1 DESCRIÇÃO DOS RECURSOS UTILIZADOS

O ambiente de testes foi constituído dos seguintes recursos: um *notebook*, duas máquinas virtuais, um *smartphone*, uma *Raspberry Pi 3* e um roteador. O *notebook* foi conectado à rede via cabo *Ethernet*, hospedando as duas máquinas virtuais, ambas conectadas à rede em modo *bridge*. A *Raspberry Pi 3* e o *smartphone* foram conectados à rede sem fio.

1.1 Características dos Dispositivos

Tabela 1: Dispositivos utilizados no ambiente de testes

Máquina	Função	Sistema Operacional	Processador	RAM	IP Local
Notebook	Hospedeiro	*Ubuntu 18.04*	*Quad Core* 2.4GHz	8GB	192.168.25.150
Máquina Virtual 1	Gerente	*Lubuntu 18.10*	*Single Core* 2.4GHz	1GB	192.168.25.151
Máquina Virtual 2	Agente	*Lubuntu 18.10*	*Single Core* 2.4GHz	1GB	192.168.25.152
RaspberryPi 3	Agente	*UbuntuMATE 16.04*	*Quad Core* 1.2GHz	1GB	192.168.25.153

2 TOPOLOGIA DE REDE

Como podemos observar na Figura 1, a topologia de rede compreende:

- uma máquina principal, a qual hospeda as máquinas virtuais;
- duas máquinas virtuais, uma operando como gerente e a outra como agente;
- uma placa *Raspberry Pi 3*, operando também como agente;
- um *smartphone*, representando todos os demais dispositivos conectados à rede, os quais não foram monitorados;
- e um roteador, o qual nos permitiu estabelecer uma conexão pela rede local e também à rede externa.

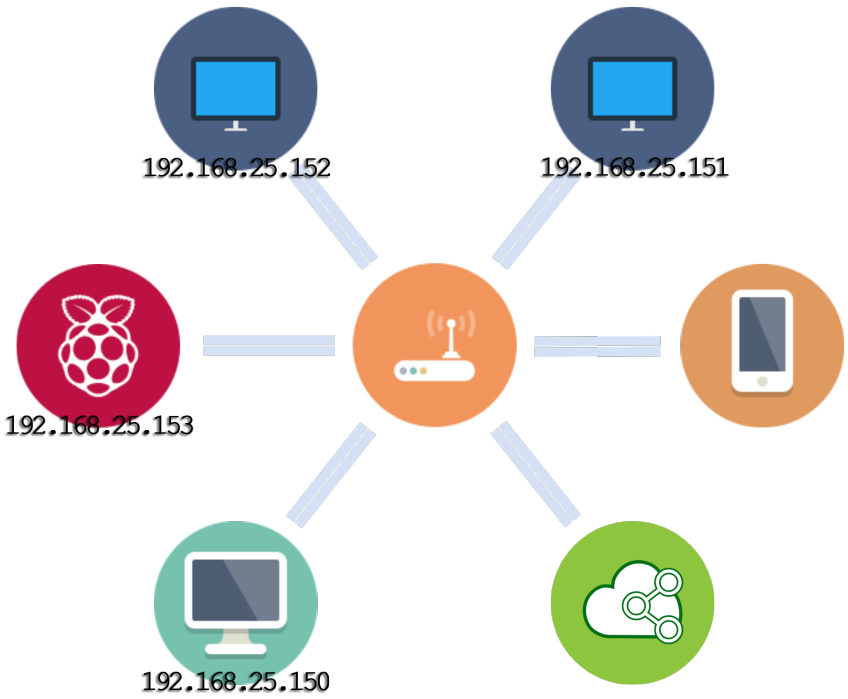

Figura 1: Topologia lógica do ambiente de testes

3 FERRAMENTAS DE GERÊNCIA

As ferramentas de gerência utilizadas neste trabalho foram o *Zabbix* e o *Wireshark*. Para monitorar diversas máquinas agentes, optou-se pelo *Zabbix* por ser um *software* de código aberto e que disponibiliza uma grande variedade de ferramentas para auxiliar na gerência das máquinas. Com ele é possível monitorar serviços simples como *HTTP*, *POP3*, *IMAP* e *SSH* sem o uso de agentes. Possui suporte nativo ao protocolo *SNMP*, além de integração com banco de dados. O *Zabbix* é de fácil instalação, permitindo o uso em diversos sistemas operacionais, e possuindo uma documentação extensa e bem detalhada.

Para capturar os pacotes da comunicação *SNMP* e garantir o funcionamento do monitoramento das máquinas, utilizou-se o *Wireshark*. O *Wireshark* é um *software* que analisa o tráfego da rede, organizando-o por protocolos. Desta forma, conseguimos realizar os testes e verificar o funcionamento de nosso sistema.

A seguir, explicaremos a instalação e a utilização de ambas as ferramentas.

3.1 *Zabbix*

3.1.1 *Zabbix Server*

O *Zabbix Server* foi instalado em uma das máquinas virtuais, a qual atuou em modo gerente. A seguir, mostramos os passos utilizados para a instalação e configuração do *Zabbix Server*.

Instalação de dependências

```
# apt update
# apt install build-essential gcc libsnmp-dev libxml2-dev
```

Instalação do banco de dados

```
# apt install mariadb-server mariadb-client libmysqld-dev
```

Instalação do servidor web Apache e PHP

```
# apt install apache2 php7.2 php7.2-mysql php7.2-gd php7.2-cli php7.2-xmlrpc
             libapache2-mod-php
```

Configuração do PHP para a execução do Zabbix Server

```
# nano /etc/php/7.2/apache2/php.ini
```

Será necessária a alteração das seguintes linhas:

```
post_max_size = 32M
max_execution_time = 600
max_input_time = 600
date.timezone = America/Sao_Paulo
always_populate_raw_post_data = 1
```

Reinicialização do servidor Apache

```
# systemctl restart apache2.service
```

Download e instalação do Zabbix Server

```
# wget https://repo.zabbix.com/zabbix/4.0/ubuntu/pool/main/z/zabbix-release/
      zabbix-release_4.0-2+bionic_all.deb
# dpkg -i zabbix-release_4.0-2+bionic_all.deb
# apt update
# apt -y install zabbix-server-mysql zabbix-frontend-php zabbix-agent
```

Configuração do banco de dados para utilização pelo Zabbix Server

```
# mysql -uroot -p
MariaDB> create database zabbix character set utf8 collate utf8_bin;
MariaDB> grant all privileges on zabbix.* to zabbix@localhost
         identified by 'password';
MariaDB> quit;
```

Importação do esquema inicial

```
# zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz
    | mysql -uzabbix -p zabbix
password
```

Configuração do Zabbix Server para acesso ao banco de dados

```
# nano /etc/zabbix/zabbix_server.conf
```

Será necessária a alteração da seguinte linha:

```
DBPassword=password
```

Configuração do fuso horário

```
# nano /etc/zabbix/apache.conf
```

Será necessária a alteração da seguinte linha:

```
php_value date.timezone America/Sao_Paulo
```

Reinicialização dos serviços

```
# systemctl restart zabbix-server zabbix-agent apache2
# systemctl enable zabbix-server zabbix-agent apache2
```

Configuração do Zabbix Frontend

Agora, acessaremos a interface do *Zabbix Server*, disponível pelo link:

<http://localhost/zabbix>

Continuamos em frente até que a senha seja requisitada. A senha definida nos passos de configuração foi:

```
password
```

Inserimos um nome para o servidor (opcional), e seguimos até o final da instalação.

Login

O acesso poderá ser feito utilizando o nome de usuário padrão **Admin** e a senha **zabbix**.

3.1.2 *Zabbix Agent*

Download e instalação do Zabbix Agent

```
# wget https://repo.zabbix.com/zabbix/4.0/ubuntu/pool/main/z/
      zabbix-release/zabbix-release_4.0-2+bionic_all.deb
# dpkg -i zabbix-release_4.0-2+bionic_all.deb
# apt update
# apt -y install zabbix-agent
```

Configuração do Zabbix Agent

```
# nano /etc/zabbix/zabbix_agentd.conf
```

Será necessária a alteração das seguintes linhas:

```
Server = 192.168.25.151
ServerActive = 192.168.25.151
Hostname = Cliente1
```

Instalação e configuração do SNMP

```
# apt install snmp snmpd
```

Por padrão, o protocolo *SNMP* está configurado para procurar por conexões apenas da própria máquina. Para permitir que o *SNMP* se conecte também a outras interfaces de rede, será necessário comentar a primeira linha e remover o comentário da segunda linha, conforme o exemplo:

```
#agentAddress udp:127.0.0.1:161
agentAddress udp:161,udp6[::1]:161
```

Reinicialização dos serviços

```
# systemctl restart snmpd zabbix-agent
# systemctl enable snmpd zabbix-agent
```

3.1.3 *Zabbix Frontend*

Agora, será necessário informar ao *Zabbix Server* todos os *hosts* aos quais ele deverá monitorar. Todo o processo ocorrerá através da interface do *Zabbix Server* pelo navegador.

Adicionando um host

No menu principal, selecionamos as opções **Configuration > Hosts > Create host**.

Escolhemos um nome e um grupo para o *host*.

Para permitirmos a captura de dados tanto pelo agente quanto pelo *SNMP*, adicionaremos uma interface para cada, informando o endereço IP do *host*.

Na aba **Templates**, há a possibilidade de escolher entre alguns *templates*, o que habilitará alguns **itens** prontos para utilizarmos. Porém, não faremos uso de nenhum *template*.

Para finalizar, basta apertar em **Add**.

Adicionando itens ao host

Itens são as atividades de coleta de dados que serão feitas no *host*. Para adicionar um item, vamos até o menu de **hosts**, aberto anteriormente, e, selecionando o *host*, vamos até a opção **Items > Create item**.

Escolhemos um nome para o item.

A chave é escolhida em um conjunto pré-definido pelo sistema, e fornece um método de coleta dos dados. Neste trabalho foram criados três itens, utilizando as seguintes *keys*:

- net.if.in[in]
- net.if.out[if]
- system.cpu.load

As duas primeiras buscam as estatísticas de entrada e saída de dados pela interface de rede definida, e a segunda registra o uso da *CPU*.

Por fim, basta selecionarmos **Add**.

Para mais informações, acesse a documentação do *Zabbix 4.0*, disponível através do link:

<https://www.zabbix.com/documentation/4.0/start>

Visualizando os dados

Para visualizarmos os gráficos, vamos em **Monitoring > Latest data**. Agora, selecionamos um dos itens e vamos até **Graph**, situado no canto direito.

3.2 *Wireshark*

3.2.1 Instalação

Para a instalação do *Wireshark*, serão necessários apenas dois comandos:

```
# apt update
# apt install wireshark
```