

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

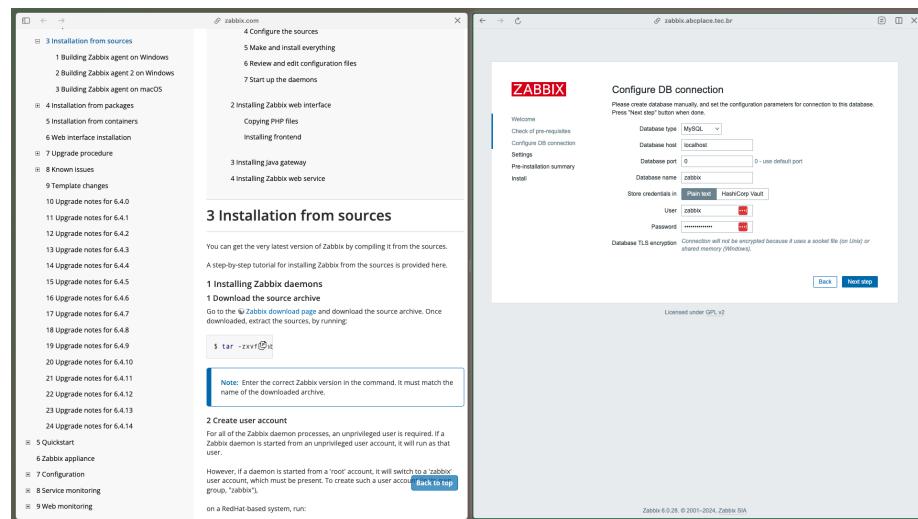
2.1 Instalação do Zabbix Server Para a instalação do Zabbix Server foram utilizados os comandos disponibilizados no roteiro desta atividade, com algumas alterações de sintaxe.

```
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
```

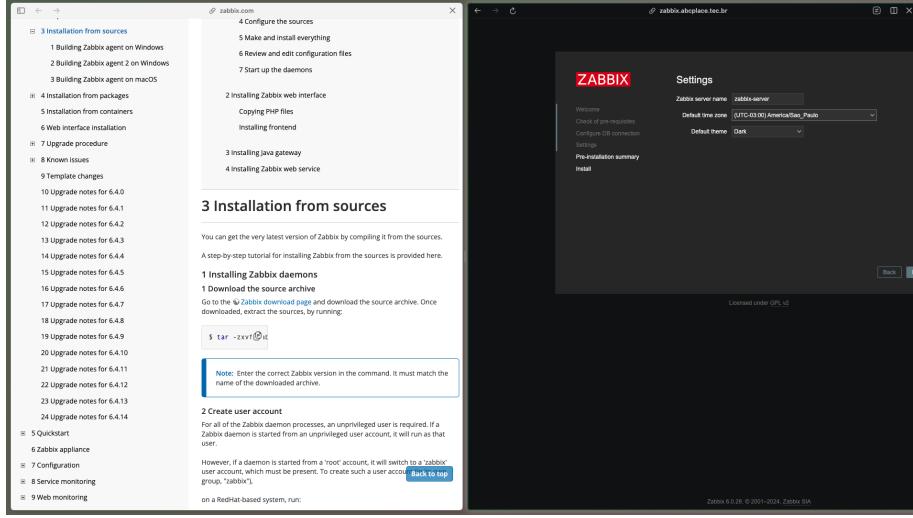
Após a instalação foi criado um novo banco de dados MySQL para o Zabbix. E foi iniciado o serviço do Zabbix Server.

```
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:

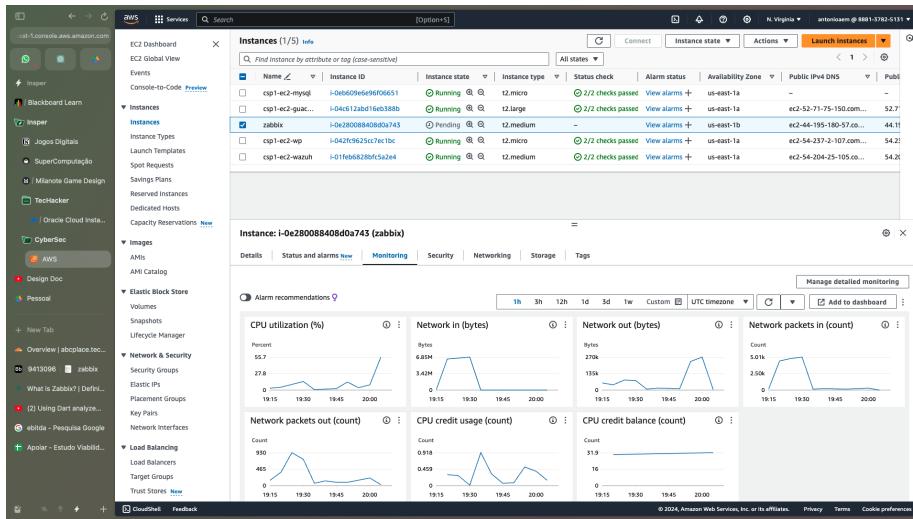


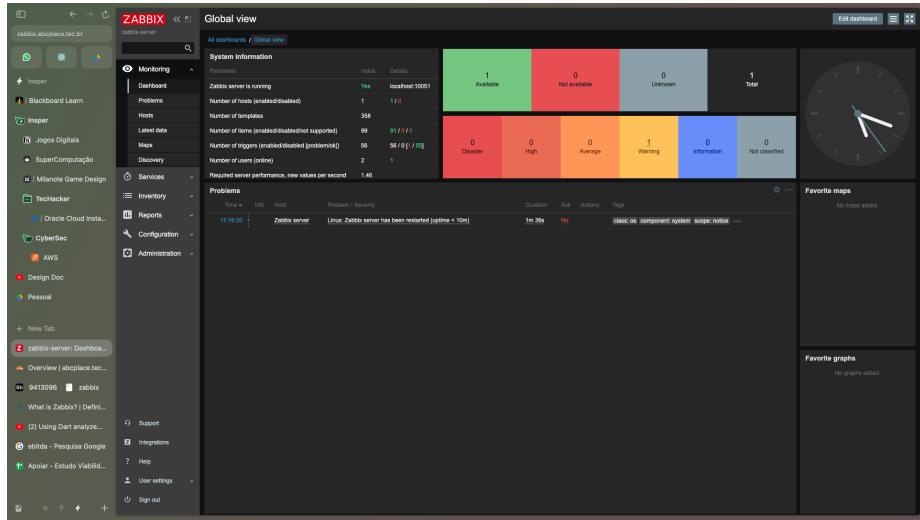
Após a configuração do banco de dados e a senha do usuário zabbix, há necessidade de se alterar o Name Server



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.





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
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 serviço 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
```

```

https://gc.apolice.tec.br/zabbix/client/mw/agent39s
Internal alias for AllowKey/DenyKey parameters depending on value:
#   0 - DenyKey$system.run[""]
#   1 - AllowKey$system.run[""]
Mandatory: no

## Option: LogServiceCommands
#   0 - disable logging of executed shell commands as warnings.
#   0 - disabled
#   1 - enabled
Mandatory: no

## Option: LogServiceErrors
#   0 - disable
#   1 - enable
Mandatory: no

## Option: Passive checks related
#   0 - list of comma delimited IP addresses, optionally in CIDR notation, or DNS names
#   Incoming connections will be accepted only from the hosts listed here.
#   IP '0.0.0.0' will accept any IPv4 or IPv6 address.
#   and '::/0' will allow any IPv6 or IPv6 address.
#   Example: Server=127.0.0.1,127.0.0.1,::ffff:127.0.0.1
#   '0.0.0.0/0' can be used to allow any IPv4 address.
#   Example: Server=127.0.0.1,127.0.0.1,0.0.0.0/0,::ffff:127.0.0.1,::ffff:127.0.0.1
Mandatory: yes, if StartAgents is not explicitly set to 0
Default:
Servers:
Server=127.31.0.197

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

new 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 list
#   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
[...]
63695:26249418:298856:593 TLS support: .....YES
63695:26249418:298856:593 agent #0 started [main process]
63695:26249418:298856:593 using configuration file: /etc/zabbix/zabbix_agentd.conf
63695:26249418:298856:593 agent #0 started [main process]
63695:26249418:298856:594 agent #1 started [main process]
63695:26249418:298856:594 agent #2 started [main process]
63695:26249418:298856:594 agent #3 started [main process]
63695:26249418:298856:594 agent #4 started [main process]
63695:26249418:298856:594 agent #5 started [main process]
63695:26249418:298856:594 agent #6 started [main process]
63695:26249418:298856:594 agent #7 started [main process]
63695:26249418:298856:594 agent #8 started [main process]
63695:26249418:298856:594 agent #9 started [main process]
63695:26249418:298856:595 agent #0 started [active checks #1]
63695:26249418:298856:595 agent #1 started [active checks #1]
63695:26249418:298856:595 agent #2 started [active checks #1]
63695:26249418:298856:595 agent #3 started [active checks #1]
63695:26249418:298856:595 agent #4 started [active checks #1]
63695:26249418:298856:595 agent #5 started [active checks #1]
63695:26249418:298856:595 agent #6 started [active checks #1]
63695:26249418:298856:595 agent #7 started [active checks #1]
63695:26249418:298856:595 agent #8 started [active checks #1]
63695:26249418:298856:595 agent #9 started [active checks #1]
63695:26249418:298856:596 agent #0 started [collector]

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
[...]
26123:20240418:204411:032 TLS support: .....YES
26123:20240418:204411:032 agent #0 started [main process]
26123:20240418:204411:032 using configuration file: /etc/zabbix/zabbix_agentd.conf
26123:20240418:204411:032 agent #0 started [main process]
26128:20240418:204411:019 agent #4 started [listener #3]
26128:20240418:204411:019 agent #5 started [active checks #1]
26129:20240418:204411:030 agent #3 started [active checks #1]
26126:20240418:204411:019 agent #2 started [listener #1]
26126:20240418:204411:019 agent #3 started [active checks #1]
26126:20240418:204411:019 agent #4 started [collector]

ubuntu@ip-172-31-0-142:~$ sudo systemctl restart zabbix-server
ubuntu@ip-172-31-0-142:~$ tail -f /var/log/zabbix/zabbix_server.log
[...]
26123:20240418:204411:032 TLS support: .....YES
26123:20240418:204411:032 agent #0 started [main process]
26123:20240418:204411:032 using configuration file: /etc/zabbix/zabbix_server.conf
26123:20240418:204411:032 agent #0 started [main process]
26128:20240418:204411:019 agent #4 started [listener #3]
26128:20240418:204411:019 agent #5 started [active checks #1]
26127:20240418:204411:030 agent #3 started [active checks #1]
26129:20240418:204411:019 agent #2 started [listener #1]
26129:20240418:204411:019 agent #3 started [active checks #1]
26129:20240418:204411:019 agent #4 started [active checks #1]
26125:20240418:204411:030 agent #1 started [active checks #1]
26125:20240418:204411:030 agent #2 started [active checks #1]
26125:20240418:204411:030 agent #3 started [active checks #1]
26125:20240418:204411:030 agent #4 started [active checks #1]
26125:20240418:204411:030 agent #5 started [active checks #1]

```

Name	Item	Triggers	Graphs	Discovery	Web	Interface	Proxy
Guacamole-Instance	Item #2	Triggers #4	Graphs #3	Discovery #1	Web	172.31.0.147:50000	Used by Zabbix agent
MySQL-Instance	Item #3	Triggers #7	Graphs #4	Discovery #1	Web	172.31.0.41:10500	Used by Zabbix agent
Web-Instance	Item #3	Triggers #7	Graphs #4	Discovery #1	Web	172.31.0.142:10500	Used by Zabbix agent
Wordpress-Instance	Item #2	Triggers #4	Graphs #3	Discovery #1	Web	172.31.0.185:10500	Used by Zabbix agent
Zabbix server	Item #21	Triggers #6	Graphs #4	Discovery #1	Web	127.0.0.1:10500	Used by Zabbix agent

2.3 Configuração das Instâncias no Zabbix Dashboard

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.