实训任务一：初识 Elastic Stack

一、目的

1、了解 Elastic Stack；

2、掌握 Elastic Stack 部署流程和基本方法；

3、实现 Windows 事件分析。

二、学时

12 学时

扫码看实训演示

扫码看任务步骤

三、类型

综合型

四、需求

1、硬件

每人配备计算机 1 台，不低于双核 CPU、8G 内存、500GB 硬盘。

2、软件

Windows 操作系统，安装 VirtualBox 虚拟化软件，安装 Termius 管理终端软件。

3、网络

计算机使用固定 IP 地址接入局域网，并支持对互联网的访问，虚拟主机可通过桥接网卡方式访问互联网。

4、工具

无。

五、任务要求

1、完成 Elastic Stack 部署（基于 VirtualBox 和 CentOS 8）；

2、完成 Windows 事件分析，实现不少于 10 个可视化分析图标。

六、考核要求

1、提交《基于 CentOS 8 部署 Elastic Stack 快速手册》，文档结构参见模板。

七、任务步骤

Elastic Stack 是一系列开源产品的合集，包括 Elasticsearch、Kibana、Logstash 以及 Beats 等，能够安全可靠地获取任何来源、任何格式的数据，能够实时地对数据进行搜索、分析和可视化。

任务 1：基于 VirtualBox 部署 CentOS 8

步骤 01：在 VirtualBox 创建虚拟机，虚拟机的配置信息如表 1-1 所示。

表 1-1 CentOS 8 操作系统配置

配置项	配置值
虚拟机名	YWSX-10.10.2.150-CentOS8X64-ElasticStack-7.8 【请自行设置】
虚拟机配置	操作系统类型：Rad Hat（64-bit） 内存：4096 MB 处理器：1 核，启用 PAE/NX 启用嵌套分页 存储：SATA 60 GB
虚拟机网络配置	网卡 1：Intel PRO/1000 MT 桌面（NAT 网络，CloudNetworkNAT）
CentOS 权限	操作系统账号：root 系统账号口令：R#labs313 【请自行设置】
备注	CentOS 8 安装时选择最小化安装，使用中文语言，正确选择时钟配置。 CentOS 8 网络配置根据实际情况设置。

步骤 02：在虚拟机中安装 CentOS 操作系统。CentOS 使用 CentOS 8.2004 X86_64 版本，建议根据实际情况选择最新版本的 CentOS 操作系统。

提醒：

①操作系统镜像文件可通过 CentOS 官方网站（http://isoredirect.centos.org/centos/8/isos/x86_64/）下载获得，本实验所使用的镜像为 CentOS-8.2.2004-x86_64-minimal.iso

②安装 CentOS 8 操作系统的具体方法，参见教学视频。

教学视频地址：

http://dms.it.hactcm.edu.cn/api/h/f?m=935492a5fa9fcd1b-1-0

Bilibili 访问地址：

https://www.bilibili.com/video/BV1j741177cu?p=8

扫码看教学视频

任务 2：Elastic Stack 部署准备

Elasticsearch 的开发语言为 Java，需完成 Java 环境配置；Elasticsearch 节点默认与外部进行通信的端口为 9200；Kibana 默认的服务端口为 5601，需调整防火墙规则，开放相应的端口。

步骤 01：安装 java 环境

参考命令：

```
#安装 Java 环境
yum install –y java
#查看 Java 环境是否安装成功
java –version
```

步骤 02：调整防火墙规则

参考命令：

```
firewall-cmd --zone=public --add-port=5601/tcp --permanent    #防火墙添加 5601 端口
firewall-cmd --zone=public --add-port=9200/tcp --permanent    #防火墙添加 9200 端口
```

```
firewall-cmd --reload                                    #防火墙重新加载配置使规则生效
```

任务 3：部署 Elasticsearch

Elasticsearch 是一个分布式、高扩展、高实时的搜索与数据分析引擎。

步骤 01：获取 rpm 包

参考命令：

```
# 获取 rpm 包
wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.8.0-x86_64.rpm
# 也可选用国内的华为开源镜像站提供的资源地址加速下载
wget https://mirrors.huaweicloud.com/elasticsearch/7.8.0/elasticsearch-7.8.0-x86_64.rpm
```

步骤 02：安装。

参考命令：

```
rpm -ivh elasticsearch-7.8.0-x86_64.rpm
```

步骤 03：修改配置文件 elasticsearch.yml

参考命令：

```
cp /etc/elasticsearch/elasticsearch.yml /etc/elasticsearch/elasticsearch.yml.bak
vi /etc/elasticsearch/elasticsearch.yml
```

配置文件：

```
node.name: node-1                                #设置节点名字
network.host:10.10.2.150                         #本机 IP 地址
http.port:9200                                   #端口
cluster.initial_master_nodes: ["node-1"]         #设置主节点
```

步骤 04：测试

参考命令：

```
systemctl start elasticsearch
```

通过浏览器访问 http://10.10.2.150:9200，验证 Elasticsearch 部署是否成功。

任务 4：部署 Logstash

Logstash 是一款具备实时管道处理能力的开源数据收集引擎，可统一对应用程序日志进行收集管理，并提供接口用于查询和统计。

步骤 01：获取 rpm 包

参考命令：

```
#获取 rpm 包
wget https://artifacts.elastic.co/downloads/logstash/logstash-7.8.0.rpm
#也可选用国内的华为开源镜像站提供的资源地址加速下载
wget https://mirrors.huaweicloud.com/logstash/7.8.0/logstash-7.8.0.rpm
```

步骤 02：安装

参考命令：

```
rpm –ivh logstash-7.8.0.rpm
```

任务 5：部署 Kibana

Kibana 是为 Elasticsearch 设计的开源分析和可视化平台，可使用 Kibana 搜索、查看存储在 **Elasticsearch** 索引中的数据并与之交互，实现数据分析和可视化，并以图表的形式展

现结果。

步骤 01：获取 rpm 包

参考命令：

```
wget http://artifacts.elastic.co/downloads/kibana/kibana-7.8.0-x86_64.rpm
#也可选用国内的华为开源镜像站提供的资源地址加速下载
wget https://mirrors.huaweicloud.com/kibana/7.8.0/kibana-7.8.0-x86_64.rpm
```

步骤 02：安装

参考命令：

```
rpm –ivh kibana-7.8.0-x86_64.rpm
```

步骤 03：配置文件 kibana.yml

参考命令：

```
vi /etc/kibana/kibana.yml
```

配置文件：

```
server.host: "10.10.2.150"                          #监听端口
server.port: 5601                                   #监听地址
elasticsearch.hosts: ["http://10.10.2.150:9200"]    #Elasticsearch 服务地址
i18n.locale: "zh-CN"                                #配置语言为简体中文
```

任务 6：Elastic Stack 部署测试

本任务配置 Logstash 读取 CentOS 系统自身日志数据，并发送到 Elasticsearch 存储，最后经 Kibana 展示分析结果，实现对 Elastic Stack 部署任务的验证。

步骤 01：配置 Logstash

在/etc/logstash/conf.d 下新增配置配置文件 test.conf，配置文件的格式为*.conf

配置文件：

```
#增加以下内容
input {
      file {
           path => "/var/log/dnf.log"                          #需采集的日志文件路径
           type => "systemlog"                                      #日志类型，可自定义
           start_position => "beginning"                            #配置 logstash 从开头读取日志文件
           stat_interval => "1"                                #配置 logstash 每隔 1s 检查一次被监听文件状
态
      }
}

output {
      elasticsearch {
            hosts => ["10.10.2.150:9200"]                          #Elasticsearch 服务地址
           index => "test-%{type}-%{+YYYY.MM.dd}"    #定义索引名称
      }
}
```

步骤 02：启动 logstash、kibana

参考命令：

```
systemctl status elasticsearch        #查看 elasticsearch 状态
systemctl start logstash              #启动 logstash
systemctl status logstash             #查看 logstash 状态
```

systemctl start kibana	#启动 kibana
systemctl status kibana	#查看 kibana 状态

步骤 03：查看结果

访问 http://10.10.2.150:5601，在 Stack Management 中切换到索引模式，点击右侧创建索引模式按钮进行创建索引，如图 1-1 所示。

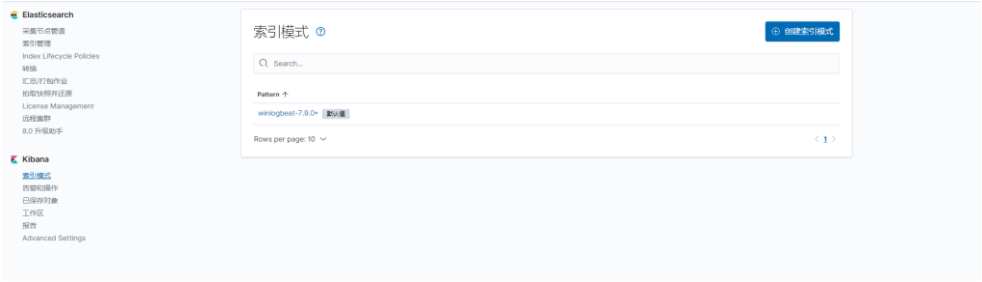

图 1-1 创建索引模式

定义索引模式并与已有的索引进行匹配，也可以匹配多个索引达到索引聚合的目的，如图 1-2 所示。

图 1-2 索引匹配

在配置设置中，通过选择使用@timestamp 字段，可以达到按照时间筛选数据的目的，如图 1-3 所示。

图 1-3 配置设置

在 Discover 中通过切换索引，可以在右侧看到采集的 CentOS 系统日志数据，说明 Elastic Stack 部署及配置成功，如图 1-4 所示。

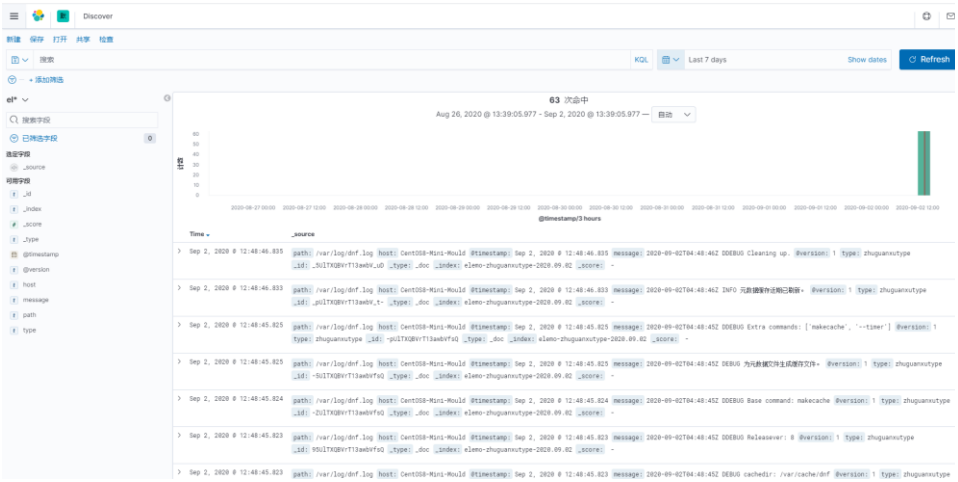

图 1-4 日志数据展示

任务 7：使用 Winlogbeat 采集 Windows Events 数据

Winlogbeat 使用 Windows API 读取一个或多个事件日志，并根据用户配置的条件过滤事件日志，然后将事件日志发送到指定的输出目的地（Elasticsearch 或 Logstash）。

步骤 01：获取 Winlogbeat 程序

从 https://www.elastic.co/cn/downloads/beats/winlogbeat 获取安装的 ZIP 文件。

步骤 02：安装配置 Winlogbeat

将 ZIP 文件解压到 C:\Program Files\winlogbeat-7.8.0-windows，并重命名文件夹为 Winlogbeat。

鼠标右键 Windows 开始按钮，打开 Windows PowerShell(管理员)，运行以下命令将 Winlogbeat 安装为 Windows 服务。

参考命令：

```
& 'C:\Program Files\winlogbeat\install-service-winlogbeat.ps1'
```

步骤 03：修改 Winlogbeat 配置文件

配置文件：

```
output.elasticsearch:
   hosts: ["10.10.2.150:9200"]          #Elasticsearch 的服务地址
   username: "elastic"                  #Elasticsearch 的用户名
   password: "changeme"                 #Elasticsearch 的密码
setup.kibana:
   host: "10.10.2.150:5601"             #Kibana 的 URL
```

步骤 04：启动 Winlogbeat

参考命令：

```
& 'C:\Program Files\winlogbeat\winlogbeat.exe ' setup
Start-Service winlogbeat
```

步骤 05：在 Elastic Stack 查看 Window 事件数据

访问 http://10.10.2.150:5601，仿照任务 6 中的步骤 3，创建索引模式。在 Discover 中通过切换索引，可以在右侧看到采集到的 Windows 事件数据。

任务 8：在 Kibana 上创建分析模型并进行分析

步骤 01：设计分析模型

表 1-2 Windows Event 分析模型

序号	分析字段	分析模型	图表类型
1	winlog.event_id	事件代码类型	柱状图
2	log.level	日志等级占比	圆饼图
3	winlog.channel	日志类型占比	圆饼图
4	event.provider	来源排行	柱状图
5	event.provider	日志来源	标签云
6	winlog.event_id:{4624,4625,4648,4778,4779}	需重点关注的安全类事件数量占比	圆饼图
7	event.code:{12,13,24576,24577,24579}	需重点关注的系统类事件占比	圆饼图
8	event.code:{1}	Windows 事件总数	指标
9	event.code:{2,3,4,5,6,7,8,10,11}	Windows 登录类型	表格
10	event.code:{0,1,33,1002}	需重点关注的应用程序类事件占比	圆饼图

步骤 02：实现 Windows 事件代码类型分析

（1） 在 Dashboards 中创建仪表盘，如图 1-5 所示。

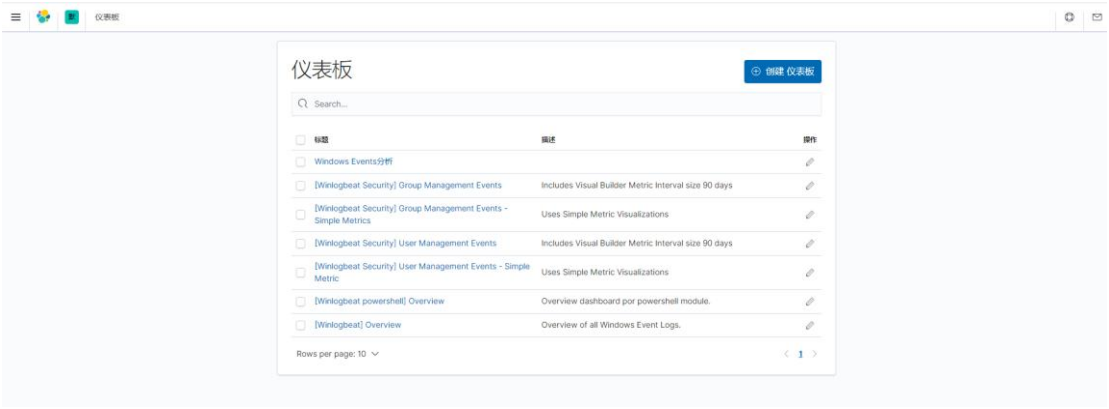

图 1-5 创建仪表盘

（2） 新建可视化类型，如图 1-6 所示。

图 1-6 新建可视化类型

（3） 选择数据源，如图 1-7 所示。

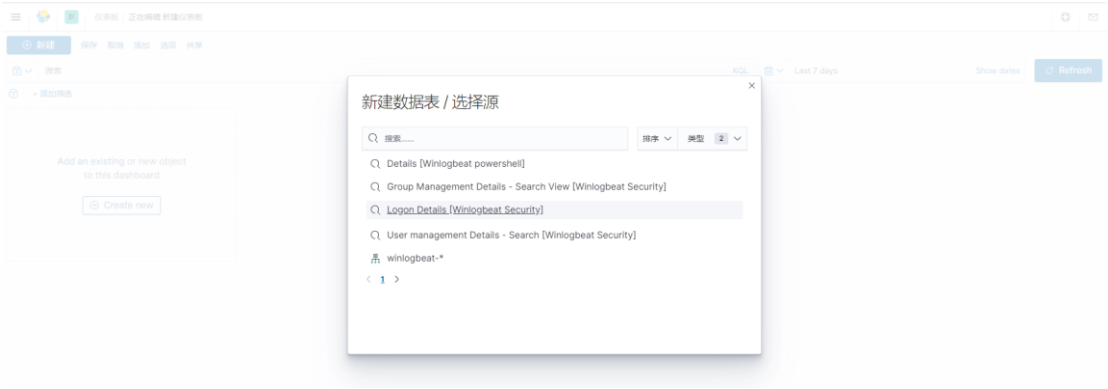

图 1-7 选择数据源

（4） 添加分析字段，更新数据并保存，如图 1-8、1-9 所示。

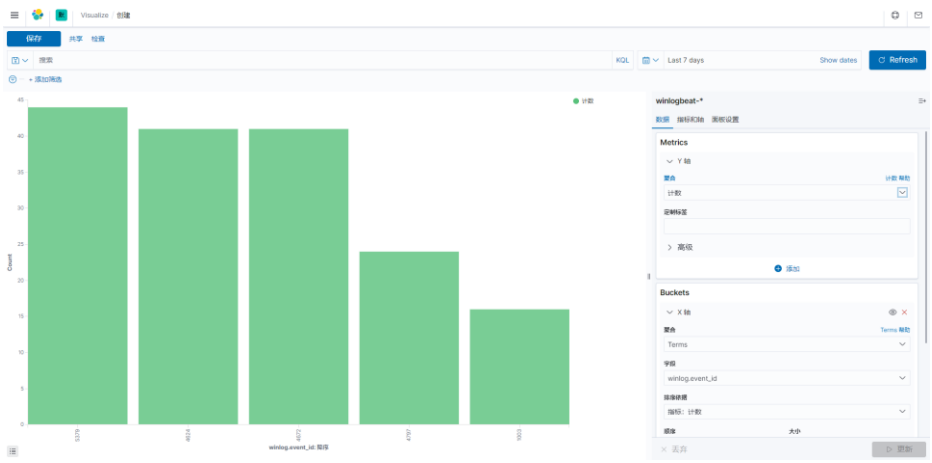

图 1-8 添加分析字段

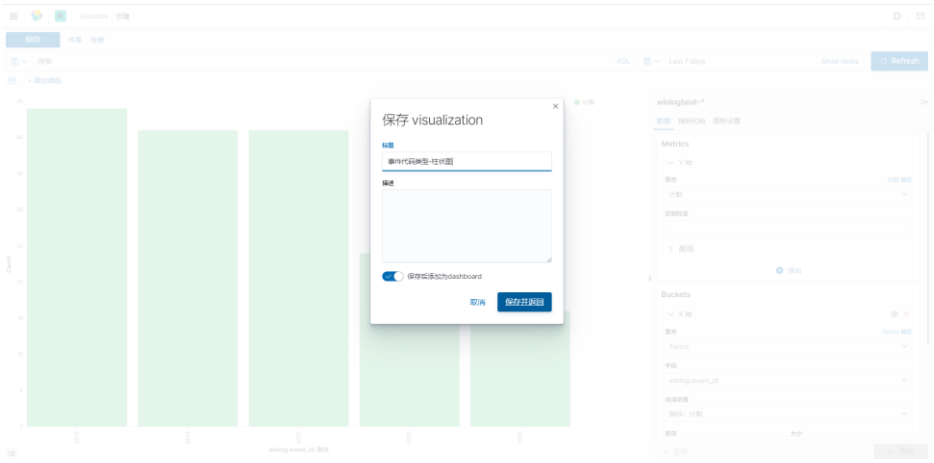

图 1-9 保存可视化图表

（5） 保存仪表板，如图 1-10 所示。

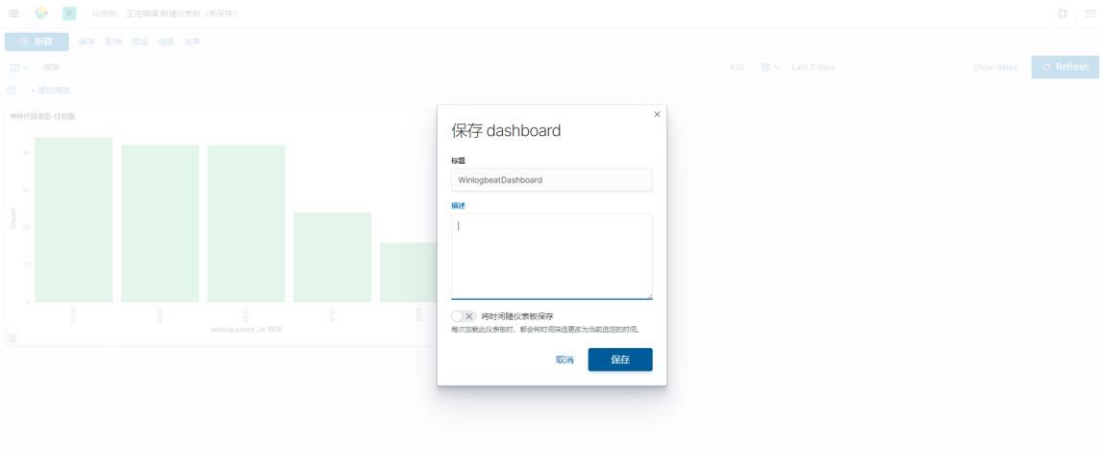

图 1-10 保存仪表板

（6） 全屏查看分析结果，如图 1-11 所示。

图 1-11 查看分析结果

步骤 03：仿照步骤 2，实现表 1-2 中的分析模型。

分析结果展示，如图 1-12 所示。

图 1-12 分析结果

八、实验思考

1、认识 Elastic Stack 和 ELK。

（1）什么是 Elastic Stack？

（2）什么是 ELK？

（3）Elastic Stack 与 ELK 的关系是什么？

2、深入理解 Elastic Stack。

（1）Elastic Stack 包含哪些软件组件？

（2）Elastic Stack 的软件组件各自功能是什么？之间的关系如何？

3、理解数据清洗与格式化。

（1）什么是数据清洗？

（2）Windows 事件数据的格式什么？

（3）本实训任务为何不使用 Logstach 对 Windows 事件数据进行数据清洗？