# 日志分析平台部署及使用说明

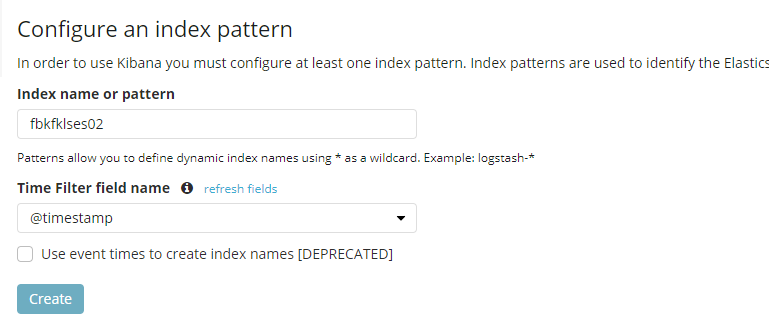
1. **系统架构**
2. 使用filebeat +kafka+elk进行日志采集
3. 每台主机部署filebeat，占用物理内存20M左右，filebeat采集信息指kafka。
4. Logstash消费kafka数据，汇总到ES，部署一个logstash实例即可，需要配置内存2g
5. **应用日志的规范**
6. 输出格式规范，统一采用以下格式

%d{yyyy-MM-dd HH:mm:ss.SSS} [%X{requestId}] [%-5level] [%thread] %logger %line - %msg%n

1. 日志输出级别，必须是info级别以上
2. 日志输出策略，采取轮转的方式，每日轮转
3. 文件名的规范${APP\_NAME}.log，轮转文件名模式${APP\_NAME}-%d{yyyy-MM-dd}.%i.log
4. **kibana的使用**
5. 登录kibana管理系统，http://{线上kibana地址}:5601
6. 点击左侧Management菜单，进入日志索引配置



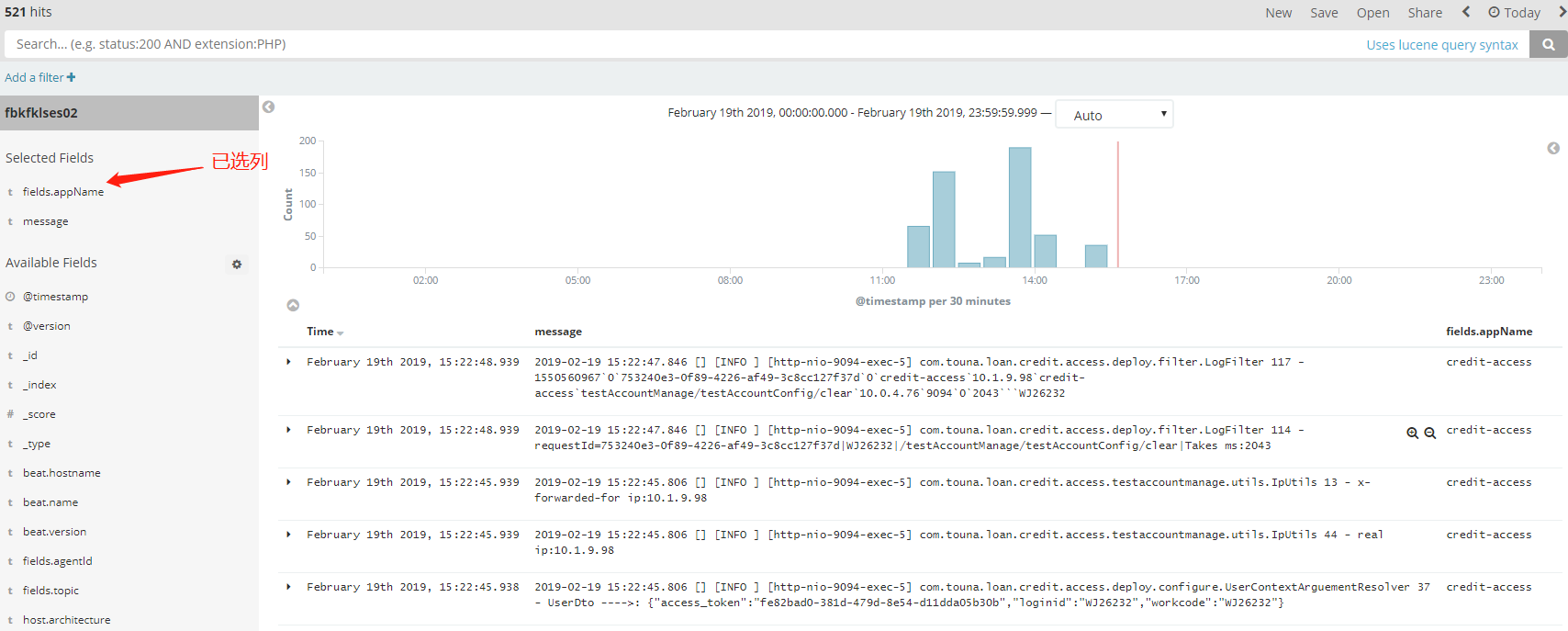
1. 在index name or pattern输入框，输入fbkfklses02，time filter field name选择@timestamp，点击create按钮



1. 点击左侧discover菜单，默认界面如下，默认展示\_source元数据



1. 鼠标移动至预选列，点击add按钮，展示所需数据



1. 条件过滤，输入查询的内容，如果是多条件，使用OR及AND关键字，可使用单或双引号包括查询内容，同时可指定列名查询，如fields.appName:credit，表示列名为fields.appName包含有credit值的数据。



1. **Filebeat的部署**
2. 使用tar -xzvf 解压，
3. 创建FILEBEAT02队列，kafka-topics --zookeeper {zk}:2181/kafka --create --topic FILEBEAT02 --partitions 5 --replication-factor 1
4. 使用./start.sh {logDir} {appName} {agentId} 启动应用
5. **Logstash部署**
6. 使用tar -xzvf 解压
7. 使用./start.sh 脚本启动
8. **应用系统告警名单收集**

1、告警系统开发（谢正龙）

2、告警名单收集 ，格式如下

****