Comparação de Ferramentas para Monitoramento de Redes de Computadores em Ambientes Simulados

Cinthia Fabiula. Matte
Centro Universitário Dinâmica das Cataratas (UDC)
Foz do Iguaçu, Brasil
cinthiamatte@gmail.com

Gabriel Langwinski
Centro Universitário Dinâmica das Cataratas (UDC)
Foz do Iguaçu, Brasil
gabriel.langwinski@gmail.com

Luciano Santos Cardoso
Centro Universitário Dinâmica das Cataratas (UDC)
Foz do Iguaçu, Brasil
luciano.cardoso@udc.edu.br

Alessandra Bussador
Centro Universitário Dinâmica das Cataratas (UDC)
Foz do Iguaçu, Brasil
alessandra@udc.edu.br

***Abstract*— This article proposes a comparison of free tools Zabbix, The Dude and Nagios for monitoring computer networks through a simulated environment using the network software emulator GNS3. With this simulation and the effort to configure each system, which is the object of this study, the SNMPv2 configuration, network latency and traffic and its data exposure were analyzed.**

***Resumo* — Este artigo propõe a comparação das ferramentas gratuitas Zabbix, The Dude e Nagios para monitoramento de redes de computadores através de um ambiente simulado utilizando o emulador de software de rede GNS3. Com esta simulação e o esforço de configuração de cada sistema, que é objeto deste estudo, foi analisada a configuração do SNMPv2, latência e tráfego da rede e sua exposição de dados.**

***Palavras-chave*—Monitoramento; Redes de Computadores; Simulação.**

I. INTRODUÇÃO

Com a evolução da tecnologia da informação, surgiu a necessidade de exploração e aperfeiçoamento dos recursos computacionais existentes, utilizando sua máxima capacidade para otimização de custos e aumento de produtividade. Seguindo esse raciocínio, no ambiente de redes de computadores, o gerenciamento é parte fundamental para que o desempenho dessas redes esteja de acordo com o esperado [1].

Para Kurose e Ross [2] o "Gerenciamento de rede inclui a implementação, a integração e a coordenação de elementos de *hardware*, *software* e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, e de elementos, para satisfazer às exigências operacionais, de desempenho e de qualidade de serviço a um custo razoável".

Vale ressaltar que o gerenciamento de redes de computadores está relacionado a gestão de tecnologia da informação, que nos últimos anos tem se tornado peça imprescindível dentro das organizações, deixando de ser apenas ferramenta de apoio e passando a ser parte integrante dos objetivos estratégicos organizacionais [3].

No ponto de vista de ferramentas de gerenciamento, os sistemas de monitoramento vêm se destacando como uma solução para empresas de pequeno, médio e grande porte.

O objetivo desse trabalho é monitorar o tráfego e disponibilidade de serviços em uma rede simulada. Atualmente existem diversas ferramentas com este propósito, sejam elas pagas ou soluções *open source* que monitoram diversos hosts por agente próprio, *Simple Network Management Protocol* (SNMPv2), *Internet Control Message Protocol* (ICMP), dentre outros [4].

Dadas estas afirmações sobre a importância do gerenciamento de redes e a diversidade de plataformas no mercado, qual é a ferramenta gratuita mais eficiente para o monitoramento de redes de computadores em um ambiente simulado?

II. REFERENCIAL TEÓRICO

A. Gerenciamento de Redes

Gerenciamento de rede é o processo de controlar a conectividade e configurações entre dispositivos e seus elementos, visando maximizar sua produtividade e eficiência. A *International Organization for Standardization* (ISO) criou o modelo FCAPS (*fault, configuration, accounting, performance e security*) de acordo com a ISO/IEC 7498-4 de gerenciamento de rede, que apresenta cenários em um quadro mais estruturado. São categorizados em cinco áreas funcionais [3]:

- *Fault Management* (Gerenciamento de Falhas) detecta falhas e determinar a origem, isolando a falha do resto da rede para corrigir eventos que fujam da normalidade;
- *Configuration Management* (Gerenciamento de configuração) permite que um administrador de rede controle e monitore as condições de ambiente da rede, mantém atualizado o inventário com dispositivos e componentes da rede, documentando as alterações de configurações físicas e lógicas da rede.
- *Accounting Management* (Gerenciamento de Contas) permite que o administrador da rede especifique, registre e controle o acesso de usuários e dispositivos aos recursos da rede.
- *Performance Management* (Gerenciamento de Desempenho) simplifica o trabalho do responsável pela rede, fornece ferramentas que permitem monitorar, modificar e controlar o uso de recursos.

- *Secutity Management* (Gerenciamento de Segurança) controla o acesso aos recursos da rede de acordo com as políticas definidas, centrais de distribuição de chaves e as autoridades certificadoras são componentes do gerenciamento de segurança.

Para Kurose e Ross [2] a estrutura de um sistema de gerenciamento de rede é conceitualmente idêntica a uma organização. O campo do gerenciamento possui vários componentes de uma estrutura de gerenciamento de rede, definidos e apresentados na Figura 1:

- Entidade gerenciadora: é o centro da atividade, ela controla a coleta, o processamento, a análise e/ou a apresentação de informações de gerenciamento de rede;
- Dispositivo gerenciado: é um equipamento de rede (incluindo seu *software*) que reside em uma rede gerenciada. Ele corresponde à filial da organização, podendo ser um hospedeiro, um roteador, uma ponte, um hub, uma impressora ou um modem. Em seu interior pode haver diversos objetos gerenciados de *hardware* e *software*;
- Dados: os dados residem em cada dispositivo gerenciado, são conhecidos como "*state*", associados a ele. Os dados de configuração são informações do dispositivo, configuradas explicitamente pelo gerenciador de rede. Dados operacionais são informações que o dispositivo adquire enquanto opera, por exemplo, a lista de imediatos no protocolo. As estatísticas do dispositivo são indicadores de status e contagens que são atualizadas conforme os operadores do dispositivo. O gerenciador de rede pode consultar os dados do dispositivo remoto e em alguns casos, controlar o dispositivo remoto gravando os valores dos dados do dispositivo;
- Agente de gerenciamento de rede: é o processo executado no dispositivo gerenciado, que se comunica com a entidade gerenciadora e que executa ações locais nos dispositivos gerenciados sob o comando e o controle da entidade gerenciadora;
- Protocolo de gerenciamento de rede: é o componente final de uma estrutura de gerenciamento de rede. Esse protocolo é executado entre a entidade gerenciadora e o agente de gerenciamento de rede dos dispositivos gerenciados, o que permite que a entidade gerenciadora investigue o estado dos dispositivos gerenciados e, indiretamente, execute ações sobre eles mediante seus agentes.

B. *Zabbix*

O Zabbix é uma solução *open source* multiplataforma sobre a GPLv2 (Licença Pública Geral GNU v2.0) de monitoramento distribuído. É um software que monitora vários parâmetros de dispositivos de rede, saúde e integridade de servidores, sistemas e aplicações, que oferece integração em todas as aplicações de um sistema de monitoramento, sendo totalmente personalizável a qualquer tipo de ambiente [4].

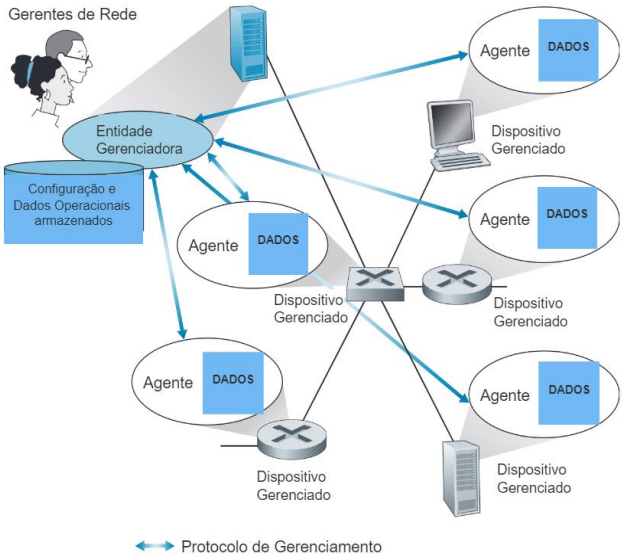

Fig. 1. Modelo de um Sistema de Gerenciamento de Rede. Fonte: Adaptado [2]

O Zabbix possui a capacidade de monitoramento em tempo real, descoberta de host, integração de sistemas, relatórios e alertas personalizados, dentre outras características disponíveis no ambiente web. Com o Zabbix é possível monitorar vários dispositivos em apenas um servidor, além de ser possível ter um monitoramento distribuído, o monitoramento pode ser realizado com ou sem o uso de Agentes. Neste contexto listamos três componentes principais para o monitoramento de redes utilizando Zabbix, sendo eles [5]:

- *Zabbix Server* é o componente central para o qual os Agentes e *Proxies* reportam informações de disponibilidade e integridade e estatísticas, que armazena os dados coletados na base de dados.
- *Zabbix Proxy* é uma parte opcional da implementação do Zabbix em pequenas instalações. O *Zabbix Proxy* é o componente agregador responsável por fazer coleta em clientes remotos, após a coleta, este transmite os dados para o *Zabbix Server.;*
- *Zabbix Agent* é responsável por disponibilizar os dados coletados para o *Zabbix Server.*

Entre os tipos de configurações Zabbix, o protocolo SNMPv2 é utilizado para monitorar dispositivos como impressoras, *switches*, roteadores ou *nobreaks* que, normalmente possuem interfaces SNMPv2 habilitadas e onde não é possível manter um Zabbix Agent em funcionamento.

C. *The Dude*

The Dude é um aplicativo criado pela empresa MikroTik, cujo objetivo é melhorar a maneira como é gerenciado o ambiente de rede. Ele verifica

automaticamente todos os dispositivos em sub-redes especificadas, desenha a topologia básica e traça um mapa de suas redes, monitora os serviços de seus dispositivos e executa ações com base nas alterações de estado do dispositivo conforme programação do administrador de rede, possibilitando uma maior visualização do estado geral da rede [7].

O monitoramento de ativos com o The Dude pode ser feito através do protocolo ICMP por meio de ping, SNMPv2, ou de agentes instalados diretamente nos computadores. Os clientes, além de rodar em Windows, também podem ser instalados em Linux (através do Wine) e no MacOS (através do Darwine). Dentre as principais características e recursos da ferramenta, podemos citar:

- Descoberta de rede e topologias automáticos e dispositivos;
- Suporta monitoramento SNMPv2, ICMP, DNS e TCP;
- Monitoramento e gráficos de uso de link individual;
- Gráfico de serviços mostrando, latência, tempos de resposta de DNS, utilização de banda, informações físicas de links;
- Armazenamento de histórico de eventos (logs) de toda a rede, com momentos de queda, restabelecimentos;
- Acesso direto a ferramentas de controle remoto, para gerenciamento de dispositivos;
- Suporta servidor Dude remoto e cliente local;
- Compatibilidade com ambiente Linux Wine, MacOS Darwine e Windows;

D. Nagios

Originalmente escrito sob o nome Netsaint, o Nagios foi criado por Ethan Galstad. Este software de monitoramento de redes é distribuído livremente, através da lei de *copyleft* Licença Pública Geral (GPL).

O Nagios é um sistema de monitoramento, que permite o monitoramento de toda infraestrutura de TI para garantir que os sistemas, aplicativos, serviços e processos de negócios estão funcionando corretamente. No caso de uma falha, o sistema emite alertas para os responsáveis, permitindo-lhes começar o processo de correção antes que as interrupções afetem os processos de negócios, usuários finais ou clientes.

Indo além das capacidades básicas de monitoramento de TI, o Nagios é um sistema de monitoramento empresarial que fornece as seguintes características: monitoramento abrangente, visibilidade e sensibilização, corretores de problemas, planejamento proativo, relatórios, recursos multi locatários, arquitetura extensível e código personalizável. Com a utilização do Nagios pode-se acompanhar o estado do link, a quantidade de perda de pacotes, a latência, o índice de disponibilidade, dentre outros recursos utilizando de plugins e addons.

E. GNS3

Trata-se de software *open source* utilizado para emular, configurar, testar e solucionar problemas de redes virtuais e reais. O GNS3 permite que sejam executadas topologias compostas por dispositivos como *switches*, *routers*, desktops, servidores, dentre outros equipamentos de rede no ambiente [8].

O GNS3 consiste em dois componentes de software, o GNS3-all-in-one (GUI) e a máquina virtual GNS3 (VM). Na interface gráfica do usuário (GUI) são implementadas as topologias de redes para simulação, quando se cria topologias no GNS3 utilizando o cliente GUI, os dispositivos criados precisam ser hospedados e executados por um processo de servidor. Tendo-se três opções para a parte do servidor do software. Sendo elas, o servidor GNS3 local, VM local GNS3 e VM GNS3 remota.

O servidor GNS3 é executado localmente no mesmo desktop em que foi instalado o software multifuncional GNS3. Utilizando um desktop *Windows*, tanto a GUI do GNS3 quanto o servidor GNS3 local estão sendo executados como processos no *Windows*. Processos adicionais, como o *Dynamips*, também serão executados no desktop. Para a execução da VM GNS3 é necessário um software de virtualização como VMware Workstation, Virtualbox ou Hyper-V, pode-se executar a VM GNS3 remotamente em um servidor usando VMware ESXi ou em nuvem. [8].

III. METODOLOGIA

A pesquisa foi embasada nos fundamentos de redes de computadores, onde os conceitos utilizados são os de protocolos e serviços de redes, e dentro dos mesmos será focado no protocolo simples de gerenciamento de redes ou SNMPv2 utilizado para monitoramento de serviços e equipamentos dentro de uma rede interna de computadores.

Os instrumentos utilizados para a coleta de dados serão os programas Zabbix, The Dude e Nagios e o recolhimento dos dados será realizado a partir das funções disponíveis para cada plataforma e armazenados em um banco de dados mysql.

A topologia estrela representada na Figura 2 foi utilizada como ambiente de teste simulado, composta por: uma conexão à rede externa e um hub para distribuição de internet, 8 máquinas virtuais, importadas do VirtualBox, dentre estas, 3 máquinas individuais com softwares de monitoramento e 5 máquinas com Linux Debian para os testes.

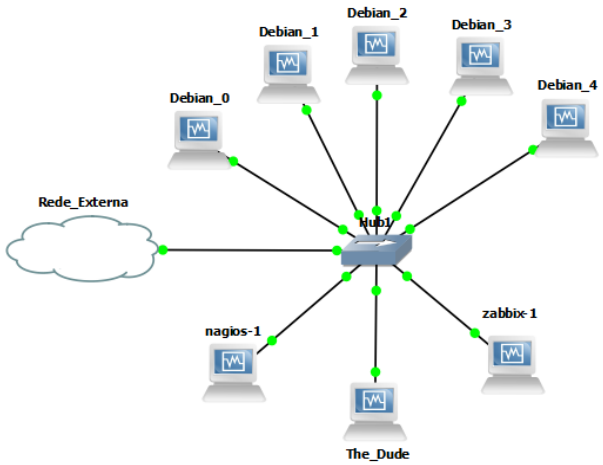

Fig. 2. Ambiente de teste utilizando topologia Estrela.

As plataformas realizaram o monitoramento e análise conforme o comportamento da rede simulada, coletando os dados das máquinas monitoradas e armazenando em um banco de dados MySQL e SQLite. Os dados de monitoramento são consultados no ambiente web de cada ferramenta gerando visualização gráfica para análise de tráfego, ping, latência e jitter.

IV. Conclusão

Realizado a implementação da topologia e testes de comunicação entre as máquinas, foi gerado os gráficos do monitoramento dos dispositivos utilizando os softwares Zabbix, The Dude e Nagios, para obtenção de dados conforme as Figuras 3 e 4.

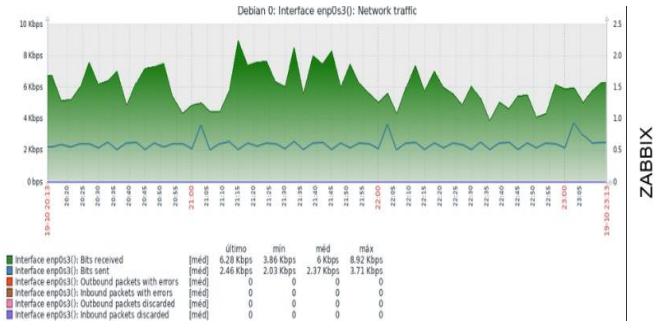

Fig. 3. Gráficos gerados em tempo real, durante o monitoramento da máquina Debian-0.

Após a conclusão dos testes, será elaborada uma tabela de comparação de eficiência nos processos de instalação, configuração, visualização de gráficos, alertas e funcionalidades das ferramentas.

Fig. 4. Gráficos gerados em tempo real, durante o monitoramento da máquina Debian-0.

Como trabalhos futuros, será implementado o monitoramento de redes em um ambiente real, onde será executado a coleta de dados durante processos, como a de transferência de arquivos entre computadores via protocolos FTP e por meio de arquitetura P2P, os dados e os softwares serão analisados.

Referências

[1] DE SOUZA, D. C.; SOARES, J. A.; DA SILVA, F. R. *Gerenciamento de redes de computadores*. 1. ed. Porto Alegre: SAGAH, 2021.

[2] KUROSE, J.; ROSS, K. *Redes de computadores e a Internet.* 8. ed. Porto Alegre: Bookman, 2021.

[3] KUROSE, J.; ROSS, K. Computer networking: A top-down approach: International edition. 6. ed. [s.l.] Pearson Education, 2013.

[4] MELO, J. D. DE et al. GERENCIAMENTO DE REDES UTILIZANDO ZABBIX. Em: *Ciência da Computação: tecnologias emergentes em computação - Volume 2*. [s.l.] Editora Científica Digital, 2021. p. 86–94.

[5] DOS REIS LIMA, J. *Monitoramento com Zabbix*. 2. ed. Rio de Janeiro: BRASPORT, 2020.

[6] *Manual do Zabbix*. Disponível em: <https://www.zabbix.com/documentation/6.0/pt/manual>. Acesso em: 15 set. 2022.

[7] MIKROTIK. Manual: The Dude. 2017. Disponível em: https://wiki.mikrotik.com/wiki/Manual:The_Dude. Acesso em: 2 jun. 2022.

[8] Getting Started with GNS3. Disponível em: <https://docs.gns3.com/docs/>. Acesso em: 20 out. 2022.