介绍

Kibana是一个旨在与Elasticsearch一起使用的开源分析和可视化平台,可以使用Kibana搜索，查看和与Elasticsearch索引中存储的数据进行交互。您可以轻松地执行高级数据分析，并在各种图表，表格和地图中可视化数据。其简单的基于浏览器的界面使您能够快速创建和共享动态仪表板，以实时显示对Elasticsearch查询的更改。

安装

需要node.js二进制文件支持。Kibana版本应该和Elasticsearch版本一致(ES版本可以比Kibana版本高，但会提示警告信息)。Kibana6.0及以上只支持64位系统。

下载地址7.5：<https://www.elastic.co/cn/downloads/kibana> 选择linux64版本

解压: tar -xzf kibana-7.5.1-linux-x86\_64.tar.gz

运行：

cd kibana-7.5.1-linux-x86\_64

./bin/kibana

配置文件—> ./config/kibana.yml

详细配置文件说明: <https://www.elastic.co/guide/en/kibana/7.5/settings.html>

默认主机地址与端口号: localhost:5601

console.enabled: 默认true，false时禁用控制台

cpu.cgroup.path.override: 如果挂载点跟 /proc/self/cgroup 不一致,覆盖cgroup cpuacct 路径

csp.rules:内容安全策略模板，可禁用浏览器中某些不必要的和可能不安全的功能,保持默认即可

csp.strict：默认false,为true时阻止任何不执行基本CSP规则的浏览器访问Kibana，实际会禁用不安全的浏览器如IE访问Kibana。

csp.warnLegacyBrowsers: 默认true，将Kibana加载到任何甚至不执行基本CSP规则的浏览器后，显示警告消息，尽管仍然可以访问Kibana。csp.strict设置后会被覆盖。

elasticsearch.customHeaders: 默认{}，发送给ES的自定义的头部信息。

elasticsearch.hosts: 默认 “<http://localhost:9200>”，用于所有查询请求的ES的URL

elasticsearch.logQueries: 默认false，记录所有发送到ES的请求日志。

elasticsearch.pingTimeout: 默认elasticsearch.requestTimeout的值，用于等待ES响应ping命令的时间

elasticsearch.preserveHost: 默认为true，为true时，Kibana使用server.host中设置的值作为主机名，为false时，使用连接到Kibana实例的主机的主机名。

elasticsearch.requestTimeout: 默认30000，等待后端或ES响应的时间，单位ms.

elasticsearch.shardTimeout: 默认30000，等待分片响应的时间。

elasticsearch.sniffOnConnectionFault: 默认false，为true时，连接故障时，会立即更新ES节点列表

elasticsearch.sniffOnStart: 默认false，为true时，在启动时会试图寻找其他ES节点。

elasticsearch.ssl.verificationMode: 默认full，控制ES提供的证书的验证，可取值none，certificate、full，full表示执行主机名验证。

server.host: 默认”localhost”，指定后端服务器主机，若想要远程用户连接，需要将值设为kibana服务器的ip地址或DNS名称。

server.port: 默认”5601”，访问kibana服务的端口号

server.name: 默认”your-hostname”，辨别此kibana实例的名字。

配置自启：

sudo /bin/systemctl daemon-reload

sudo /bin/systemctl enable kibana.service

**访问Kibana**: <http://localhost:5601>, 访问Kibana之前必须先启动ES服务，否则会提示” Kibana server is not ready yet”。

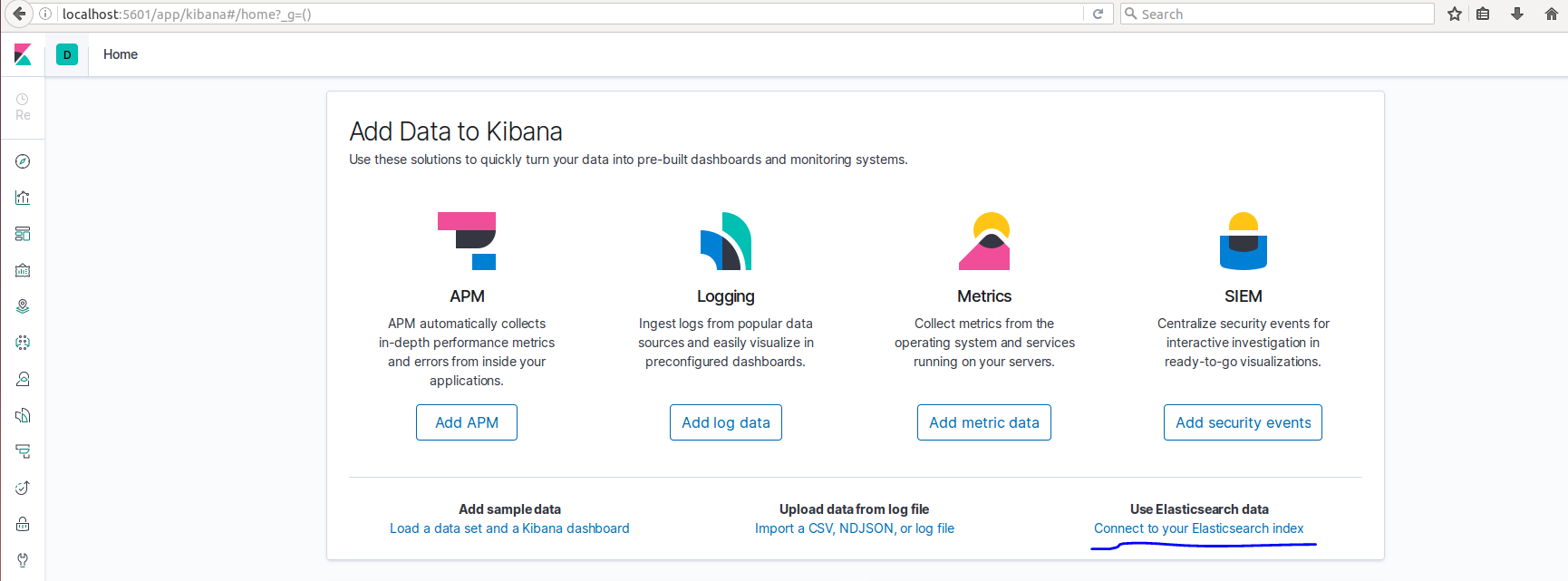
检查Kibana状态：<http://localhost:5601/status>, 会列出服务器资源使用信息及已经安装的插件。

连接Kibana和Elasticsearch

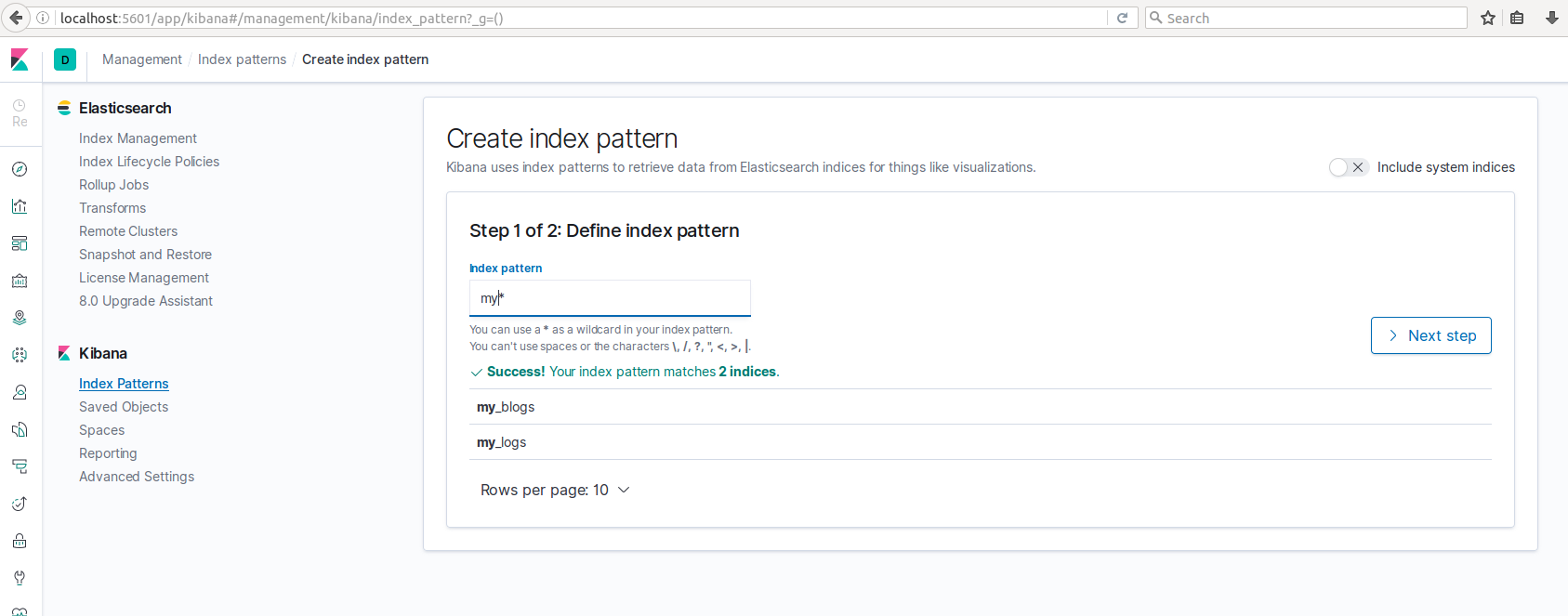
在开始使用KIbana之前，需要告诉它想要探索哪个ES索引。需要定义索引模式，该模式可匹配一个或多个索引(可以匹配多个索引的带可选通配符的字符串)。**(Management->Kibana->Index Patterns)**。默认情况下，Kibana连接运行在localhost上的es实例，若要连接不同实例，修改kibana.yml配置文件的ES URL并重启kibana。当有多个索引模式时，可以通过**Management->Index Patterns**点击索引模式上星星图标选定为默认索引模式。

创建索引模式(m\*及my\*)：

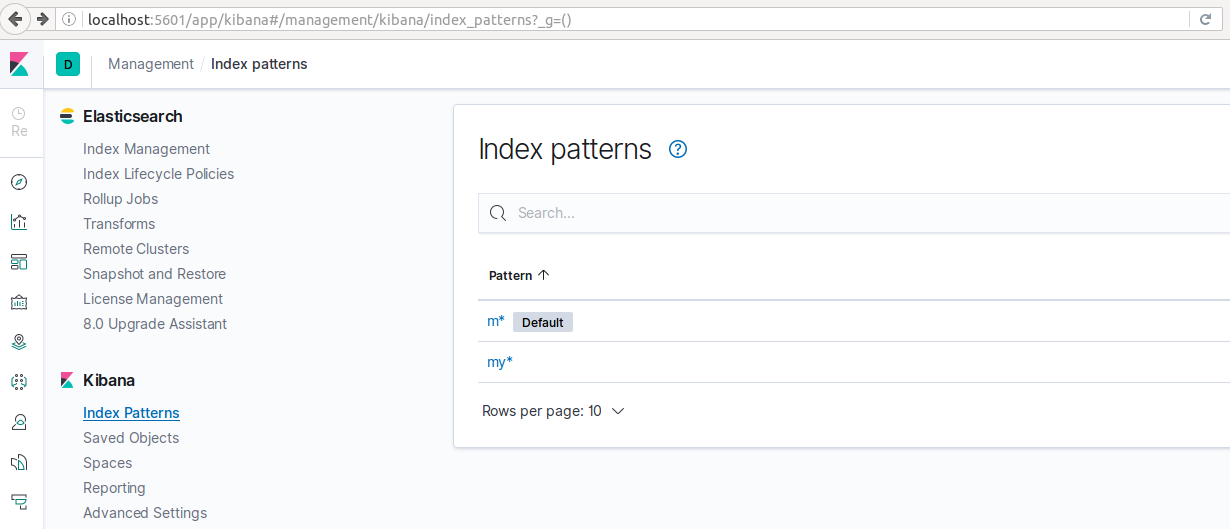
1. 启动ES及Kibana,访问<http://localhost:5601>,选择Use Elasticsearch data.



1. 选择Kibana->Index Patterns，页面显示kibana.yml中ES URL设置的主机的ES实例中的所有索引。填写m\*(匹配三个索引：megacorp、my\_blogs、mylogs)或者my\*(匹配两个索引: my\_blogs、mylogs)创建两个索引模式。



先创建的m\*模式为默认索引模式。



基础入门：