastic.co/guide/en/kibana/6.2/ml-settings-kb.html) | No |
| Management | No | No | [Yes](http://www.elastic.co/guide/en/logstash/6.2/configuring-centralized-pipelines.html#configuration-management-settings) |
| Monitoring | [Yes](https://www.elastic.co/guide/en/elasticsearch/reference/6.2/monitoring-settings.html) | [Yes](https://www.elastic.co/guide/en/kibana/6.2/monitoring-settings-kb.html) | [Yes](http://www.elastic.co/guide/en/logstash/6.2/configuring-logstash.html#monitoring-settings) |
| Reporting | No | [Yes](https://www.elastic.co/guide/en/kibana/6.2/reporting-settings-kb.html) | No |
| Security   * Auditing | [Yes](https://www.elastic.co/guide/en/elasticsearch/reference/6.2/security-settings.html) | [Yes](https://www.elastic.co/guide/en/kibana/6.2/security-settings-kb.html) | No |
| [Yes](https://www.elastic.co/guide/en/elasticsearch/reference/6.2/auditing-settings.html) | No | No |
| Watcher | [Yes](https://www.elastic.co/guide/en/elasticsearch/reference/6.2/notification-settings.html) | No | No |

## 卸载 x-pack

To uninstall X-Pack:

1. Stop Elasticsearch.
2. Remove X-Pack from Elasticsearch:

bin/elasticsearch-plugin remove x-pack

1. Restart Elasticsearch.
2. Remove X-Pack from Kibana:

bin/kibana-plugin remove x-pack

1. Restart Kibana.
2. Remove X-Pack from Logstash:

bin/logstash-plugin remove x-pack

1. Restart Logstash.

# Security

## Security简介

x-pack security 组件从下面三个方面为 ES stack 提供安全防护。

* [Preventing unauthorized access](https://www.elastic.co/guide/en/x-pack/current/elasticsearch-security.html#preventing-unauthorized-access) with password protection, role-based access control, and IP filtering.
* [Preserving the integrity of your data](https://www.elastic.co/guide/en/x-pack/current/elasticsearch-security.html#preserving-data-integrity) with message authentication and SSL/TLS encryption.
* [Maintaining an audit trail](https://www.elastic.co/guide/en/x-pack/current/elasticsearch-security.html#maintaining-audit-trail) so you know who’s doing what to your cluster and the data it stores.

### 工作原理

* User authentication
* Authorization and Role Based Access Control (a.k.a RBAC)
* Node/Client Authentication and Channel Encryption
* Auditing

### Authentication 认证

支持从多个安全数据源获取用户数据：

|  |  |
| --- | --- |
| native | An internal realm where users are stored in a dedicated Elasticsearch index. With this realm, users are authenticated by usernames and passwords. The users are managed via the [User Management API](https://www.elastic.co/guide/en/elasticsearch/reference/6.2/security-api-users.html). |
| ldap | A realm that uses an external LDAP server to authenticate the users. With this realm, users are authenticated by usernames and passwords. |
| active\_directory | A realm that uses an external Active Directory Server to authenticate the users. With this realm, users are authenticated by usernames and passwords. |
| pki | A realm that authenticates users using Public Key Infrastructure (PKI). This realm works in conjunction with SSL/TLS and identifies the users through the Distinguished Name (DN) of the client’s X.509 certificates. |
| file | An internal realm where users are defined in files stored on each node in the Elasticsearch cluster. With this realm, users are authenticated by usernames and passwords. The users are managed via dedicated tools that are provided by X-Pack on installation. |
| saml | A realm that uses SAML 2.0 Web SSO. This realm is designed to be used with Kibana. |

多个realm是如何工作的、及如何配置，详细参考：

https://www.elastic.co/guide/en/x-pack/current/how-authc-works.html

### authorization 鉴权

鉴权基于用户-角色-权限。

Secured Resource

A resource to which access is restricted. Indices/aliases, documents, fields, users and the Elasticsearch cluster itself are all examples of secured objects.

Privilege

A named group representing one or more actions that a user may execute against a secured resource. Each secured resource has its own sets of available privileges. For example, read is an index privilege that represents all actions that enable reading the indexed/stored data. For a complete list of available privileges see [Security Privileges](https://www.elastic.co/guide/en/x-pack/current/security-privileges.html).

Permissions

A set of one or more privileges against a secured resource. Permissions can easily be described in words, here are few examples:

* read privilege on the products index
* manage privilege on the cluster
* run\_as privilege on john user
* read privilege on documents that match query X
* read privilege on credit\_card field

Role

A named sets of permissions

User

The authenticated user.

权限有功能权限和数据权限，可类比数据库中的系统权限和对象权限。

数据权限粒度可控制到字段级别。

## 用户管理

### 内建用户

elastic

A built-in superuser. See [Built-in Roles](https://www.elastic.co/guide/en/x-pack/current/built-in-roles.html).

kibana

The user Kibana uses to connect and communicate with Elasticsearch.

logstash\_system

The user Logstash uses when storing monitoring information in Elasticsearch.

### 三种途径管理用户

#### 命令行

https://www.elastic.co/guide/en/elasticsearch/reference/6.2/users-command.html

用法：

bin/x-pack/users

([useradd <username>] [-p <password>] [-r <roles>]) |

([list] <username>) |

([passwd <username>] [-p <password>]) |

([roles <username>] [-a <roles>] [-r <roles>]) |

([userdel <username>])

示例

新增用户：

bin/x-pack/users useradd jacknich -p theshining -r network,monitoring

重置密码：

bin/x-pack/users passwd jachnich

修改用户角色，-r remove ， –a add

bin/x-pack/users roles jacknich -r network,monitoring -a user

删除用户：

bin/x-pack/users userdel jacknich

#### API

https://www.elastic.co/guide/en/elasticsearch/reference/6.2/security-api-users.html

GET /\_xpack/security/user

GET /\_xpack/security/user/<username>

DELETE /\_xpack/security/user/<username>

POST /\_xpack/security/user/<username>

PUT /\_xpack/security/user/<username>

PUT /\_xpack/security/user/<username>/\_disable

PUT /\_xpack/security/user/<username>/\_enable

PUT /\_xpack/security/user/<username>/\_password

#### Kibana management

用有系统管理权限的用户（如 elastic）登录kibana，在 management菜单中进行用户、角色管理。

## 角色管理

### 内建角色

https://www.elastic.co/guide/en/x-pack/6.2/built-in-roles.html

### API

https://www.elastic.co/guide/en/elasticsearch/reference/6.2/security-api-roles.html

GET /\_xpack/security/role

GET /\_xpack/security/role/<name>

POST /\_xpack/security/role/<name>/\_clear\_cache

POST /\_xpack/security/role/<name>

PUT /\_xpack/security/role/<name>

### Kibana management

用有系统管理权限的用户（如 elastic）登录kibana，在 management菜单中进行用户、角色管理。

## Client中加入 x-pack

### Java client中加入x-pack

1、在工程的pom文件中加入x-pack的jar依赖。需从elasticsearch的maven库上获取。如果无法从maven库中获取。则从官网上的地址下载对应的jar包。

https://www.elastic.co/guide/en/elasticsearch/reference/6.2/setup-xpack-client.html

<project ...>

<repositories>

<!-- add the elasticsearch repo -->

<repository>

<id>elasticsearch-releases</id>

<url>https://artifacts.elastic.co/maven</url>

<releases>

<enabled>true</enabled>

</releases>

<snapshots>

<enabled>false</enabled>

</snapshots>

</repository>

...

</repositories>

...

<dependencies>

<!-- add the x-pack jar as a dependency -->

<dependency>

<groupId>org.elasticsearch.client</groupId>

<artifactId>x-pack-transport</artifactId>

<version>{version}</version>

</dependency>

...

</dependencies>

...

</project>

2、客户端改用x-pack的，并指定对应的用户名密码

TransportClient client = new PreBuiltXPackTransportClient(Settings.builder()

.put("cluster.name", "myClusterName")

.put("xpack.security.user", "transport\_client\_user:x-pack-test-password")

...

.build())

.addTransportAddress(new TransportAddress("localhost", 9300))

.addTransportAddress(new TransportAddress("localhost", 9301));

### High level REST client

在构造lower level client实例时，通过setHttpClientConfigCallback方法加入认证信息：

final CredentialsProvider credentialsProvider = new BasicCredentialsProvider();

credentialsProvider.setCredentials(AuthScope.ANY,

new UsernamePasswordCredentials("elastic", "123456"));

RestHighLevelClient client = new RestHighLevelClient(

RestClient.builder(new HttpHost("localhost", 9200, "http"),

new HttpHost("localhost", 9201, "http"))

.setHttpClientConfigCallback(new RestClientBuilder.HttpClientConfigCallback() {

@Override

public HttpAsyncClientBuilder customizeHttpClient(HttpAsyncClientBuilder httpClientBuilder) {

return httpClientBuilder.setDefaultCredentialsProvider(credentialsProvider);

}

}));

# Monitoring 监控

https://www.elastic.co/guide/en/x-pack/current/xpack-monitoring.html

目标：

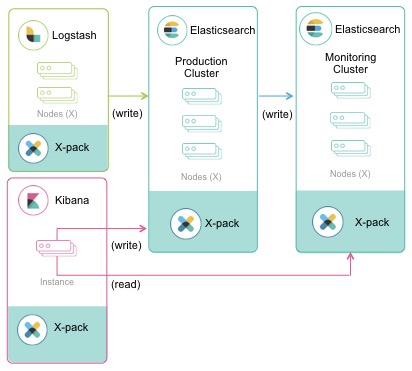
1. 掌握x-pack监控的工作原理。
2. 掌握x-pack监控的生成应用方法。

问题：

1. 为什么要监控？
2. 监控活动的本质是什么？
3. 监控活动的产出是什么？

## 监控工作原理

https://www.elastic.co/guide/en/x-pack/current/how-monitoring-works.html



## 监控生产环境

https://www.elastic.co/guide/en/x-pack/current/monitoring-production.html

# alerting 告警

目标：

1. 掌握x-pack告警模块的核心概念、watcher工作原理
2. 会配置告警watcher

问题：

1. 什么情况下需要告警？
2. 如何测定这种情况？
3. 以何种动作来告警？

## 简介

https://www.elastic.co/guide/en/x-pack/current/xpack-alerting.html

## 基本用法

https://www.elastic.co/guide/en/x-pack/current/watcher-getting-started.html

https://www.elastic.co/guide/en/x-pack/current/managing-watches.html

## Watcher 工作原理

https://www.elastic.co/guide/en/x-pack/current/how-watcher-works.html

## watcher 各组件

https://www.elastic.co/guide/en/x-pack/current/input.html

https://www.elastic.co/guide/en/x-pack/current/trigger.html

https://www.elastic.co/guide/en/x-pack/current/condition.html

https://www.elastic.co/guide/en/x-pack/current/actions.html

https://www.elastic.co/guide/en/x-pack/current/transform.html

# report 报告

x-pack的报告模块可让我们定时、实时生成各种图表数据报告。

https://www.elastic.co/guide/en/kibana/6.2/xpack-reporting.html