版 本	2020.1

《基于 CentOS 8 部署 Elastic Stack 快速手册》

文档时间：

学生学号：

学生姓名：

年级专业：2017 级 信息管理与信息系统

任课教师：阮晓龙 许成刚 高海波 冯顺磊(工程师)

河南中医药大学信息技术学院

2020 年 9 月

目 录

一、部署准备

1.1 基于 VirtualBox 部署 CentOS8

介绍虚拟机的配置信息。

配置项	配置值
虚拟机名	
虚拟机配置	操作系统类型： 内存： 处理器： 存储：
虚拟机网络配置	网卡 1：
CentOS 权限	操作系统账号： 系统账号口令：
备注	

1.2 Elastic Stack 部署准备

介绍部署准备所需要的依赖环境。

撰写部署步骤及配置代码。

二、部署过程

2.1 部署 Elasticsearch

撰写部署步骤及配置代码。

2.2 部署 Logstash

撰写部署步骤及配置代码。

2.3 部署 Kibana

撰写部署步骤及配置代码。

2.4 Elastic Stack 部署测试

撰写测试步骤及配置代码。

提供结果截图。

2.5 使用 Winlogbeat 采集 Windows Events 数据

撰写部署步骤及配置代码。

提供结果截图。

2.5 在 Kibana 上创建分析模型并进行分析

撰写部署步骤。

填写设计分析模型图表

序号	分析字段	分析模型	图表类型
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

展示分析结果并提供截图，多张截图，要确保图片能够看清。