* server.port:

****默认值: 5601**** Kibana 由后端服务器提供服务，该配置指定使用的端口号。

* server.host:

****默认值: "localhost"**** 指定后端服务器的主机地址。

* server.basePath:

如果启用了代理，指定 Kibana 的路径，该配置项只影响 Kibana 生成的 URLs，转发请求到 Kibana 时代理会移除基础路径值，该配置项不能以斜杠 (/)结尾。

* server.maxPayloadBytes:

****默认值: 1048576**** 服务器请求的最大负载，单位字节。

* server.name:

****默认值: "您的主机名"**** Kibana 实例对外展示的名称。

* server.defaultRoute:

****默认值: "/app/kibana"**** Kibana 的默认路径，该配置项可改变 Kibana 的登录页面。

* elasticsearch.url:

****默认值: "http://localhost:9200"**** 用来处理所有查询的 Elasticsearch 实例的 URL 。

* elasticsearch.preserveHost:

****默认值: true**** 该设置项的值为 true 时，Kibana 使用 server.host 设定的主机名，该设置项的值为 false时，Kibana 使用主机的主机名来连接 Kibana 实例。

* kibana.index:

****默认值: ".kibana"**** Kibana 使用 Elasticsearch 中的索引来存储保存的检索，可视化控件以及仪表板。如果没有索引，Kibana 会创建一个新的索引。

* kibana.defaultAppId:

****默认值: "discover"**** 默认加载的应用。

* tilemap.url:

Kibana 用来在 tile 地图可视化组件中展示地图服务的 URL。默认时，Kibana 从外部的元数据服务读取 url，用户也可以覆盖该参数，使用自己的 tile 地图服务。例如："https://tiles.elastic.co/v2/default/{z}/{x}/{y}.png?elastic\_tile\_service\_tos=agree&my\_app\_name=kibana"

* tilemap.options.minZoom:

****默认值: 1**** 最小缩放级别。

* tilemap.options.maxZoom:

****默认值: 10**** 最大缩放级别。

* tilemap.options.attribution:

****默认值:**"© [Elastic Tile Service](https://www.elastic.co/elastic-tile-service)"** 地图属性字符串。

* tilemap.options.subdomains:

服务使用的二级域名列表，用 {s} 指定二级域名的 URL 地址。

* elasticsearch.username: 和 elasticsearch.password:

Elasticsearch 设置了基本的权限认证，该配置项提供了用户名和密码，用于 Kibana 启动时维护索引。Kibana 用户仍需要 Elasticsearch 由 Kibana 服务端代理的认证。

* server.ssl.enabled

****默认值: "false"**** 对到浏览器端的请求启用 SSL，设为 true 时， server.ssl.certificate 和 server.ssl.key 也要设置。

* server.ssl.certificate: 和 server.ssl.key:

PEM 格式 SSL 证书和 SSL 密钥文件的路径。

* server.ssl.keyPassphrase

解密私钥的口令，该设置项可选，因为密钥可能没有加密。

* server.ssl.certificateAuthorities

可信任 PEM 编码的证书文件路径列表。

* server.ssl.supportedProtocols

****默认值: TLSv1、TLSv1.1、TLSv1.2**** 版本支持的协议，有效的协议类型: TLSv1 、 TLSv1.1 、 TLSv1.2 。

* server.ssl.cipherSuites

****默认值: ECDHE-RSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES256-GCM-SHA384, DHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA256, DHE-RSA-AES128-SHA256, ECDHE-RSA-AES256-SHA384, DHE-RSA-AES256-SHA384, ECDHE-RSA-AES256-SHA256, DHE-RSA-AES256-SHA256, HIGH,!aNULL, !eNULL, !EXPORT, !DES, !RC4, !MD5, !PSK, !SRP, !CAMELLIA****. 具体格式和有效参数可通过[OpenSSL cipher list format documentation](<https://www.openssl.org/docs/man1.0.2/apps/ciphers.html#CIPHER-LIST-FORMAT>) 获得。

* elasticsearch.ssl.certificate: 和 elasticsearch.ssl.key:

可选配置项，提供 PEM格式 SSL 证书和密钥文件的路径。这些文件确保 Elasticsearch 后端使用同样的密钥文件。

* elasticsearch.ssl.keyPassphrase

解密私钥的口令，该设置项可选，因为密钥可能没有加密。

* elasticsearch.ssl.certificateAuthorities:

指定用于 Elasticsearch 实例的 PEM 证书文件路径。

* elasticsearch.ssl.verificationMode:

****默认值: full**** 控制证书的认证，可用的值有 none 、 certificate 、 full 。 full 执行主机名验证，certificate 不执行主机名验证。

* elasticsearch.pingTimeout:

****默认值:**elasticsearch.requestTimeout**setting**** 的值，等待 Elasticsearch 的响应时间。

* elasticsearch.requestTimeout:

****默认值: 30000**** 等待后端或 Elasticsearch 的响应时间，单位微秒，该值必须为正整数。

* elasticsearch.requestHeadersWhitelist:

****默认值:**[ 'authorization' ]** Kibana 客户端发送到 Elasticsearch 头体，发送 ****no**** 头体，设置该值为[]。

* elasticsearch.customHeaders:

****默认值:**{}** 发往 Elasticsearch的头体和值， 不管 elasticsearch.requestHeadersWhitelist 如何配置，任何自定义的头体不会被客户端头体覆盖。

* elasticsearch.shardTimeout:

****默认值: 0**** Elasticsearch 等待分片响应时间，单位微秒，0即禁用。

* elasticsearch.startupTimeout:

****默认值: 5000**** Kibana 启动时等待 Elasticsearch 的时间，单位微秒。

* pid.file:

指定 Kibana 的进程 ID 文件的路径。

* logging.dest:

****默认值:**stdout** 指定 Kibana 日志输出的文件。

* logging.silent:

****默认值: false**** 该值设为 true 时，禁止所有日志输出。

* logging.quiet:

****默认值: false**** 该值设为 true 时，禁止除错误信息除外的所有日志输出。

* logging.verbose

****默认值: false**** 该值设为 true 时，记下所有事件包括系统使用信息和所有请求的日志。

* ops.interval

****默认值: 5000**** 设置系统和进程取样间隔，单位微妙，最小值100。

* status.allowAnonymous

****默认值: false**** 如果启用了权限，该项设置为 true 即允许所有非授权用户访问 Kibana 服务端 API 和状态页面。

* cpu.cgroup.path.override

如果挂载点跟 /proc/self/cgroup 不一致，覆盖 cgroup cpu 路径。

* cpuacct.cgroup.path.override

如果挂载点跟 /proc/self/cgroup 不一致，覆盖 cgroup cpuacct 路径。

* console.enabled

****默认值: true**** 设为 false 来禁用控制台，切换该值后服务端下次启动时会重新生成资源文件，因此会导致页面服务有点延迟。

* elasticsearch.tribe.url:

Elasticsearch tribe 实例的 URL，用于所有查询。

* elasticsearch.tribe.username: 和 elasticsearch.tribe.password:

Elasticsearch 设置了基本的权限认证，该配置项提供了用户名和密码，用于 Kibana 启动时维护索引。Kibana 用户仍需要 Elasticsearch 由 Kibana 服务端代理的认证。

* elasticsearch.tribe.ssl.certificate: 和 elasticsearch.tribe.ssl.key:

可选配置项，提供 PEM 格式 SSL 证书和密钥文件的路径。这些文件确保 Elasticsearch 后端使用同样的密钥文件。

* elasticsearch.tribe.ssl.keyPassphrase

解密私钥的口令，该设置项可选，因为密钥可能没有加密。

* elasticsearch.tribe.ssl.certificateAuthorities:

指定用于 Elasticsearch tribe 实例的 PEM 证书文件路径。

* elasticsearch.tribe.ssl.verificationMode:

****默认值: full**** 控制证书的认证，可用的值有 none 、 certificate 、 full 。 full 执行主机名验证， certificate 不执行主机名验证。

* elasticsearch.tribe.pingTimeout:

****默认值:**elasticsearch.tribe.requestTimeout**setting**** 的值，等待 Elasticsearch 的响应时间。

* elasticsearch.tribe.requestTimeout:

****Default: 30000**** 等待后端或 Elasticsearch 的响应时间，单位微秒，该值必须为正整数。

* elasticsearch.tribe.requestHeadersWhitelist:

****默认值:**[ 'authorization' ]** Kibana 发往 Elasticsearch 的客户端头体，发送 ****no**** 头体，设置该值为[]。

* elasticsearch.tribe.customHeaders:

****默认值:**{}** 发往 Elasticsearch的头体和值，不管 elasticsearch.tribe.requestHeadersWhitelist 如何配置，任何自定义的头体不会被客户端头体覆盖。