

Roteiro 2 - Operação e Gerenciamento

Cyber Segurança em Nuvem 2024.1

Grupo: Antônio Martins, Ariel Leventhal e Enricco Gemha

1. Introdução

O Zabbix é uma ferramenta **OpenSource** de monitoramento de infraestrutura que permite o monitoramento de diversos tipos de dispositivos, entre eles servidores, identificando o uso de CPU, memória, disco, entre outros parâmetros. O Zabbix é uma ferramenta muito utilizada por empresas devido a sua facilidade de uso e configuração, além de ser uma ferramenta gratuita.

2. Instalação

2.1 Instalação do Zabbix Server

Para a instalação do Zabbix Server foram utilizados os comandos disponibilizados no roteiro desta atividade, com algumas alterações de sintaxe.

```
sudo dpkg -i zabbix-release_6.0-4+ubuntu22.04_all.deb
sudo apt update
sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-
conf zabbix-sql-scripts zabbix-agent
```

Após a instalação foi criado um novo banco de dados MySQL para o Zabbix. E foi iniciado o serviço do Zabbix Server.

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

2.1.2 Configuração do Zabbix

Com o Zabbix server instalado há a necessidade de acessar o frontend do Zabbix para finalizar sua configuração:

The left window displays the Zabbix documentation for '3 Installation from sources'. It lists various steps and notes, such as:

- 4 Configure the sources
- 5 Make and install everything
- 6 Review and edit configuration files
- 7 Start up the daemons
- 2 Installing Zabbix web interface
 - COPYING PHP files
 - Installing frontend
- 3 Installing Java gateway
- 4 Installing Zabbix web service

The right window shows the 'Configure DB connection' step of the Zabbix setup wizard. The 'Database type' is set to 'MySQL', and the 'Database host' is set to 'localhost'. Other fields include 'Database port' (0), 'Database name' (zabbix), and 'User' (zabbix). The note at the bottom states: 'Connection will not be encrypted because it uses a socket file (on Unix) or shared memory (Windows)'.

Após a configuração do banco de dados e a senha do usuário zabbix, há necessidade de se alterar o Name Server

The left window displays the Zabbix documentation for '3 Installation from sources', showing the same steps as the previous screenshot.

The right window shows the 'Settings' step of the Zabbix setup wizard. The 'Zabbix server name' is set to 'zabbix-server', the 'Default time zone' is set to '(UTC-03:00) America/Sao_Paulo', and the 'Default theme' is set to 'Dark'. The note at the bottom states: 'Licensed under GPL v2'.

Com isso o Zabbix Server inicia a configuração automática de seu ambiente.

Neste momento o grupo percebeu que a CPU da instância T2.micro não aguentou a instalação do Zabbix Server, atingiu 100% de uso e travou. Com isso o serviço foi iniciado novamente em uma nova instância T2.medium.

The screenshot shows the AWS CloudWatch Metrics Insights interface. On the left, there's a sidebar with various AWS services like EC2, S3, Lambda, etc. The main area is titled "Instances (1/5) info" and shows a table of EC2 instances. One instance, "zabbix" (ID: i-0e28008408d0a743), is selected. Below the table, a detailed view for "Instance: i-0e28008408d0a743 (zabbix)" is shown. The "Monitoring" tab is selected, displaying several line charts over a 1-hour period. The charts include "CPU utilization (%)", "Network in (bytes)", "Network out (bytes)", "Network packets out (count)", "CPU credit usage (count)", and "CPU credit balance (count)". Each chart has a legend and some specific data points labeled.

The screenshot shows the Zabbix Global view dashboard. On the left, there's a sidebar with navigation links like Monitoring, Services, Inventory, Reports, Configuration, Administration, Support, Integrations, Help, User settings, and Sign out. The main area is titled "Global view" and contains several sections: "System information" (with a table showing metrics like Zabbix server is running, number of hosts, templates, items, triggers, and users), a "Problems" table (showing a single entry for a Zabbix server restart), and "Favorite maps" and "Favorite graphs" sections. A large clock icon is also present on the right side.

2.2 Instalação do Zabbix Agent

Com o Zabbix Server instalado, há a necessidade de conectar todas as instâncias da rede privada utilizando o Zabbix Agent. Para isso foram utilizados os seguintes comandos, em cada uma das instâncias:

```
sudo wget http://repo.zabbix.com/zabbix/3.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_3.0-2+bionic_all.deb
sudo apt update
sudo apt-get install zabbix-agent
sudo ufw allow 10050/tcp
```

Após a instalação do Zabbix Agent, é necessário configurar o arquivo de configuração do Zabbix Agent, localizado em `/etc/zabbix/zabbix_agentd.conf`. Neste arquivo é necessário alterar o `Server` e `ServerActive` para o IP do Zabbix Server, e o `Hostname` para o nome da instância.

```
Server=172.31.0.197
ServerActive=172.31.0.197:10051
```

Após a configuração do arquivo de configuração do Zabbix Agent, é necessário reiniciar o serviço do Zabbix Agent.

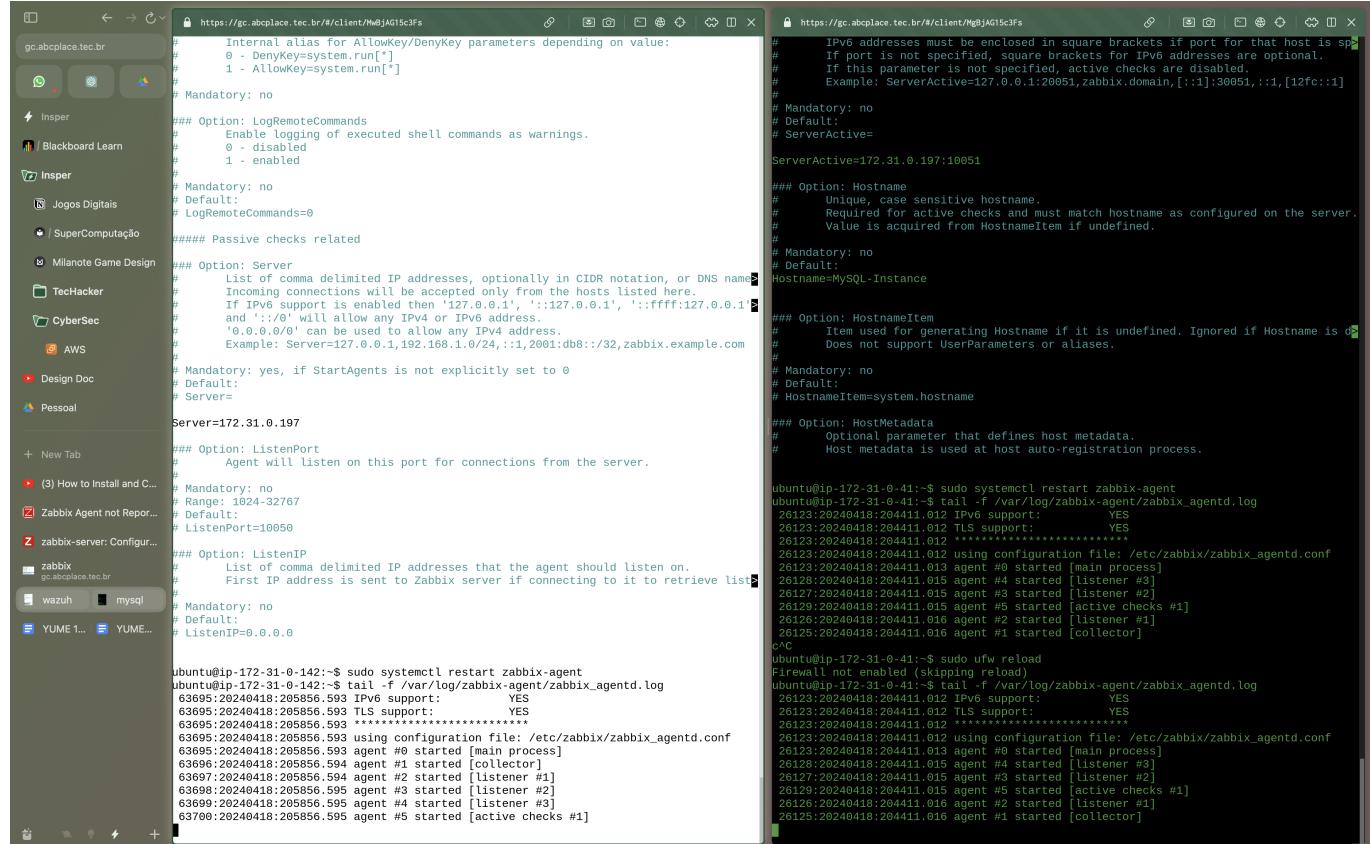
```
sudo service zabbix-agent restart
```

Caso o service não esteja `enabled` é necessário habilitar o serviço.

```
sudo systemctl enable zabbix-agent
```

Para checar se o Zabbix Agent está em funcionamento é necessário acessar o seguinte LOG:

```
tail -f /var/log/zabbix/zabbix_agentd.log
```



```
# Internal alias for AllowKey/DenyKey parameters depending on value:
#   0 - DenyKey=system.run[*]
#   1 - AllowKey=system.run[*]
#
# Mandatory: no

### Option: LogRemoteCommands
#   Enable logging of executed shell commands as warnings.
#   0 - disabled
#   1 - enabled
#
# Mandatory: no
# Default:
# LogRemoteCommands=0

##### Passive checks related

### Option: Server
#   List of comma delimited IP addresses, optionally in CIDR notation, or DNS names
# Incoming connections will be accepted only from the hosts listed here.
# If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1'
# and '::/0' will allow any IPv4 or IPv6 address.
# '0.0.0.0/0' can be used to allow any IPv4 address.
# Example: Server=127.0.0.1,192.168.1.0/24,:1,2001:db8::/32,zabbix.example.com
#
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=172.31.0.197

Server=172.31.0.197

### Option: ListenPort
#   Agent will listen on this port for connections from the server.
#
# Mandatory: no
# Range: 1024-32767
# Default:
# ListenPort=10050

### Option: ListenIP
#   List of comma delimited IP addresses that the agent should listen on.
# First IP address is sent to Zabbix server if connecting to it to retrieve lists
#
# Mandatory: no
# Default:
# ListenIP=0.0.0.0

ubuntu@ip-172-31-0-142:~$ sudo systemctl restart zabbix-agent
ubuntu@ip-172-31-0-142:~$ tail -f /var/log/zabbix-agent/zabbix_agentd.log
63695:20240418:205856.593 IPv6 support: YES
63695:20240418:205856.593 TLS support: YES
63695:20240418:205856.593 ****
63695:20240418:205856.593 using configuration file: /etc/zabbix/zabbix_agentd.conf
63695:20240418:205856.593 agent #0 started [main process]
63695:20240418:205856.594 agent #1 started [collector]
63697:20240418:205856.594 agent #2 started [listener #1]
63698:20240418:205856.595 agent #3 started [listener #2]
63699:20240418:205856.595 agent #4 started [listener #3]
63700:20240418:205856.595 agent #5 started [active checks #1]

ubuntu@ip-172-31-0-41:~$ sudo ufw reload
Firewall not enabled (skipping reload)
ubuntu@ip-172-31-0-41:~$ tail -f /var/log/zabbix-agent/zabbix_agentd.log
26123:20240418:204411.012 IPv6 support: YES
26123:20240418:204411.012 TLS support: YES
26123:20240418:204411.012 ****
26123:20240418:204411.012 using configuration file: /etc/zabbix/zabbix_agentd.conf
26123:20240418:204411.013 agent #0 started [main process]
26123:20240418:204411.014 agent #1 started [listener #3]
26127:20240418:204411.015 agent #3 started [listener #2]
26129:20240418:204411.015 agent #5 started [active checks #1]
26126:20240418:204411.016 agent #2 started [listener #1]
26125:20240418:204411.016 agent #1 started [collector]
c

ubuntu@ip-172-31-0-41:~$ sudo ufw reload
Firewall not enabled (skipping reload)
ubuntu@ip-172-31-0-41:~$ tail -f /var/log/zabbix-agent/zabbix_agentd.log
26123:20240418:204411.012 IPv6 support: YES
26123:20240418:204411.012 TLS support: YES
26123:20240418:204411.012 ****
26123:20240418:204411.012 using configuration file: /etc/zabbix/zabbix_agentd.conf
26123:20240418:204411.013 agent #0 started [main process]
26123:20240418:204411.014 agent #4 started [listener #3]
26127:20240418:204411.015 agent #3 started [listener #2]
26129:20240418:204411.015 agent #5 started [active checks #1]
26126:20240418:204411.016 agent #2 started [listener #1]
26125:20240418:204411.016 agent #1 started [collector]
```

2.3 Configuração das Instâncias no Zabbix Dashboard

The screenshot shows the Zabbix 'Hosts' configuration interface. At the top, there are search and filter fields for 'Host groups', 'Templates', 'Name', 'DNS', 'IP', and 'Port'. Below these are buttons for 'Monitored by Any', 'Server', and 'Proxy'. There are also 'Tags' and 'Filter' dropdowns. The main area displays a table of hosts with columns: Name, Items, Triggers, Graphs, Discovery, Web, Interface, Proxy, Templates, Status, Availability, Agent encryption, Info, and Tags. The table lists the following hosts:

Name	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption	Info	Tags
Guacamole-Instance	Items 42	Triggers 14	Graphs 6	Discovery 3	Web	172.31.0.147:10050	Linux by Zabbix agent		Enabled	ZBX	None		
MySQL-Instance	Items 73	Triggers 27	Graphs 14	Discovery 3	Web	172.31.0.41:10050	Linux by Zabbix agent		Enabled	ZBX	None		
Wazuh-Instance	Items 73	Triggers 27	Graphs 14	Discovery 3	Web	172.31.0.142:10050	Linux by Zabbix agent		Enabled	ZBX	None		
Wordpress-Instance	Items 42	Triggers 14	Graphs 8	Discovery 3	Web	172.31.0.188:10050	Linux by Zabbix agent		Enabled	ZBX	None		
Zabbix server	Items 121	Triggers 85	Graphs 24	Discovery 4	Web	127.0.0.1:10050	Linux by Zabbix agent, Zabbix server health		Enabled	ZBX	None		

At the bottom left are buttons for '0 selected', 'Enable', 'Disable', 'Export', 'Mass update', and 'Delete'. On the right, it says 'Displaying 5 of 5 found'. The footer indicates 'Zabbix 6.0.28. © 2001–2024, Zabbix SIA'.

Com isso todas as instâncias estão conectadas ao Zabbix Server e estão sendo monitoradas.

3. Perguntas

3.1 O gerenciamento do ambiente Zabbix será realizado por meio de um agente instalado nos servidores. Qual a diferença do gerenciamento por agente e pelo protocolo SNMP?

Normalmente o Agente Zabbix ou Zabbix Agent é utilizado para monitorar servidores e computadores que tenham a capacidade de instalar o agente, havendo a necessidade de utilizarem sistema operacional compatível com o agente, e terem interfaces de rede que permitam a comunicação nas portas necessárias (10050 e 10051). Para dispositivos que não detenham estes pré requisitos é possível utilizar o protocolo SNMP, que possibilitará a coleta de informações sobre o dispositivo.

Caso fosse utilizado neste roteiro o SNMP ao invés do Zabbix Agent, haveria apenas a necessidade de se configurar o SNMP em todas as instâncias seguindo a documentação do Zabbix (<https://www.zabbix.com/documentation/current/pt/manual/config/items/itemtypes/snmp>). Porém em situações que hajam dispositivos não compatíveis como Switchs, roteadores, impressoras, seria necessária a configuração de ambos os serviços.

3.2 O que é um NOC?

O Network Operations Center (NOC) é um local de monitoramento, gerenciamento e controle de uma rede de computadores, sendo responsável por possibilitar o funcionamento de uma rede de forma eficiente e segura. Em muitas empresas este centro de operações é responsável por monitorar a rede 24 horas por dia, tendo um sistema de monitoramento híbrido, que utiliza tanto computadores, sistemas de alertas, inteligência artificial e pessoas para monitorar a rede.

Uma vez que o NOC detecta um problema na rede, ele é responsável por identificar a causa do problema e corrigi-lo, ou então encaminhar o problema para a equipe responsável pela correção.

3.3 O que é uma MIB?

O Management Information Base (MIB) é um banco de dados que têm como objetivo armazenar dados de entidades em uma rede de computadores. A MIB é utilizada para armazenar informações de dispositivos de rede, como servidores, mantendo informações sobre o status de cada dispositivo, uso de CPU, memória, disco, entre outras informações relacionadas a capacidade e performance dos dispositivos.

Como funciona o protocolo SNMP?

O Simple Network Management Protocol (SNMP) é um protocolo utilizado para o gerenciamento de dispositivos de rede, sejam eles roteadores, computadores, servidores, entre outros que estejam conectados a rede e suportem o protocolo. Este protocolo funciona na camada de aplicação, do modelo OSI, e é utilizado para monitorar e gerenciar dispositivos de rede.