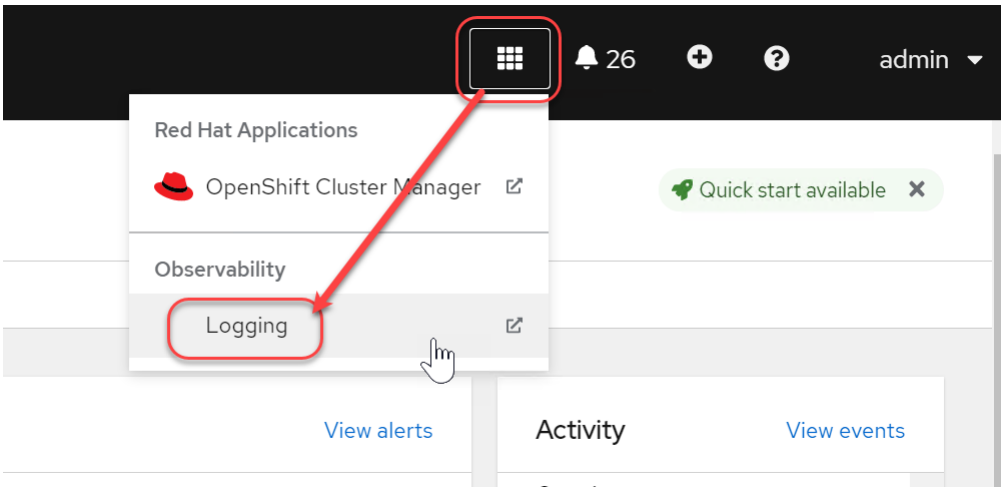
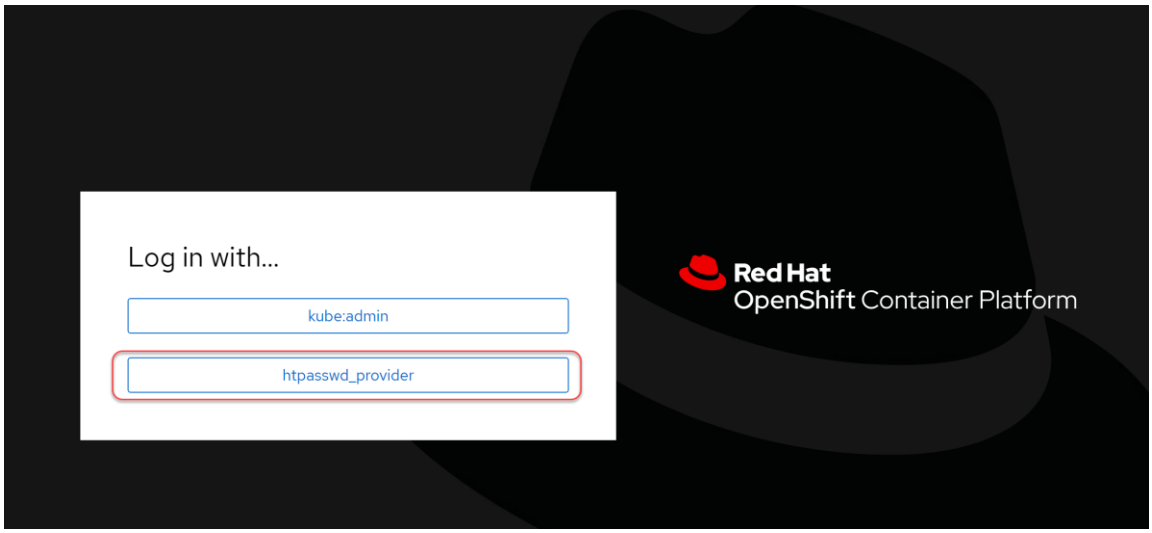
OCP 上的 EFK 安装后，如果日志不需要转发到外部，默认是不需要配置日志转发的。但如果要收集 audit 日志，就需要配置 LogForwarder。
如下所示：

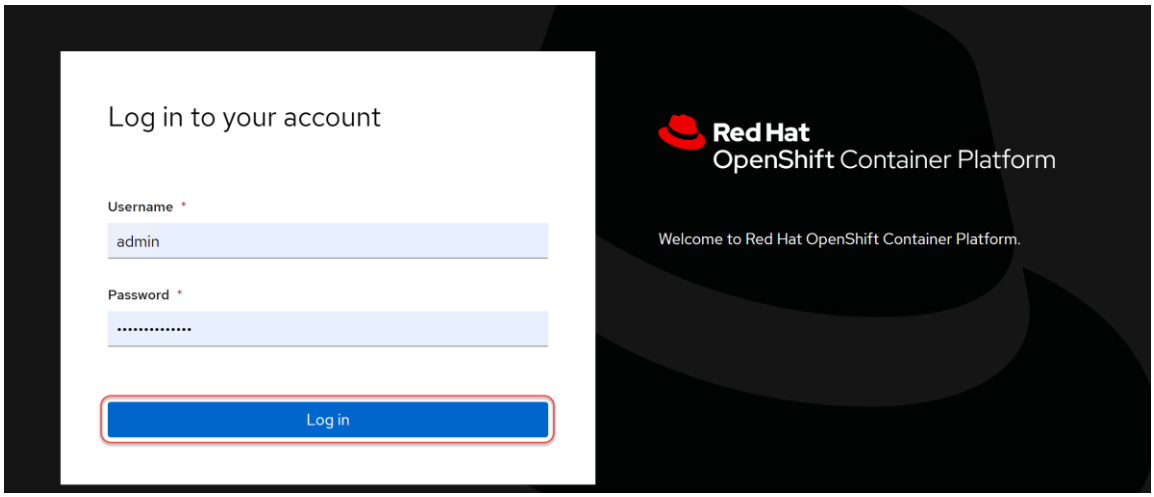
```
cat << EOF | oc create -f -
---
apiVersion: logging.openshift.io/v1
kind: ClusterLogForwarder
metadata:
  name: instance
  namespace: openshift-logging
spec:
  pipelines:
  - name: all-to-default
    inputRefs:
    - infrastructure
    - application
    - audit
    outputRefs:
    - default
EOF
```

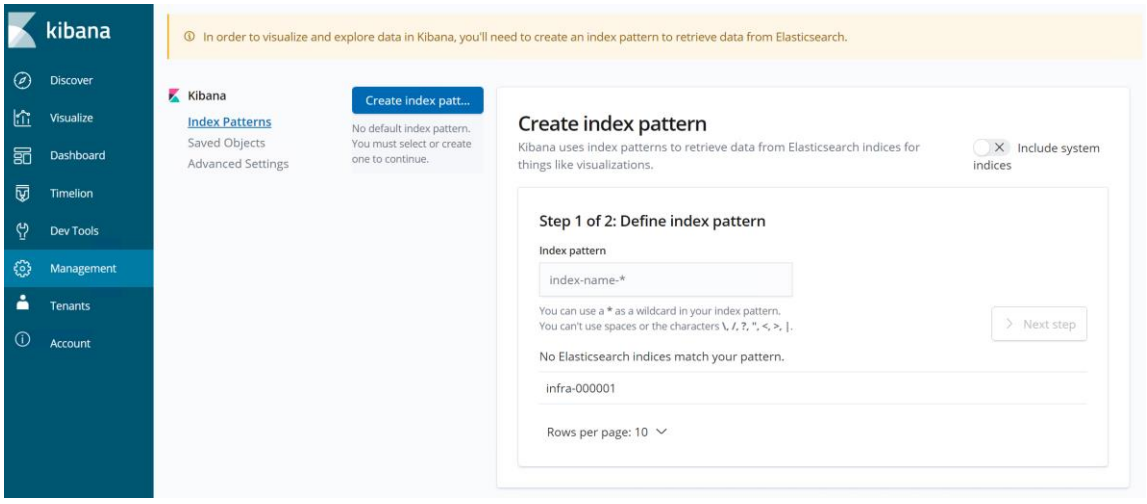
此时，您可以在 OCP 主页右上角的按钮中看到 Logging 的链接，具体如下



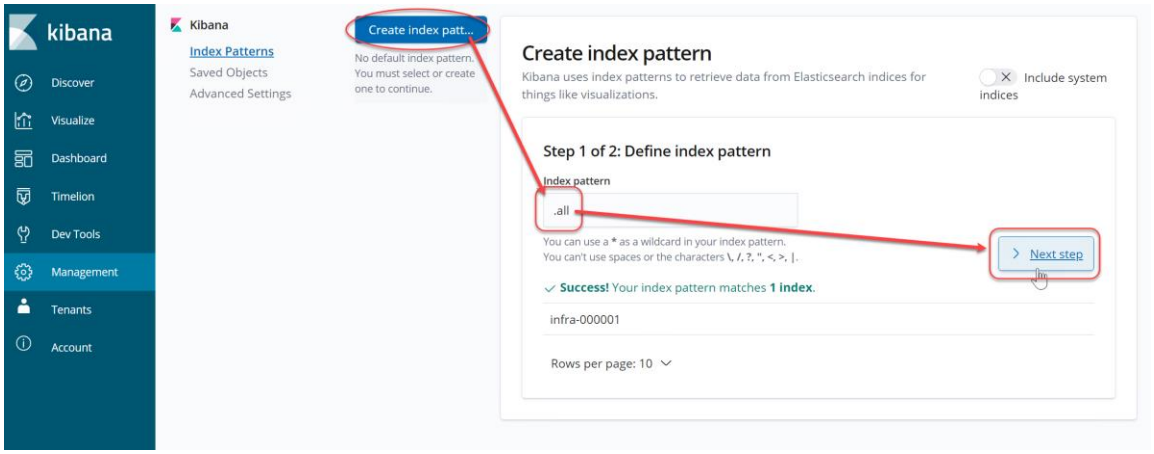
该链接会打开如下的地址访问 Kibana 页面，如 https://kibana-openshift-logging.apps.ocp4-1.example.internal

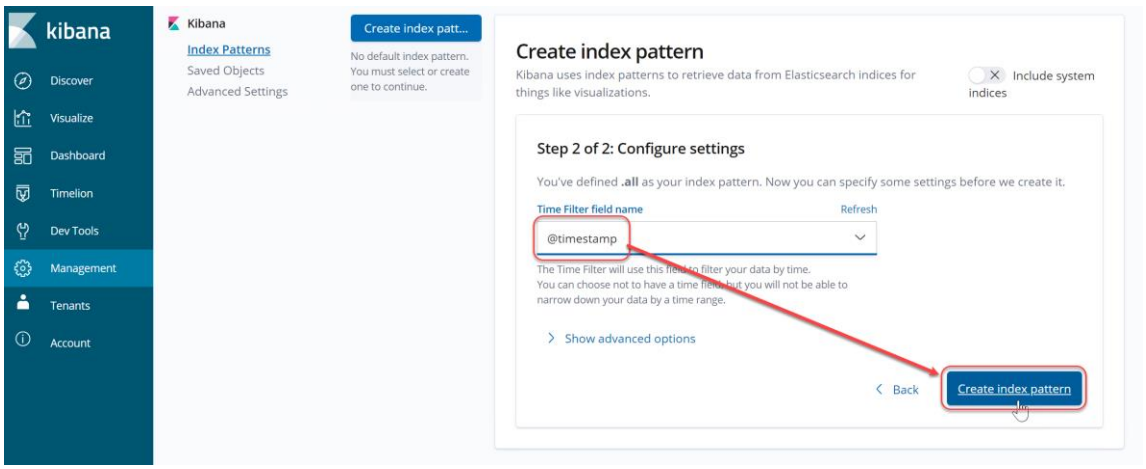

Log in with...
kube:admin
htpasswd_provider
Red Hat
OpenShift Container Platform


Log in to your account
Username *
admin
Password *
Log in
Red Hat
OpenShift Container Platform
Welcome to Red Hat OpenShift Container Platform.

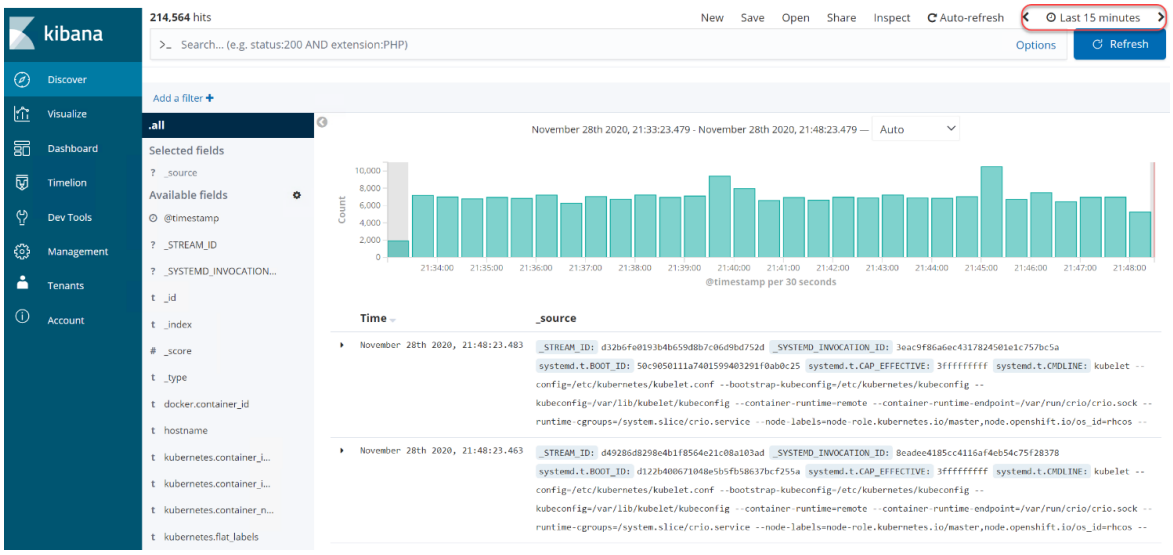

kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Tenants
Account
In order to visualize and explore data in Kibana, you'll need to create an index pattern to retrieve data from Elasticsearch.
Kibana
Index Patterns
Saved Objects
Advanced Settings
Create index patt...
No default index pattern. You must select or create one to continue.
Create index pattern
Kibana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations.
Include system indices
Step 1 of 2: Define index pattern
Index pattern
index-name-*
You can use a * as a wildcard in your index pattern.
You can't use spaces or the characters \, /, ?, ", <, >, |.
Next step
No Elasticsearch indices match your pattern.
infra-000001
Rows per page: 10

创建自定义索引

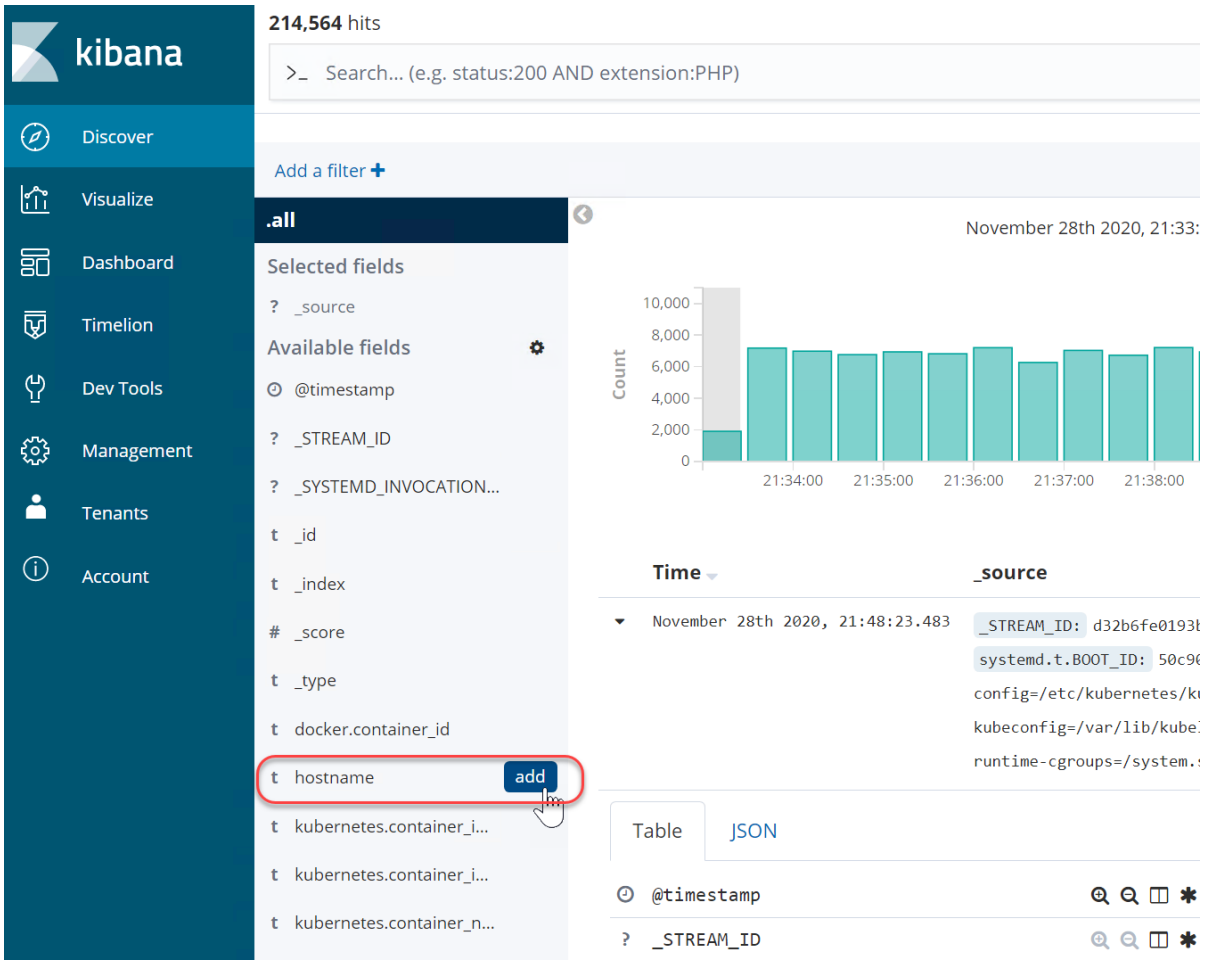


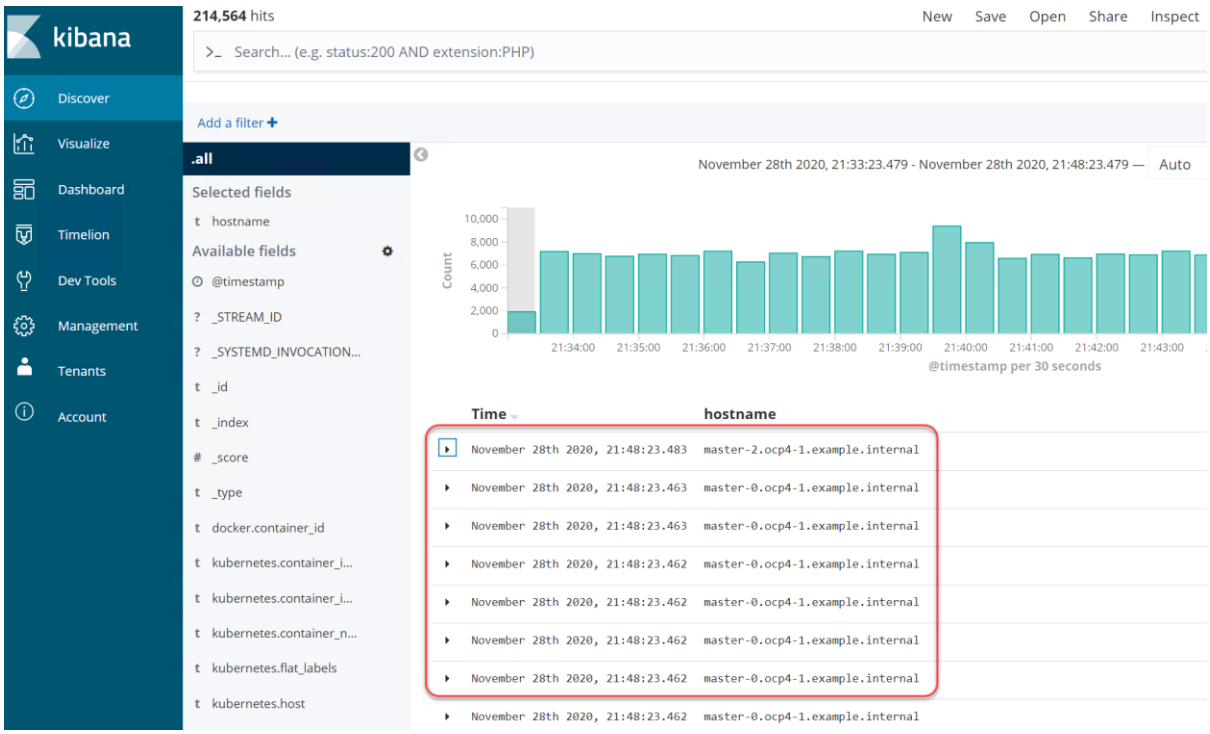


Kibana 默认展示过去十五分钟的日志内容，可通过右上角的按钮进行修改

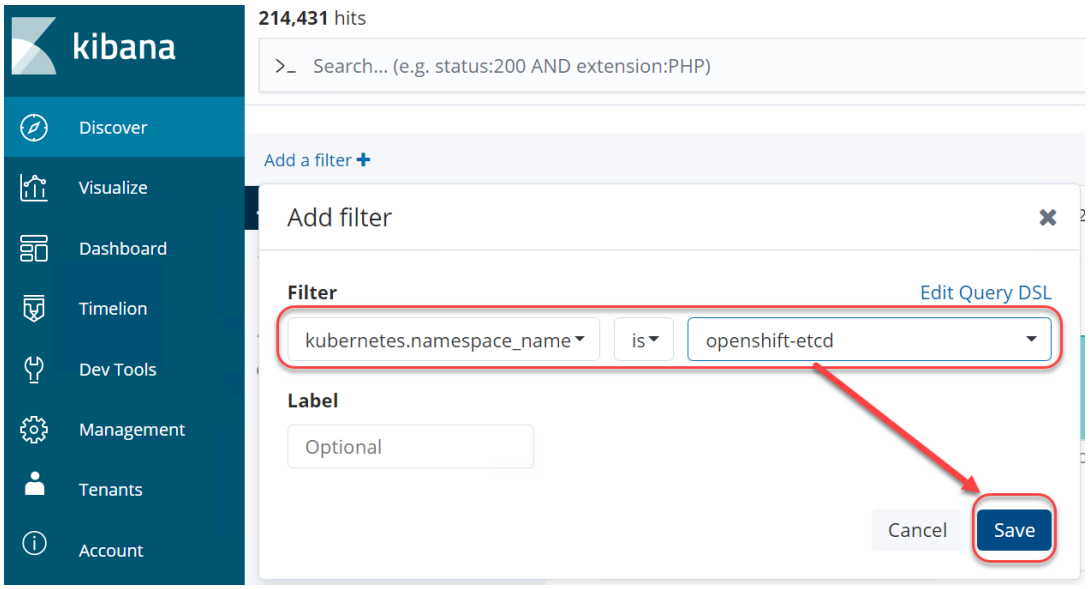


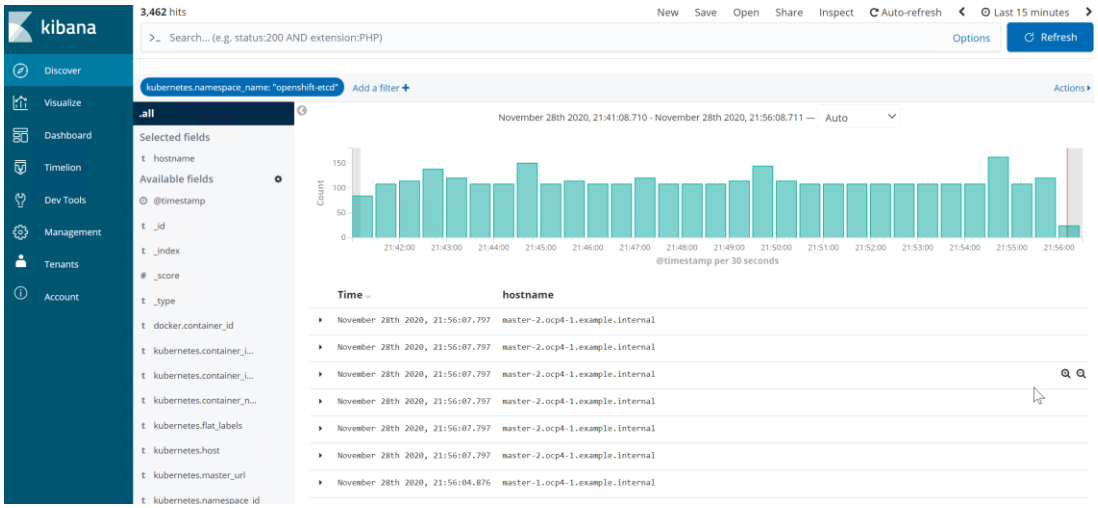
点击左侧的下拉菜单，选择`.all` `hostname` `add`,这将按照主机名列出相应的日志内容



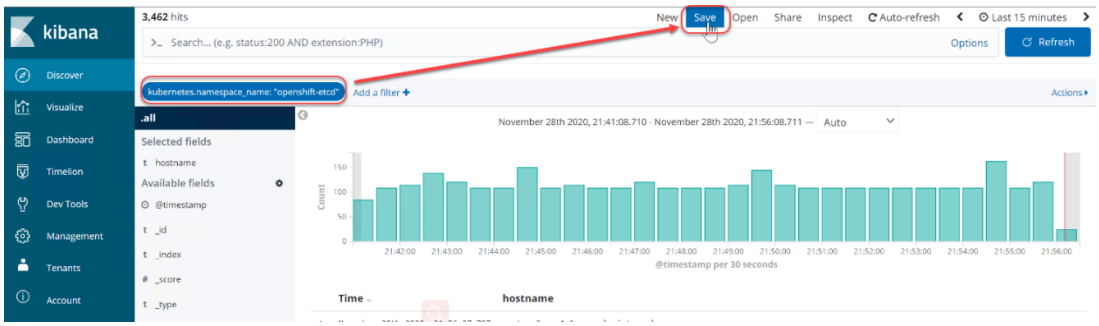


查询 openshift-etcd 这个命名空间中的所有日志

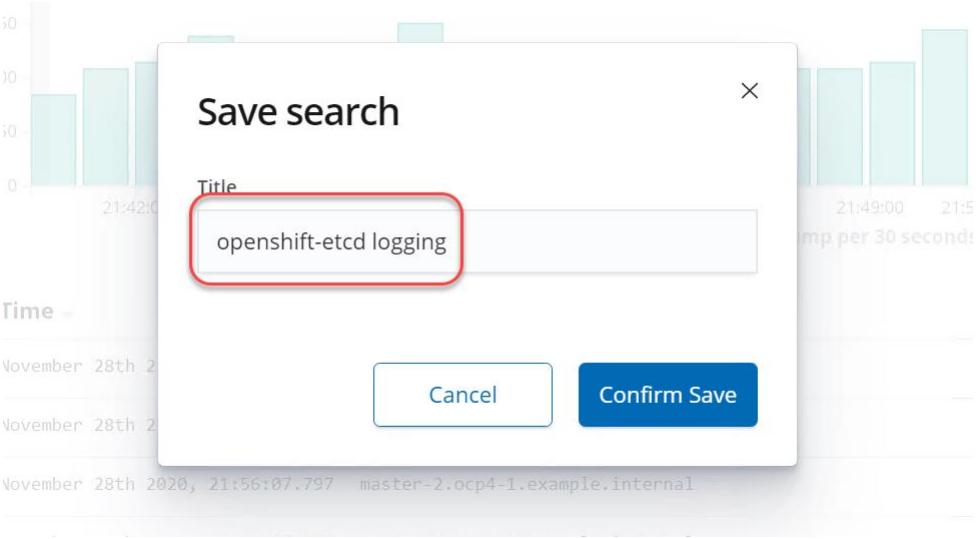




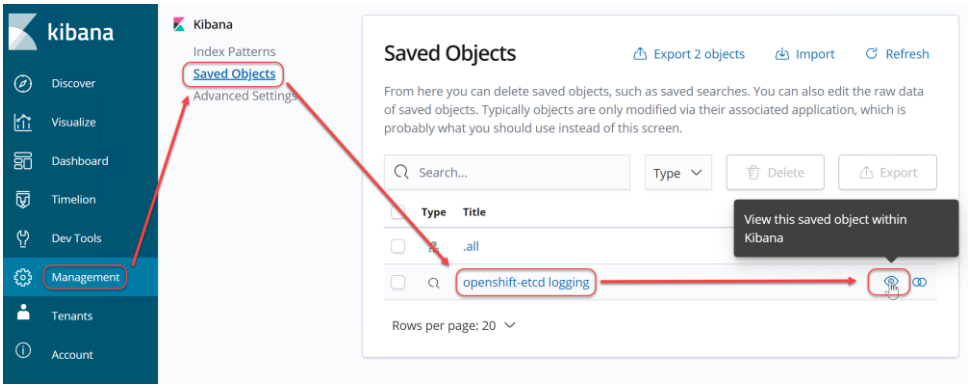
保存查询

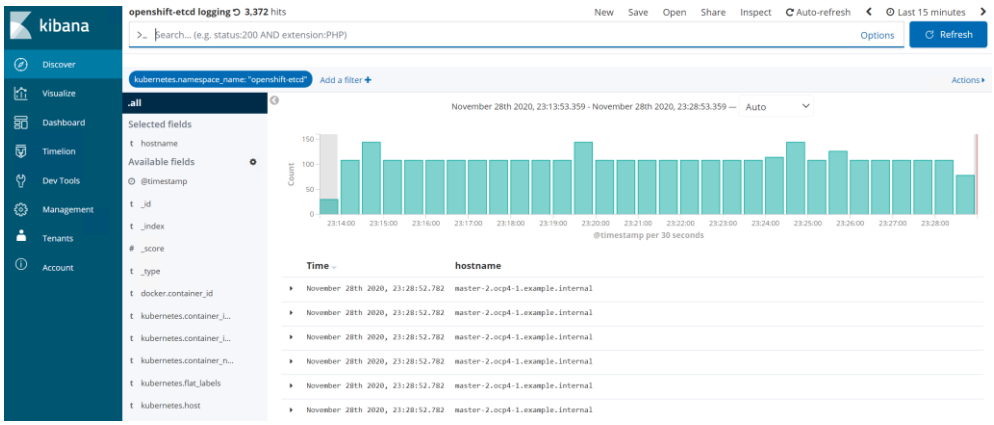


输入要保存的名字



之后，我们可以在 Management 中的 Saved Objects 中，找到刚才保存的对象





如果想将日志转发到外部平台，如 splunk，可以参照如下文章：
https://www.openshift.com/blog/forwarding-logs-to-splunk-using-the-openshift-log-forwarding-api