# 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

# 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。

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			

#### 表 3-1 虚拟机列表

## 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。

域名	缓存有效期	SOA	
		权威域名	dns.yunwei.local.
		管理员邮箱	mail.yunwei.local.
		版本号(serial)	20200901
yunwei.local	1 天	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 3-2 域名规划表

#### 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.	

А	dns	10.10.2.163
А	cacti	10.10.2.162
А	en1	10.10.2.152
А	en2	10.10.2.153
А	en3	10.10.2.154
А	ln4	10.10.2.155
А	ln5	10.10.2.156
А	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; }
allow-query { any; }
zone "yunwei.local" IN {
 type master;
 file "yunwei.local.zone";

#指定监听接口 #配置所有主机可查询服务器的权威解析记录 #定义域 #设置域类型为权威域名服务器 #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				
域角				
\$TT	L1D			
@	IN	SOA	dns.yu	nwei.local. mail.yunwei.local. (
			20200	901
			1D	
			1H	
			1W	
			3H	
			)	
	IN	NS	dns.yu	inwei.local.
	IN	MAX	1	mail.yunwei.local.
	dns	IN	А	10.10.2.163
	cacti	IN	А	10.10.2.162
	en1	IN	А	10.10.2.152
	en2	IN	А	10.10.2.153
	en3	IN	А	10.10.2.154
	ln4	IN	А	10.10.2.155
	ln5	IN	А	10.10.2.156
	kn6	IN	А	10.10.2.157

# 步骤 04: 配置防火墙规则

# 参考命令:

firewall-cmdzone=publicadd-port=53/tcppermanent	#防火墙添加 tcp53 端口
firewall-cmdzone=publicadd-port=53/udppermanent	#防火墙添加 udp53 端口
firewall-cmdzone=publicadd-port=161/udppermanent	#防火墙添加 udp161 端口
firewall-cmdreload	#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

## <u>提醒:</u>

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



# 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。

## <u>提醒:</u>

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



步骤 02: 调整防火墙规则并关闭 SELinux

### 参考命令:

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

## <u>提醒:</u>

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

# 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 3-2 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 3-6 启动 SSH

图 3-5 System Customization



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。

检制台 图形 投音	88	
(注制台) 设备) (	(発展)	当期登录50月户为: admin =
📜 Main Console	Device [new]	
🗠 कहा	设施基本选项	â
新選形	宿送●	ESXi
新设备	主机名 <b>O</b>	10.10.2.121
<b>삼</b> 번째	020	None -
- 政保平規 1 1 1015	poller 信息 @	Main Poller ×
O nate	运择设备站在 🛛	None *
5276	没备情近	Local Linux Machine +
<b>≓</b> 9入/9出	采集的线程数 <b>O</b>	#65程(激以) =
<b>≆</b> 系統配置	禁用设备 <b>Θ</b>	
🗱 SHIH	SNMP 选项	
<u>A</u> 1880	SNMP 版本 😡	版本 2 ×
	SNMP 即体 @	suneei
	SNMP IN O	181
	SNMP 過时 🖗	500
	Maximum OIDs Per Get Request 🕖	10
	可用性/可达性选项	A
	の単位に相当	Ping #25NMP Uptime -
	Ping 模式 @	ICMP Ping -
	Ping 题时时间 🕢	400
	Ping 重成次数 🛛	1
	其他活动	¥
		Chand All

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。

← → C ▲ 7	安全   10.10.2.105/graphs_new.php	★ <b>0</b> :
控制論 图形 报告 日	8	
控制台 创建新面形		当朝登录的用户为: admin =
Main Console	New Graphs for [ ESXi ] (10.10.2.121 Local Linux Machine)	\$
म्ह भाषा	设备 E5Xi - 图形类型 所有 - Go 清除	保存 *@#25
新聞形 新聞帝	按数 请输入搜索闭 Q 行数: 数从 *	~创建和设计
A 192	四形模板	
in the second se	型形機板名称	
🛄 機板	Linux - Memory Usage	
0 自动化	Unix - Load Average	
- 92 <u>1</u>	Unix - Logged in Users	
≓ 9X/9±	Unix - Processes	
SKRAEN	8/ 建 (法科要创議的因形供型) -	
👯 CHIH	数组织前词 [Unix - Get Mounted Partitions]	
<u>it</u> 1130	—共3个	「項目
0	Device Name	Mount Point
	/dev/mapper/cl-root	/ 0
	/dev/sda1	/boot/efi
	/dev/sda2	/boot
7		Cancel

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。

🔰 拉利词 -> Cacti 说题	× +		- 0 ×
← → C ▲ ⊼s	₽£   cacti.yumwel.local/settings.php?tab=mail&		☆ <b>⊖</b> :
<b>注制台 </b>			
128/st Cacti (RM			目的登录的用户为: admin =
Main Console		E/REF/ DNS	
- est	Cacti Settings (#F#/#25/ DNS)		
2 mm	URL 1949		2
8849	服务器性URL O	http://iocalhost.localdomais/	
115	电子邮件包裹		发达测试电子邮件
1 nav	Notify Primary Admin of Issues O	0	
	测试邮件 😡	13838625175@163.com	
- 9X/9±	邮件报告 <b>O</b>	SMTP +	
系统和题	Ping 邮件服务器 😡	县 -	
2	发件33注 😡	2104548655@qq.com	
Bo tea	发祥人 <b>Q</b>	cacli	
8PM	B 約約行 🛛	120	
619	SMTP 西根		8
C SHII	SMTP ±118 0	smip.qq.com	
110	SMTP DEL O	25	
	SMTP 用户名 O	2104548655@qq.com	
	SMTP 密码 O	******	
		******	
7	SMTP 安全 0	None *	
	SMTP Hat O	10	
	· 全古预设		*
	新以图形图●核式 <b>●</b>	内御PNG 圆像 *	
	●大电子部阵大小 ●	10 Megabyte +	
	Cacti 报酬中的采集日志收制 😡	LOW - MitHallit	
		_	

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?