实训任务三：实现对 Elastic Stack 日志分析平台的运维监控

一、目的

1、了解企业级日志分析平台综合运维监控体系；

2、掌握使用 BIND 部署 DNS 服务的方法；

3、掌握使用 Cacti 部署综合运维监控服务的方法。

二、学时

4 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。

每小组配备服务器 1 台。

2、软件

Windows 操作系统，安装 puTTY 管理终端软件，安装 VMware ESXi 控制台软件。

服务器安装 VMware ESXi 7.0。

3、网络

计算机、服务器、虚拟主机使用固定 IP 地址接入局域网，并支持对互联网的访问。

4、工具

无。

五、任务要求

1、完成 BIND 部署并实现 DNS 服务；

2、完成 Cacti 部署并实现运维监控服务；

3、完成企业级日志分析平台的整体监控。

六、考核要求

1、提交《运维监控服务部署方案与监控分析报告》。

七、任务步骤

本任务旨在实现企业级 Elastic Stack 日志分析平台的运维监控，需部署 DNS 实现域名解析，部署 Cacti 实现监控虚拟机监控。

参照《企业级 Elastic Stack 日志分析平台建设方案》确定虚拟机列表如表 3-1 所示。

表 3-1 虚拟机列表

序号	虚拟机名称
1	YWSX-10.10.2.152-CentOS8X64-Elasticsearch-Node1-Master
2	YWSX-10.10.2.153-CentOS8X64-Elasticsearch-Node2-Data
3	YWSX-10.10.2.154-CentOS8X64-Elasticsearch-Node3-Data
4	YWSX-10.10.2.155-CentOS8X64-Logstash-Node4
5	YWSX-10.10.2.156-CentOS8X64-Logstash-Node5
6	YWSX-10.10.2.157-CentOS8X64-Kibana-Node6
7	YWSX-10.10.2.162-CentOS8X64-Cacti
8	YWSX-10.10.2.163-CentOS8X64-DNS

任务 1：安装配置 BIND

DNS 是域名解析系统，在 Internet 中提供域名和 IP 地址的转换服务。BIND 是一款实现 DNS 服务器的开源软件，是全球最广泛使用的 DNS 服务器软件。

步骤 01：安装 BIND

参考命令：

```
yum install bind bind-utils –y
```

步骤 02：规划域名与记录

依据《企业级 Elastic Stack 日志分析平台建设方案》，设计域名规划表、记录规划表，如表 3-2，表 3-3 所示。

表 3-2 域名规划表

域名	缓存有效期	SOA	
yunwei.local	1 天	权威域名	dns.yunwei.local.
		管理员邮箱	mail.yunwei.local.
		版本号（serial）	20200901
		主辅同步周期（refresh）	1 天
		主辅同步重试间隔（retry）	1 小时
		同步数据存活期（expire）	1 周
		最小缓存有效期（minimum）	3 小时

表 3-3 记录规划表

记录类型	记录值	解析地址
NS	dns.yunwei.local.	
MX	mail.yunwei.local.	

A	dns	10.10.2.163
A	cacti	10.10.2.162
A	en1	10.10.2.152
A	en2	10.10.2.153
A	en3	10.10.2.154
A	ln4	10.10.2.155
A	ln5	10.10.2.156
A	kn6	10.10.2.157

步骤 03：配置主配置文件

参考命令：

```
vi /etc/named.conf
```

配置文件：

```
lisen-on port 53   { any; }                    #指定监听接口
allow-query   { any; }                         #配置所有主机可查询服务器的权威解析记录
zone  “yunwei.local”  IN {                     #定义域
      type master;                             #设置域类型为权威域名服务器
      file  “yunwei.local.zone”;               #定义域数据文件
}
```

步骤 04：配置解析域

参考命令：

```
vi /var/named/yunwei.local.zone
```

域解析文件：

```
$TTL 1D
@    IN        SOA       dns.yunwei.local.    mail.yunwei.local.   (
                         20200901
                         1D
                         1H
                         1W
                         3H
                         )
     IN        NS        dns.yunwei.local.
     IN        MAX       1          mail.yunwei.local.
     dns       IN        A          10.10.2.163
     cacti     IN        A          10.10.2.162
     en1       IN        A          10.10.2.152
     en2       IN        A          10.10.2.153
     en3       IN        A          10.10.2.154
     ln4       IN        A          10.10.2.155
     ln5       IN        A          10.10.2.156
     kn6       IN        A          10.10.2.157
```

步骤 04：配置防火墙规则

参考命令：

```
firewall-cmd --zone=public --add-port=53/tcp --permanent      #防火墙添加 tcp53 端口
firewall-cmd --zone=public --add-port=53/udp --permanent      #防火墙添加 udp53 端口
firewall-cmd --zone=public --add-port=161/udp --permanent     #防火墙添加 udp161 端口
firewall-cmd --reload                                         #防火墙重新加载配置使规则生效
```

步骤 05：测试 DNS 解析

参考命令：

```
#首先，将网卡 DNS 配置为 DNS 服务器 IP 地址 10.10.2.163
dig dns.yunwei.local          #查询 DNS 记录
```

提醒：

①实现 DNS 查询与域名解析的具体方法，参见教学视频。

教学视频地址：

http://dms.it.hactcm.edu.cn/api/h/f?m=f2d370da2d2861e2-1-0

Bilibili 访问地址：

https://www.bilibili.com/video/BV1j741177cu?p=49

扫码看教学视频

任务 2：部署 Cacti

Cacti 是一套基于 PHP、MySQL、SNMP 及 RRDTool 开发的网络流量监测图形分析工具。Cacti 通过 snmpget 来获取数据，使用 RRDtool 绘画图形。在需要监控的机器上，可以自定义脚本采集相关参数数据，通过 SNMP 服务采集发送给 Cacti，由 RRDTool 绘制参数变化趋势图。

步骤 01：部署 LAMP 环境

LAMP 是发布 PHP 程序的开源稳定架构，由 Linux 作为操作系统、Apache 作为网站服务器、MySQL/MariaDB 作为数据库管理系统、PHP/Perl/Python 作为服务器端脚本解释器。

提醒：

①实现 LAMP 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=17d3c89abb2298a5-1-0

Bilibili 访问地址：

https://www.bilibili.com/video/BV1j741177cu?p=26

扫码看教学视频

步骤 02：调整防火墙规则并关闭 SELinux

参考命令：

```
firewall-cmd --zone=public --add-port=80/tcp --permanent    #防火墙添加 tcp80 端口
firewall-cmd --reload                                       #防火墙重新加载配置使规则生效
setenforce 0                                                #关闭 SELinux
```

步骤 03：安装 RRDTool

参考命令：

```
yum install rrdtool -y
```

步骤 04：获取 Cacti 软件

参考命令：

```
yum install wget tar -y
wget https://www.cacti.net/downloads/cacti-1.2.10.tar.gz
```

步骤 05：安装 Cacti

提醒：

①使用 Cacti 建设网络监控服务的具体方法，参见教学视频。

教学视频地址：

http://dms.it.hactcm.edu.cn/api/h/f?m=5d32376a266eefbf-1-0

Bilibili 访问地址：

https://www.bilibili.com/video/BV1j741177cu?p=48

扫码看教学视频

任务 3：配置 SNMP

SNMP 是简单网络管理协议，可实现对设备的监控与管理。

步骤 01：在 CentOS 上配置 SNMP

（1）安装 net-snmp

参考命令：

```
yum install net-snmp -y
```

（2）配置 SNMP

参考命令：

```
vi /etc/snmp/snmpd.conf
com2sec notConfigUser  default  yunwei
```

（3）启动 SNMP 并设置开机自启

参考命令：

```
systemctl start snmpd
systemctl enable snmpd
```

（4）调整防火墙规则

参考命令：

```
firewall-cmd --add-port=161/udp --permanent
firewall-cmd --reload
```

步骤 02：在 Windows 10 上配置 SNMP

（1）安装 SNMP

以管理员身份运行 PowerShell，使用命令安装 SNMP。

参考命令：

```
add-windowscapability -online -name  “SNMP.Client~~~~0.0.1.0”
```

（2）设置 SNMP 团体名

启动“服务”程序，找到 SNMP 服务，设置团体名，如图 3-1。

（3）设置防火墙规则

启动“高级安全 Windows Defender 防火墙”，选择“入站规则”，找到“SNMP 服务”规则，启用、允许连接、远程 IP 地址设为任何 IP 地址，如图 3-2 和 3-3 所示。

步骤 03：在 VMware ESXi 上配置 SNMP

（1）通过控制台登录 VMware ESXi，如图 3-4 所示。

（2）按“F2”键进入“System Customization”，如图 3-5 所示。

（3）选择“Troubleshooting Options”菜单，启动 SSH，如图 3-6 所示。

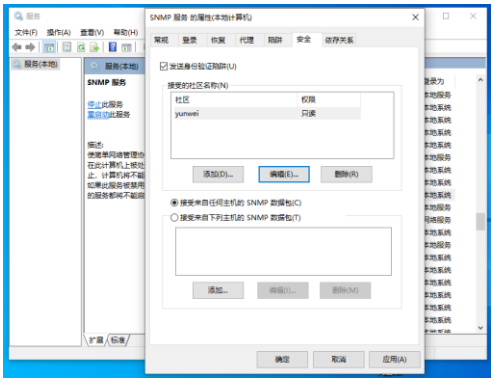

图 3-1 设置团体名

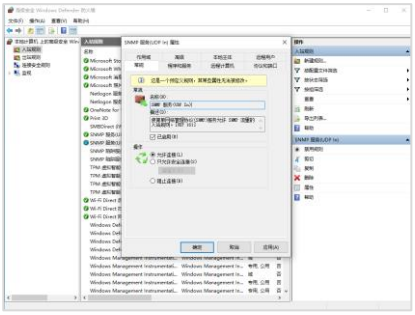

图 3-2 防火墙 SNMP 服务常规选项卡

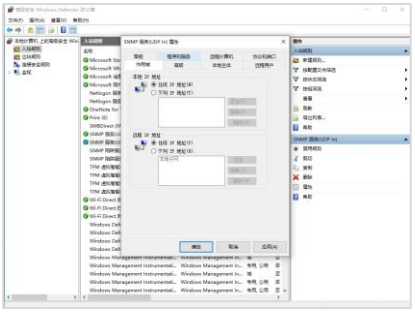

图 3-3 防火墙 SNMP 服务作用域选项卡

（4）通过 puTTY 远程登录 VMware ESXi，并配置 SNMP，如图 3-7 所示。

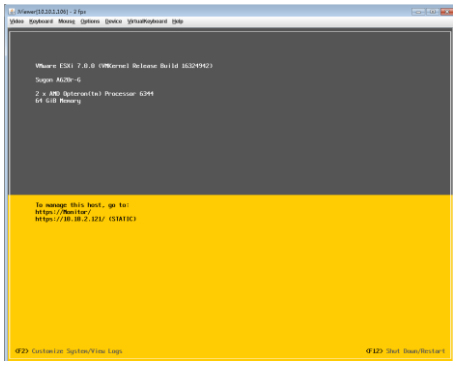

图 3-4 通过控制台登录 VMware ESXi

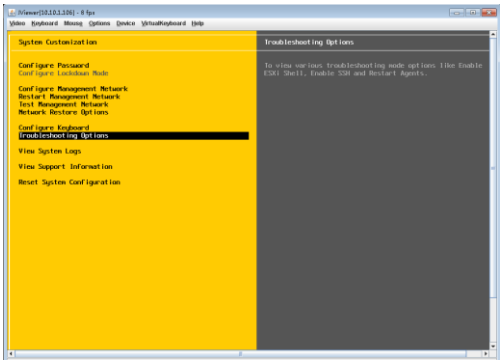

图 3-5 System Customization

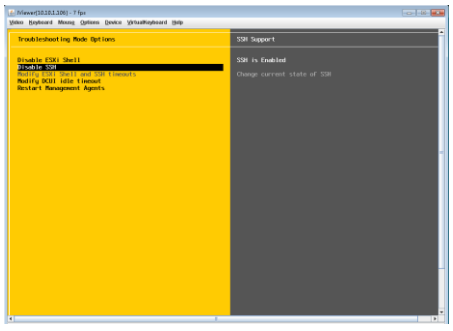

图 3-6 启动 SSH

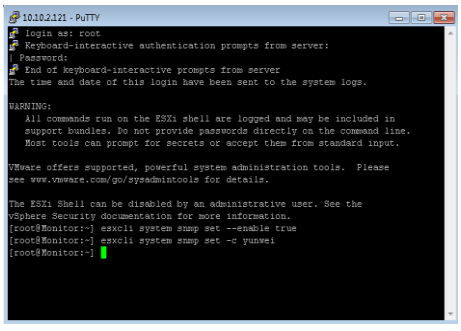

图 3-7 启动 SNMP 并设置共同体名

任务 4：实现监控

步骤 01：对虚拟化服务器进行监控

（1）点击“创建”，“新设备”，填写描述、主机名，选择“Local Linux Machine”模板，团体名为“yunwei”，点击“创建”按钮添加设备，如图 3-8 所示。

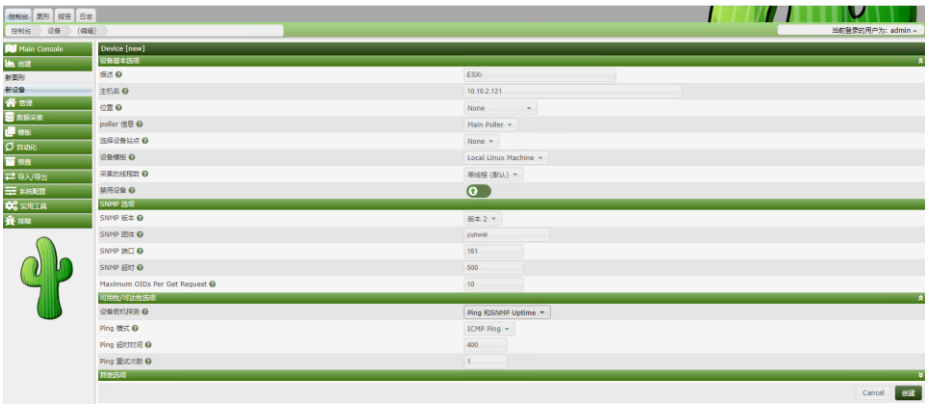

图 3-8 创建新设备

（2）点击“创建”，“新图形”，为设备添加新的图形，如图 3-9 所示。

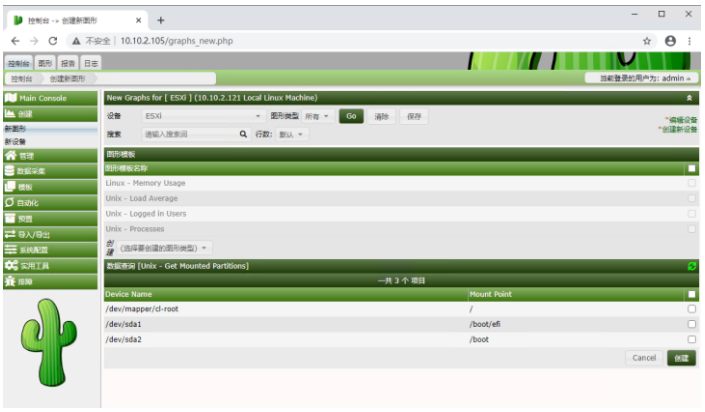

图 3-9 创建新图形

步骤 02：对虚拟机进行监控

依次完成表 1-1 所含的虚拟机监控配置。

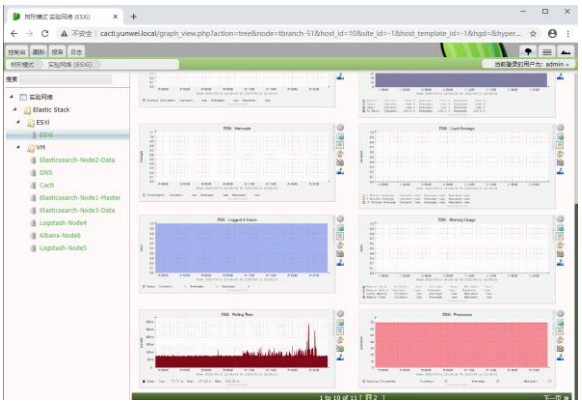

图 3-10 设备监控图形

步骤 03：查看监控图形

点击“图形”按钮，选择要查看的设备的监控图形，如图 3-10 所示。

步骤 04：部署预警与故障推送

点击“系统配置”，“设置”，“邮件/报告/DNS”设置电子邮箱并测试，如图 3-11 所示。

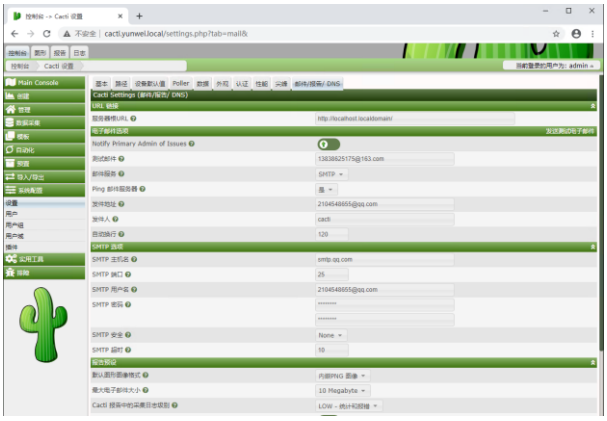

图 3-11 保存之后，点击“发送测试电子邮件”

八、实验思考

1、了解运维监控。

（1）为什么要对 Elastic Stack 日志分析平台进行运维监控？

（2）运维监控软件有哪些？

2、理解 SNMP。

（1）什么是 SNMP？其基本原理是什么？

（2）除了 SNMP 之外，还有哪些实现监控的技术或者协议？

3、监控服务的监控指标分析。

（1）虚拟化服务器的监控指标有哪些？

（2）虚拟主机的监控指标有哪些？

（3）企业级日志分析平台的监控指标有哪些？