UNIVERSIDADE FEDERAL DE SANTA MARIA
COLÉGIO TÉCNICO INDUSTRIAL DE SANTA MARIA
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

ANÁLISE DE FERRAMENTAS DE GERÊNCIA DE REDES E INTERFACES WEB

TRABALHO DE CONCLUSÃO DE CURSO

Alex Henrique Scapin

Santa Maria, RS, Brasil
2015

ANÁLISE DE FERRAMENTAS DE GERÊNCIA DE REDES E INTERFACES WEB

Alex Henrique Scapin

Trabalho de Conclusão de Curso (TCC) apresentado ao Curso Superior de Tecnologia em Redes de Computadores, Área de concentração em Segurança da Informação da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Tecnólogo em Redes de Computadores**

Orientador: Prof. Me. Renato Preigschadt de Azevedo

Santa Maria, RS, Brasil
2015

Colégio Técnico Industrial de Santa Maria
Curso Superior de Tecnologia em Redes de Computadores
Universidade Federal de Santa Maria

A Comissão Examinadora, abaixo assinada,
aprova a Monografia

ANÁLISE DE FERRAMENTAS DE GERÊNCIA DE REDES E INTERFACES WEB

elaborada por
Alex Henrique Scapin

Como requisito parcial para obtenção de grau de
Tecnólogo em Redes de Computadores

COMISSÃO EXAMINADORA

Renato Preigschadt de Azevedo, Me.
(Presidente/Orientador)

Simone Regina Ceolin, Dra. (UFSM)

Tarcísio Ceolin Junior, Me. (UFSM)

Santa Maria, 06 de julho de 2015.

AGRADECIMENTOS

Agradeço primeiramente aos meus pais Ivania L. G. Scapin e Valderi P. Scapin por todo o apoio e confiança depositados em mim, à minha namorada Daniela B. Kemmerich por estar todos os dias ao meu lado, incentivando e ajudando a passar pelos desafios ao longo desta jornada.

Agradeço ao meu sogro Marcos O. Kemmerich e sogra Dircemara B. Kemmerich, por estarem sempre presentes, assim como meu irmão Lucas A. Scapin e cunhada Patrícia Hatschbach.

Agradeço ao professor Renato Preigschadt de Azevedo, meu orientador, por toda ajuda, instruções e orientações a mim prestadas no decorrer deste trabalho de conclusão; aos demais professores, agradeço pelo companheirismo, paciência e ensinamentos compartilhados ao decorrer do curso.

Agradeço também aos amigos e colegas pela amizade e parceria, por estarem sempre dispostos a ajudar e principalmente, pelos momentos descontraídos ao longo desses anos de estudo.

RESUMO

Trabalho de Conclusão de Curso
Colégio Técnico Industrial de Santa Maria
Curso Superior de Tecnologia em Redes de Computadores
Universidade Federal de Santa Maria

ANÁLISE DE FERRAMENTAS DE GERÊNCIA DE REDES E INTERFACES WEB

AUTOR: Alex Henrique Scapin
ORIENTADOR: Me. Renato Preigschadt de Azevedo
Data e Local da Defesa: Santa Maria, 13 de julho de 2015

A utilização da internet e os serviços providos pelas redes de computadores estão evoluindo de forma significativa, sendo necessário garantir o funcionamento e a disponibilidade dos serviços prestados a maior parte de tempo, e ao menor custo possível. Neste cenário surge o gerenciamento e monitoramento de redes, que busca manter o funcionamento correto dos ativos que compõem a estrutura da rede, através da coleta e análise dos dados referentes ao status dos dispositivos gerenciados. O ato de monitorar pode expor estatísticas detalhadas sobre o funcionamento dos dispositivos, gerando alertas com base em dados históricos sobre os eventos que fujam da normalidade a fim de corrigi-los antes de se tornarem um problema real a toda estrutura da rede. Este trabalho apresenta um estudo sobre algumas destas ferramentas responsáveis por mostrar de forma clara e eficaz, as informações valiosas acerca do funcionamento dos ativos pertencentes à rede de computadores. Serão abordadas questões referentes à instalação e configuração das ferramentas Zabbix, Nagios e MRTG, as funcionalidades e usabilidade das interfaces *Web*, tecnologias e linguagens de programação empregadas para gerar os gráficos assim como a capacidade de gerar alertas.

Palavras-chave: ferramentas; monitoramento; gerenciamento; estatísticas; funcionamento; redes de computadores.

ABSTRACT

Completion Of Course Work
Colégio Técnico Industrial de Santa Maria
Curso Superior de Tecnologia em Redes de Computadores
Universidade Federal de Santa Maria

ANALYSIS OF NETWORK MANAGEMENT TOOLS AND WEB INTERFACES

AUTHOR: Alex Henrique Scapin
SUPERVISOR: Msc. Renato Preigschadt de Azevedo
Date and Place of Defense: Santa Maria, july 13, 2015

The use of the Internet and the services provided by computer networks are evolving significantly, it is necessary to ensure the functioning and availability of services and the increased use of these technologies , so does the need to ensure the network to function properly and that the service is available most of the time, and the lowest possible cost. In this scenario arises the management and monitoring of networks, which seeks to maintain proper operation of the assets that make up the network structure, by collecting and analyzing data on the status of managed devices. The act of monitoring exposes detailed statistics on the operation of the devices, generating alerts based on historical data about the events that escape normal in order to correct them before they become a real problem to the whole structure of the network. This paper presents a study of some of these tools, which are responsible for showing clearly and effectively, the valuable information on the operation of the assets belonging to the computer network. They will address issues relating to the installation and configuration of Zabbix tools, Nagios and MRTG, the functionality and usability of Web interfaces, technologies and programming languages used to generate the graphics and the ability to generate alerts.

Keywords: tools; monitoring; management; statistics; operation; computer network.

LISTA DE TABELAS

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

SNMP	*Simple Network Management Protocol*
IETF	*Internet Engineering Task Force*
RFC	*Request for Comments*
OSI	*Open Systems Connection*
SMI	*Structure of Management Information*
IP	*Internet Protocol*
UDP	*User Datagram Protocol*
NMS	*Network Management Systems*
MIB	*Management Information Base*
CPU	*Central Processing Unit*
CGI	*Common Gateway Interface*
GPL	*General Public License*
MRTG	*Multi Router Traffic Grapher*
SMS	*Short Message Service*

LISTA DE ANEXOS E APÊNDICES

SUMÁRIO

1 INTRODUÇÃO

Pode-se definir gerenciamento de redes de computadores como a análise de todos os recursos materiais e/ou lógicos presentes na constituição da rede física de uma organização (Pinheiro, 2002). Neste contexto, o ato de gerenciar tem como principal objetivo, manter uma análise constante sobre tudo o que está acontecendo nos equipamentos que compõe a rede, a fim de gerar informações de grande valia para os responsáveis pelo seu funcionamento. Estas informações podem ser úteis tanto para a prevenção, como para a detecção e resolução de problemas que possam acabar com a disponibilidade da rede, e que por muitas vezes, acabará livrando a empresa ou instituição, de quem sabe, sofrer um duro golpe financeiro devido a falhas oriundas do mal funcionamento da rede.

Conexão à internet e utilização de computadores deixaram de ser sinônimo de poder aquisitivo a muitos anos, onde a grande maioria ao menos tinha ideia de o que poderia ser feito com o uso de tais tecnologias. Hoje, basta olhar ao redor para ter certeza de que a realidade é completamente diferente, pois a internet faz parte do cotidiano das pessoas, está presente tanto em suas casas, como no trabalho e no processo de educação, assim como na grande maioria das empresas, que sem este recurso, muitas delas jamais existiriam.

Partindo em uma visão paralela ao uso, chegamos a um ponto crucial, os recursos necessários para manter o serviço em pleno funcionamento. Devido ao crescimento desenfreado, se faz extremamente necessário o investimento em novas tecnologias, equipamentos, políticas e regras de procedimentos.

Atualmente, a grande maioria das empresas que necessitam de disponibilidade e confiabilidade de serviços vem adotando a utilização de ferramentas de gerenciamento e monitoramento, a fim de facilitar desde a avaliação de informações resultantes da análise diária dos equipamentos, até a correção de problemas antes mesmo deles acontecerem através da identificação prévia de riscos.

> Ter um ambiente mapeado e monitorado é fundamental para o processo de crescimento de uma empresa, já está mais do que comprovado que um ambiente de T.I bem planejado tem mais chances de dar certo, mesmo para as empresas em que o principal foco seja T.I, pois todos dependem hoje da internet e dos serviços que ela disponibiliza. (COSTA, 2008, p.Introdução)

A organização deste trabalho está segmentada em Capítulos. O Capítulo 2 apresenta informações básicas para auxiliar o entendimento do conteúdo discutido. O Capítulo 3 expõe os trabalhos relacionados, servindo como base para a realização deste estudo. No Capítulo 4 é realizado um estudo sobre as ferramentas de gerência e monitoramento de redes MRTG, Nagios e Zabbix tendo ênfase na *interface Web* e a forma em que as mesmas exibem as informações graficamente. O Capítulo 5 traz um estudo comparativo referente a configuração, funcionalidades, metodologia e linguagem utilizada para a criação/atualização de gráficos destas ferramentas a fim de propor melhorias.

Por fim, no Capítulo 6 serão expostos os resultados desta análise, relacionando com o objetivo principal, que é discutir uma forma de tornar a prática de gerência e monitoramento de redes mais versátil aos profissionais responsáveis por esta tarefa. Serão citados ainda algumas sugestões para trabalhos futuros.

1.1 Objetivos gerais

Obter conhecimentos sobre gerência e monitoramento de rede, bem como a importância de utilizar ferramentas que simplificam o trabalho do administrador e ao mesmo tempo, permitem que questões voltadas à disponibilidade e funcionamento da rede seja atingida ao manter o controle sobre o funcionamento dos dispositivos a compõe. Ainda, pretende-se compreender a estrutura das ferramentas de monitoramento e a forma que estas geram os gráficos com base nas informações coletadas dos ativos da rede.

1.2 Objetivos específicos

Após o entendimento sobre assuntos referentes ao monitoramento e funcionamento das ferramentas, pretende-se instalar e configurar algumas destes *softwares* a fim de explorar suas principais características e funcionalidades. Para o desenvolvimento futuro de uma aplicação *Web*, que tenha como principal objetivo a projeção dos resultados e gráficos de

monitoramento de forma diferenciada, com o auxílio de tecnologias mais recentes, será realizada uma análise comparativa entre as interfaces *Web* dessas ferramentas, seguindo os seguintes tópicos:

- As configurações necessárias para que estas ferramentas possam exibir os gráficos de monitoramento;

- As funcionalidades e usabilidade das interfaces *Web*;

- As características das ferramentas sobre o tipo de tecnologia e linguagens de programação utilizadas para gerar os gráficos;

- A capacidade de interagir com o administrador da rede através dos alertas, através de diferentes meios de comunicação.

2 REVISÃO BIBLIOGRÁFICA

Neste capítulo são apresentados conceitos básicos presentes na elaboração deste trabalho, a fim de possibilitar um melhor entendimento sobre os assuntos abordados.

2.1 Gerenciamento de redes

Segundo Saito e Madeira (2001, p.1) "O gerenciamento de rede pode ser visto como um conjunto de mecanismos operacionais e administrativos necessários para controlar os recursos da rede, manter os recursos da rede operacionais, facilitar o aumento da rede, gerenciar os recursos e controlar o acesso à rede".

Para Kurose e Ross (2010, p.553) "Gerenciamento de rede inclui a disponibilização, 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 em tempo real a um custo razoável".

O gerenciamento da rede permite ao administrador, responsável pelo seu funcionamento, ter uma visão detalhada e precisa do que está acontecendo em tempo real nos ativos presentes na topologia da rede, onde é possível detectar precocemente algum evento que esteja fugindo da rotina e que possa causar prejuízos no futuro. Permite adoção de ações preventivas ao invés de apenas corretivas, ou seja, possibilita corrigir os erros antes de que se agravem e prejudiquem a qualidade da rede.

> O objetivo da Gerência de Redes é monitorar e controlar os elementos da rede (sejam eles físicos ou lógicos), assegurando um certo nível de qualidade de serviço. Para realizar esta tarefa, os gerentes de redes são geralmente auxiliados por um sistema de gerência de redes. Um sistema de gerência de rede pode ser definido como uma coleção de ferramentas integradas para a monitoração e controle da rede. Este sistema oferece uma interface única, com informações sobre a rede e pode oferecer também um conjunto poderoso e amigável de comandos que são usados para executar quase todas as tarefas da gerência da rede.
> (Stallings, 1998 citado por SUAVE; LOPES; NICOLLETTI, 2003).

Para garantir que a rede ofereça qualidade e disponibilidade de serviços aos usuários, é necessário que esta seja gerenciada, independente do seu tamanho. Contudo, quanto maior e mais dispositivos existirem, maior é a dificuldade para realizar a gerência de forma manual, e através da utilização de ferramentas é possível diminuir essa complexidade, tornando mais fácil a visualização dos resultados obtidos através da análise dos equipamentos ativos da rede.

Com base nesta evolução e o desenvolvimento do modelo OSI (*Open Systems Connection*) foram definidas as áreas funcionais do gerenciamento, sendo conhecida como modelo FCAPS, constituído basicamente por cinco gerências, que são:

• *Faults* (Gerencia de Falhas) – tem a habilidade de detectar a falha e determinar a origem, isolar a falha do resto da rede e corrigir eventos que fujam da normalidade, prevenindo que aconteça o mal funcionamento do sistema.

• *Configuration* (Gerência de Configuração) – controla e monitora condições de ambiente da rede, mantém atualizado o inventário com dispositivos e componentes da rede, mantém documentadas as alterações de configurações físicas e lógicas da rede e permite a adaptação de funcionalidades para clientes em particulares (provisionamento).

• *Accounting* (Gerência de Contabilidade) – possibilita a medição dos custos de uso da rede, ou seja, pode-se cobrar por serviços utilizados além de permitir o crescimento da rede e detectar abusos no uso dos recursos.

• *Performance* (Gerência de Desempenho) – simplifica o trabalho do responsável pela rede, fornece ferramentas que permitem monitorar, modificar e controlar o uso de recursos. Assegura a capacidade de tráfego mínimo na rede.

• *Secutity* (Gerência de Segurança) – refere-se à questão de autenticação e autorização de usuários, a fim de manter a segurança de informações e integridade dos dados.

2.2 Protocolo SNMP *(Simple Network Management Protocol)*

Protocolo SNMP é um tipo de protocolo da camada de aplicação com o objetivo principal de facilitar a troca de informações entre os dispositivos gerenciados, é o protocolo mais utilizado no paradigma de gerenciamento e monitoramento de redes. Foi reconhecida como padrão de fato no final dos anos 80, e evoluído posteriormente para as versões SNMPv1, SNMPv2 até chegar à versão mais recente SNMPv3.

A versão SNMPv1 é definida basicamente em três padrões da IETF (*Internet Engineering Task Force*), sendo elas as RFCs (*Request for Comments*): RFC1155[1], RFC1212[2] e RFC1157[3]. Onde a primeira define o SMI (*Structure of Management Information*), que nada mais é do que os mecanismos usados para definir e nomear os objetos que serão gerenciados, e a segunda, na verdade é apenas uma melhoria no mecanismo de descrição do SMI existente. A terceira RFC é propriamente a que define o protocolo SMNP.

Esta versão inicial do SNMP baseava-se em "*community strings*", ou seja, *strings* e *passwords* em texto aberto, um problema sério relacionado à segurança dos dispositivos da rede, acessados facilmente através dessa *string*.

O SNMPv2 composto pelas RFCs: RFC1905[4], RFC1906[5] e 1907[6] surgiu com status experimental, procurando resolver algumas deficiências da versão anterior. Nesta versão foram melhoradas as questões referente à segurança, adição de novas operações e funcionalidades, como por exemplo, a adição da função que permite gerenciar e configurar servidores remotamente via SNMP.

A versão mais recente do protocolo é a SNMPv3, composta pelas RFCs: RFC1905, RFC1906, RFC1907, RFC2570[7], RFC2571[8], RFC2572[9], RFC2573[10], RFC2574[11] e RFC2575[12]. Esta versão buscou melhorar ainda, falhas de segurança presente nas versões anteriores, implementando funções de controle de acesso, autorização, autenticação e privacidade, e buscou ainda inserir uma forma de modelo administrativo para nomeação das entidades, gerenciamento de chaves, notificações dos destinos, relacionamento de *proxy* e para a configuração remota através de operadores SNMP.

SNMPv3 utiliza o protocolo UDP (*User Datagram Protocol*) para realizar a comunicação entre as NMS (*Network Management Systems*) e os dispositivos gerenciados. O SNMP é responsável por produzir informações como status do funcionamento da rede,

---

[1] RFC 1155 - http://datatracker.ietf.org/doc/rfc1155/
[2] RFC 1212 - https://datatracker.ietf.org/doc/rfc1212/
[3] RFC 1157 - https://datatracker.ietf.org/doc/rfc1157/
[4] RFC 1905 - https://datatracker.ietf.org/doc/rfc1905/
[5] RFC 1906 - https://datatracker.ietf.org/doc/rfc1906/
[6] RFC 1907 - https://datatracker.ietf.org/doc/rfc1907/
[7] RFC 2570 - https://datatracker.ietf.org/doc/rfc2570/
[8] RFC 2571 - https://datatracker.ietf.org/doc/rfc2571/
[9] RFC 2572 - https://datatracker.ietf.org/doc/rfc2572/
[10] RFC 2573 - https://datatracker.ietf.org/doc/rfc2573/
[11] RFC 2574 - https://datatracker.ietf.org/doc/rfc2574/
[12] RFC 2575 - https://datatracker.ietf.org/doc/rfc2575/

utilização de memória, quantidade de processamento, porcentagem de utilização do disco rígido, e várias outras opções, com base na troca de mensagens entre gerentes e agentes.

Segundo Black (2008, p.21), o protocolo SNMP possui cinco tipos de mensagens utilizadas para a troca de informações entre os gerentes e agentes, sendo eles:

• *get-request-PDU* - mensagem enviada pelo gerente ao agente solicitando o valor de uma variável;

• *get-next-request-PDU* - mensagem utilizada pelo gerente para solicitar o valor da próxima variável depois de uma ou mais variáveis que foram especificadas;

• *set-request-PDU* - mensagem enviada pelo agente ao gerente para solicitar que seja alterado o valor de uma variável;

• *get-response-PDU* - mensagem enviada pelo agente ao gerente, informando o valor de uma variável que lhe foi solicitado;

• *trap-PDU* - mensagem enviada pelo agente ao gerente, informando um evento ocorrido;

Em uma rede gerenciada com a utilização do protocolo SNMP pode-se determinar a existência de três componentes principais, onde:

• Dispositivos gerenciados - são nós presentes na estrutura da rede gerenciada contendo um agente SNMP, tem a função de coletar e armazenar informações a fim de serem utilizadas pelas NMSs. Podem ser qualquer elemento da rede, como por exemplo, roteadores, *switches*, *hubs*, computadores clientes, entre outros.

• Agentes - módulos de *software* que armazenam informações sobre os dispositivos gerenciados em MIBs (*Management Information Base*). Informações, como por exemplo, utilização de memória, quantidade de processamento, entre outros.

• NMS - os sistemas de gestão de redes são responsáveis pelo monitoramento e controle dos dispositivos gerenciados. Trazem opções de visualizar graficamente as informações coletadas e armazenadas nas MIBs.

Na Figura 1 é possível ver a disposição dos três componentes do protocolo SNMP da seguinte forma: a máquina que possui o agente (NMS) está ligado ao dispositivo gerenciado, que possui o agente, e este é o responsável por criar os objetos contendo estatísticas sobre o funcionamento deste dispositivo dentro da MIB.

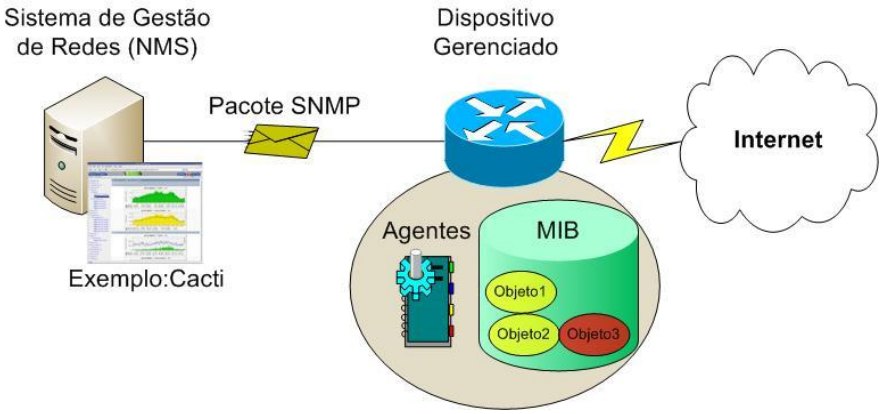

Figura 1 - Arquitetura de rede gerenciada por meio de SNMP
Fonte: http://www.ti-redes.com/gerenciamento/snmp/intro/

2.3 MIB *(Management Information Base)*

Conforme a Figura 1, uma MIB é uma estrutura de armazenamento presente nos dispositivos gerenciados, semelhante a um banco de dados onde são armazenadas as informações coletadas através dos agentes. Quando o agente gera informações sobre o *status* de operação de um dispositivo gerenciado utilizando o protocolo SNMP, é criado então, um objeto dentro da MIB com os dados coletados para compartilhar estas informações com o módulo gerente presentes nos Sistemas de Gestão de Redes. Estas informações são utilizadas pelas NMS, e com base nestes dados, são gerados os gráficos e informações dos dispositivos exibidos na *interface Web*.

2.4 Virtualização ou Máquinas virtuais

Conforme Ciriaco (2008), máquina virtual é o termo associado a uma máquina instalada através da utilização de um programa, executando as mesmas funções que uma máquina real, conforme a Figura 2.

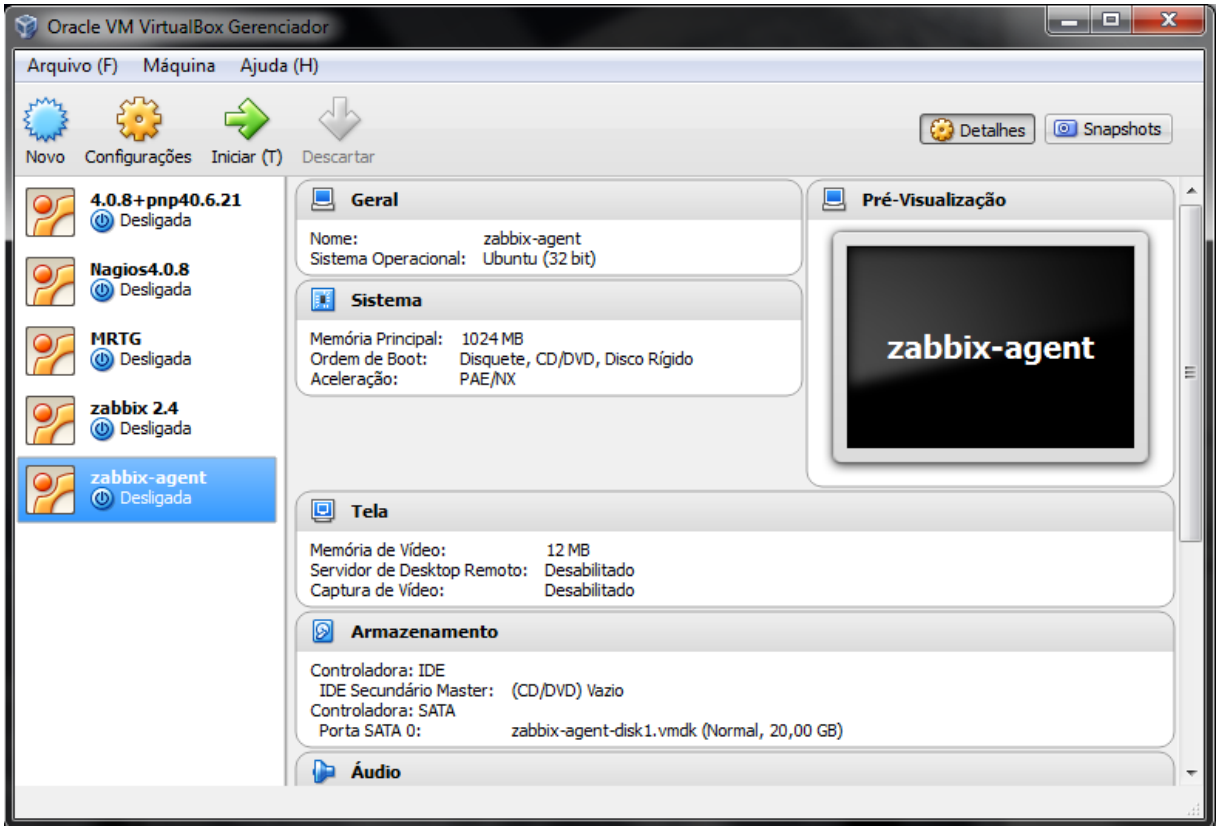

Figura 2 - Software VirtualBox e máquinas virtuais criadas.
Fonte: Acervo pessoal.

A figura 2 ilustra a interface do *software* Oracle VM VirtualBox, responsável por gerenciar as máquinas virtuais. Ainda nesta figura, é possível perceber que existem cinco máquinas virtuais criadas, assim como informações de cada uma delas e opções referentes às configurações destas maquinas e configurações do *software* em si.

A virtualização é utilizada atualmente em várias áreas, desde uso particular para realização de testes ou trabalhos, até o uso em empresas e universidades. Com sua utilização, é possível a utilizar diversos sistemas operacionais a partir de uma máquina real com um sistema operacional próprio, sem interferência alguma.

Com base na importância da utilização de maquinas virtuais, pode-se salientar algumas das características positivas de seu uso:

• Melhor aproveitamento de recursos provenientes da infraestrutura existente - permite executar vários servidores ou conjunto de máquinas ao mesmo tempo.

• Menor estrutura física (parque de máquinas) - devido ao fato de poder ter várias máquinas virtuais em um único computador, gerando economia de *hardware*, espaço e inclusive custos com resfriamento e manutenção de salas de máquinas.

• Uso de sistemas legados - permite o uso de máquinas com *software* e *hardware* ultrapassados/limitados, necessitando apenas de uma máquina virtual compatível com os requisitos de ambiente.

• Migração e ampliação mais fácil - maior rapidez na tarefa de mudar o serviço de ambiente e ampliar a infraestrutura.

• Multiplataformas – possibilita a utilização de plataformas variadas, utilizada geralmente para realização de testes de desempenho com a utilização dos mesmos *softwares*, com sistemas operacionais diferente.

• Ambiente de testes – pode ser utilizado para realização de testes, utilizando *softwares* e configurações sem correr o risco de danificar o sistema operacional da máquina real.

• Segurança e confiabilidade – tudo o que acontece em uma máquina não afeta as demais, por serem independentes. Permite que se tenha dois servidores idênticos (clones), por exemplo, possibilitando que um segundo entre em funcionamento assim que o primeiro falhar.

3 TRABALHOS RELACIONADOS

Este trabalho apresenta um estudo na área de gerencia de redes, tendo como ênfase a parte visual e usual de interfaces referentes a ferramentas responsáveis pelo monitoramento e gerenciamento de redes de computadores. Dando suporte a esta pesquisa, foram analisados alguns trabalhos com temas propostos na mesma área de estudo.

Black (2008) propõe um estudo sobre ferramentas de gerenciamento e monitoramento com base no crescimento constante de redes de computadores de todos os portes, assim como o crescente número destas ferramentas, cuja função é auxiliar na tarefa de coleta de informações sobre o funcionamento, prevenção e correção de falhas. Neste trabalho, é feita uma análise entre nove ferramentas, sendo elas, o CACTI, ZENOSS, ManageOP Engine, BigBrother4, Spice Works, Look@LAN, Zabbix, Nagios e um *front-end* baseado em RRD. Importante salientar, que o autor não possui intenção de apontar o melhor s*oftware*, e sim apoiar e incentivar o uso destas ferramentas no âmbito de gerência de redes.

Proposta semelhante é feita por Majewski (2009) e Braga (2011), onde ambos realizam um estudo comparativo entre as ferramentas Nagios, Cacti e Zabbix, com objetivo também, de apontar funcionalidades, pontos positivos e negativos, sem a intenção de apontar qual delas é a melhor ferramenta.

Em comum, entre o presente trabalho e os citados anteriormente nesta seção, está a intenção de apoiar e incentivar a utilização de ferramentas de gerenciamento e monitoramento de redes, devido a necessidade de um serviço que ofereça qualidade e disponibilidade para suprir a demanda imposta pelo cenário atual. Porém, este trabalho dará mais ênfase em questões de usabilidade e funcionalidades presentes na *interface Web* das ferramentas MRTG, Nagios e Zabbix, a fim de comparar as mesmas destacando pontos importantes sobre o funcionamento e questões ligadas a forma de gerar os gráficos de monitoramento.

4 TRABALHO PROPOSTO

Nesta etapa será descrita a proposta desse trabalho, que se baseia em um estudo sobre ferramentas que servem de apoio aos responsáveis pelo funcionamento correto da rede, a fim de diminuir o esforço empregado no monitoramento e na correção de falhas dando ênfase na análise da capacidade de expor os resultados graficamente através das interfaces *Web*. Este estudo servirá de base para a elaboração de um método que busque a agilidade e versatilidade na tarefa de gerência em tempo real, facilitando o controle sobre o funcionamento da rede.

Com base nesta necessidade de controlar o funcionamento dos componentes em uma rede de computadores, oriunda do aumento da utilização de dispositivos, tanto em ambientes escolares, domésticos ou em empresas de todos os portes, surgem *softwares* cuja principal funcionalidade é auxiliar na análise das estatísticas de seu funcionamento. Existem diversas ferramentas, entre estas existem *softwares* proprietários e *softwares* livres, disponíveis para auxiliar na tarefa de gerência e monitoramento de uma rede.

Dentre estes *softwares* existem inúmeras opções, podendo citar como exemplo: o MRTG, RRDtool, CACTI, Nagios, Zabbix, ZenOSS, BigBrother4, Pandora FMS, PRTG, Spiceworks, entre muitas outras. Neste trabalho, porém, serão estudadas apenas três destas ferramentas, sendo as seguintes: MRTG, que segundo BLACK (2008, p.30) teve seus conceitos utilizados como base para o desenvolvimento de outras ferramentas. O Zabbix que segundo sites e fóruns especializados em monitoramento de redes vem ganhando bastante espaço no ambiente de gerência e monitoramento, e por fim, o Nagios que é uma ferramenta muito utilizada por oferecer diversos *plug-ins*, e permitir que os mesmos possam ser modificados para melhor atender as necessidades do profissional e da rede monitorada.

4.1 MRTG (*Multi Router Traffic Grapher*)

A ferramenta MRTG foi desenvolvido por Tobias Oetiker no ano de 1994, com o objetivo de monitorar o tráfego em um *link* de internet gerando gráficos para facilitar a visualização dos resultados. É distribuída sob a licença GNU GPL (*General Public License*) e funciona na maioria dos sistemas Unix/Linux, Windows e servidores *NetWare*, servindo de

parâmetro para o desenvolvimento de várias outras ferramentas de monitoramento que se utilizaram dos conceitos do MRTG, evoluindo em muitos aspectos as suas funcionalidades.

Inicialmente desenvolvido em Perl e utilizando o protocolo SNMP, mostrou-se uma ferramenta muito lenta, e foi então com o interesse e ajuda de Dave Rand que teve a velocidade de execução aumentada de forma drástica através da reescrita de partes críticas do MRTG utilizando a linguagem C. Após esta melhoria, Tobias Oetiker distribuiu várias cópias do *software* e em troca conseguiu muitos *feedbacks* de usuários sobre correções de erros e *bugs*.

Além do monitoramento de tráfego de rede, foram desenvolvidas novas funcionalidades a fim de manter estatísticas sobre monitoramento de utilização da CPU, memória, número de usuários, basicamente qualquer informação do sistema que possa ser extraída através da utilização de *shell script*.

4.2 Nagios

O Nagios é uma ferramenta de monitoramento de redes *open-source* distribuída sob licença GNU GPLv2, criado por Ethan Galstad para rodar inicialmente sob a plataforma Linux, apesar de ser executado na maioria dos sistemas baseados em UNIX. Permite a coleta de informações sobre os serviços, servidores impressoras e demais ativos de rede a fim de gerar estatísticas e dados importantes sobre o funcionamento da rede.

Esta ferramenta possui uma grande comunidade de desenvolvedores ao redor do planeta que participa do seu desenvolvimento. Pode ser considerada um *software* de gerenciamento devido ao grande número de *plug-ins* disponibilizados pela comunidade, onde também são disponibilizados vários tutoriais de desenvolvimento de *plug-ins* a fim de incentivar os usuários a desenvolver novas funcionalidades à ferramenta.

Estes *plug-ins* disponibilizados na comunidade Nagios são desenvolvidos utilizando diversas linguagens de programação, como por exemplo, C, Pearl, PHP e C#. A utilização destes, possibilita aos administradores de rede terem serviços adicionais, necessários conforme for a necessidade de cada empresa ou gerente de redes.

Esta ferramenta funciona basicamente nos seguintes sistemas operacionais: Unix/Linux o módulo Gerente e Agente, no Windows através do *software* NagWin (apenas o módulo agente) e no Mac OS/X (apenas modulo agente).

O Nagios, assim como o Zabbix, possui versões diferentes de ferramentas onde o Nagios Core é uma ferramenta gratuita e o Nagios XI é uma solução de monitoramento empresarial desenvolvido pela *Nagios Enterprises*. A principal diferença entre estas ferramentas não está relacionada às funcionalidades exclusivamente, mas sim, ligado diretamente à usabilidade e interação com o administrador no ato da gerência.

Para melhor entendimento à questão da usabilidade, existe um comparativo entre o Nagios e o mecanismo de pesquisa do Google, onde o Nagios Core é relacionado ao algoritmo de busca utilizado, e o Nagios XI é relacionado à *webpage* do Google.com. Com base neste comparativo, pode-se perceber claramente que o Nagios Core possui características de ser menos amigável na realização da gerência e monitoramento, em relação à versão comercial.

Para que se possa perceber a diferença entre configurar novos serviços utilizando Nagios Core (Figura 3) e a interface oferecida para a configuração de novos serviços e dispositivos no Nagios XI (Figura 4), basta analisar as ilustrações referente ao comparativo destas versões quando pretende-se configurar um novo serviço.

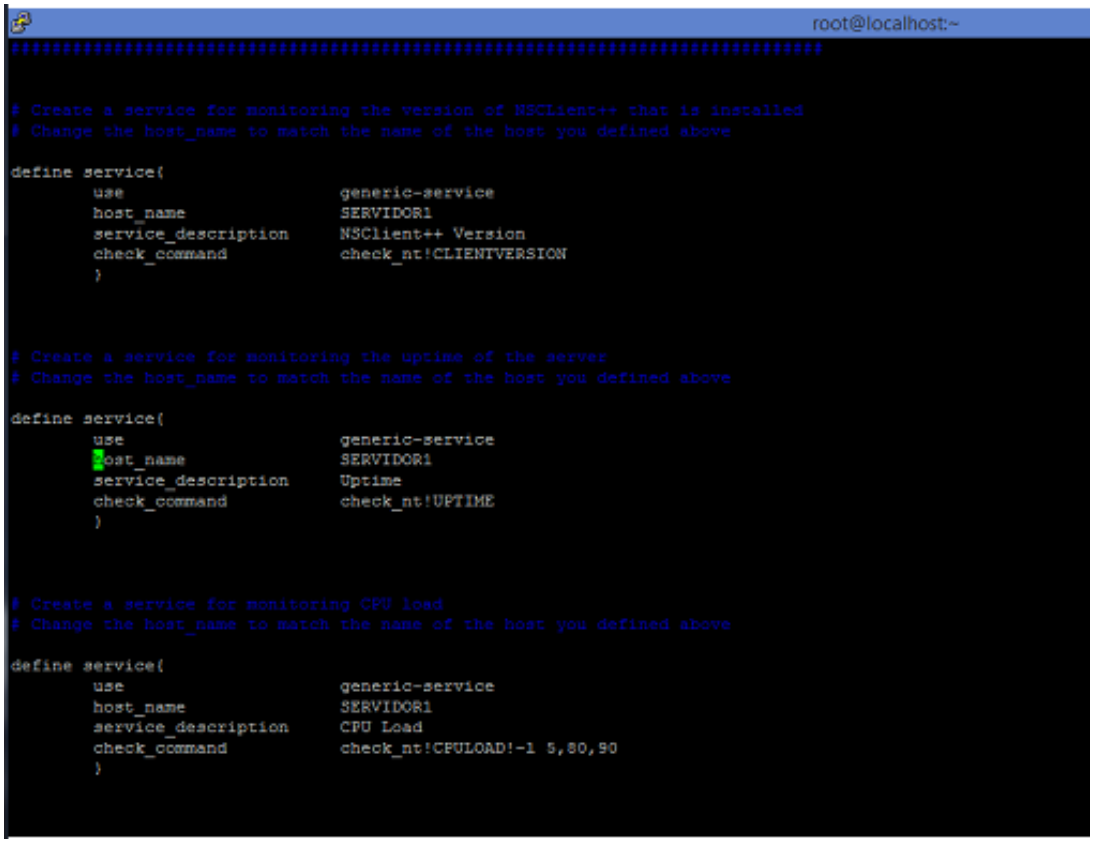

Figura 3 - Definindo novos serviços Nagios Core.
Fonte: http://nagios-br.com/diferencas-entre-o-nagios-core-e-o-xi-free-e-paga

A Figura 3 mostra a organização do arquivo de configurações de novos serviços de monitoramento no Nagios Core, o qual não oferece de forma gratuita a interface gráfica para adição de forma mais simples e rápida. Se comparar a imagem anterior com a Figura 4, é possível perceber a diferença em relação à usabilidade de utilizar as versões gratuita e comercial.

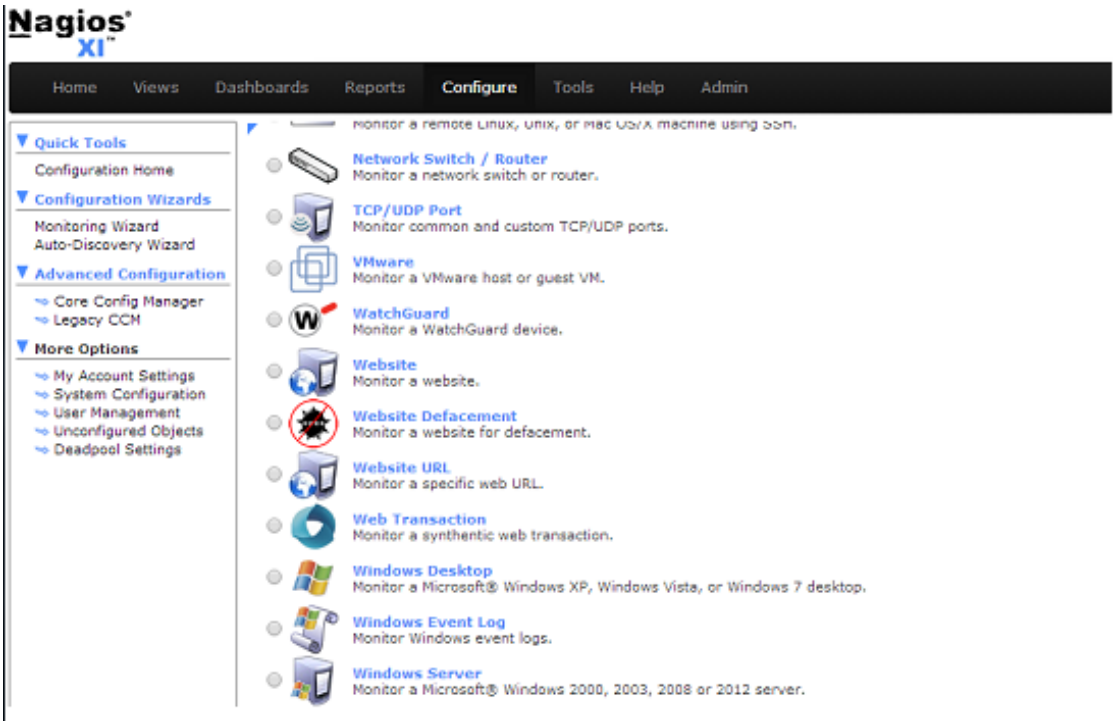

Figura 4 - Interface para definir novos serviços no Nagios XI.
Fonte: http://nagios-br.com/diferencas-entre-o-nagios-core-e-o-xi-free-e-paga

Nagios na sua versão paga, ilustrada na Figura 4, é determinado um *software SMART*, onde isto significa uma abreviação das seguintes características:

• Simplificado – oferece interfaces para novas configurações, praticamente extingue a edição em arquivos;

• Management (gerenciamento) – mais funcionalidades e recursos ao gerenciamento de *hosts* e serviços;

• Avançado – além de monitorar a rede, oferece uma solução de monitoramento de fácil entendimento, permitindo ao administrador da rede a compreensão do que está sendo executado;

• Recurso – projetado para poupar recursos, e auxiliar no planejamento de capacidade de *hardware*, ou seja, avalia a utilização de CPU (*Central Processing Unit*), disco e memória e informa quando é necessário realizar melhorias na capacidade do *hardware*;

• Tempo – monitora a rede com maior eficiência e oferece uma interface gráfica intuitiva.

4.3 Zabbix

Criado por Alexei Vladishev e mantido atualmente pela Zabbix SAI, o Zabbix é um *software open-source* de gerenciamento de redes de computadores distribuído sob a licença GNU GPLv2 para monitoramento de performance de dispositivos. Com ele é possível monitorar sistemas operacionais, tanto clientes como servidores, ativos de rede (*switch, access points*, roteadores, entre outros), impressoras, enfim, é capaz de monitorar qualquer equipamento que possua IP (*Internet Protocol*).

Cabe salientar, que existem suportes técnicos de dois tipos, sendo um gratuito, disponibilizado na página oficial do Zabbix ou através de fóruns, e o suporte comercial, que é subdividido em níveis (*Bronze, Silver, Gold, Platinum* e *Enterprise*). Vale ressaltar que o *software* é o mesmo, diferindo apenas pelo fato de que o suporte comercial implica na disponibilidade de acompanhamento por profissionais especializados para solucionar problemas da ferramenta, entre outras vantagens que pode-se ver na Figura 5:

	Bronze	Silver	Gold	Platinum	Enterprise
Number of incidents	4	8	Unlimited	Unlimited	Unlimited
Number of authorized support contacts	1	1	2	3	5+
Support availability times (h-d)	8 x 5	8 x 5	8 x 5	24 x 7	24 x 7
Guaranteed response times *	2 Days	1 Day	4 Hours	4 Hours	4 Hours
Online case submission	✔	✔	✔	✔	✔
Phone technical support		✔	✔	✔	✔
Standard Zabbix builds		✔	✔	✔	✔
Remote Troubleshooting			✔	✔	✔
Distributed monitoring with Zabbix Proxy			✔	✔	Unlimited
Emergency response within 90 minutes				✔	✔
Performance Tuning				✔	✔
Pre-compiled software according to customer request				✔	✔
Assigned primary support contact					✔
On-site visit **					✔
On-site professional training ***					✔
Upgrade to the latest version by Zabbix					✔
Environment Reviews					✔
Custom Zabbix builds					✔
Sponsored development priority					✔

Figura 5 - Quadro comparativo dos níveis de suporte comercial.
Fonte: http://www.zabbix.com/support.php

Na Figura 5, pôde-se perceber que os benefícios oferecidos pelo suporte comercial variam conforme o valor ou nível do suporte.

A ferramenta Zabbix é composta por quatro componentes, que são: *Zabbix server*, *Zabbix agent, Zabbix Proxy e Interface Web*. Dentre estes, a utilização do *Zabbix proxy* fica opcional ao administrador da rede.

4.3.1 Zabbix server

Zabbix server é o componente central da estrutura do Zabbix, é responsável por armazenar todas as configurações, estatísticas, dados operacionais, calcular *triggers* e enviar notificações aos usuários informando sobre ativos que necessitam de algum tratamento de exceções. Todas as informações geradas pelos agentes são reportadas ao *Zabbix server*, como por exemplo, disponibilidade, integridade de informações e estatísticas de servidores.

Devido à natureza de missão crítica de seu funcionamento, o servidor Zabbix precisa cumprir alguns requisitos de segurança, e desta forma, apenas o sistema operacional UNIX e seus derivados cumprem de forma eficaz a questão de desempenho, resiliência e tolerância a falhas do qual é necessário para prover estatísticas confiáveis. O *Zabbix server* foi testado em diversas plataformas, tendo suporte oficial para as seguintes: Linux, Solaris, AIX, HP-UX, Mac OS/X, FreeBSD, OpenBSD, NetBSD, SCO Open Server e Tru64/OSF1.

4.3.2 Zabbix agent

O agente Zabbix é o responsável por reunir informações operacionais do sistema e enviar estes dados para o *Zabbix server* realizar o processamento. Informações sobre recursos e aplicações locais, como por exemplo, estatísticas de espaço livre em discos rígidos, ocupação de memória, processamento, tráfego da rede são alguns dos dados coletados e enviados ao servidor.

Figura 6 - Relação entre Servidor e Agente Zabbix.
Fonte: http://zabbixbrasil.org/files/Tutorial_de_instalacao_do_agente_Zabbix.pdf

Conforme a Figura 6, o agente presente no dispositivo gerenciado reúne informações sobre o funcionamento do equipamento e quando solicitado pelo servidor, envia estas

informações para que sejam geradas informações estatísticas sobre a operação. Caso esses dados coletados pelo agente sejam dados que fujam da normalidade, o servidor dispara alertas para informar o administrador da rede sobre o ocorrido.

O agente deve ser instalado no dispositivo que se deseja monitorar. Existem dois tipos de verificações do agente Zabbix, sendo elas:

Verificação passiva – quando o servidor ou o *proxy* solicita informações e o usuário responde com o resultado do teste requisitado.

Verificação ativa – neste caso é necessário que o agente receba uma lista com informações solicitadas pelo servidor ou *proxy* dos itens a monitorar, e um intervalo de tempo para realizar a coleta dos dados. Esta verificação necessita de maior processamento devido ao grau de complexidade, podendo coletar informações até mesmo se o servidor não estiver disponível e enviando assim que houver disponibilidade.

O *Zabbix agent* é suportado pelas seguintes plataformas: Linux, IBM AIX, FreeBSD, NetBSD, OpenBSD, HP-UX, Mac OS/X, Solaris: 9, 10, 11 e Windows: 2000, Server 2003, XP, Vista, Server 2008, 7.

4.3.3 Zabbix proxy

O *Zabbix proxy* fica encarregado em nome do *Zabbix server* de coletar informações sobre o desempenho e disponibilidade dos dispositivos monitorados, posteriormente sendo enviados ao servidor. Pode ser útil quando se pretende diminuir a carga sofrida pelo servidor, tendo assim, a coleta realizada por um ou mais *proxies* restando ao componente central apenas o processamento destas informações.

Este componente necessita de um banco de dados para armazenar as informações coletadas, desta forma, os que possuem suporte são: MySQL, PostgreSQL e SQLite. Importante salientar, como citado na seção 4.1.1, este componente é opcional e varia conforme as necessidades e preferência do responsável pelo gerenciamento da rede.

4.3.4 Interface Web

A *interface Web* faz parte do *Zabbix server* e é responsável por permitir que sejam acessadas as informações de monitoramento e configuração de forma mais prática, independentemente da plataforma e lugar de onde está ocorrendo o acesso.

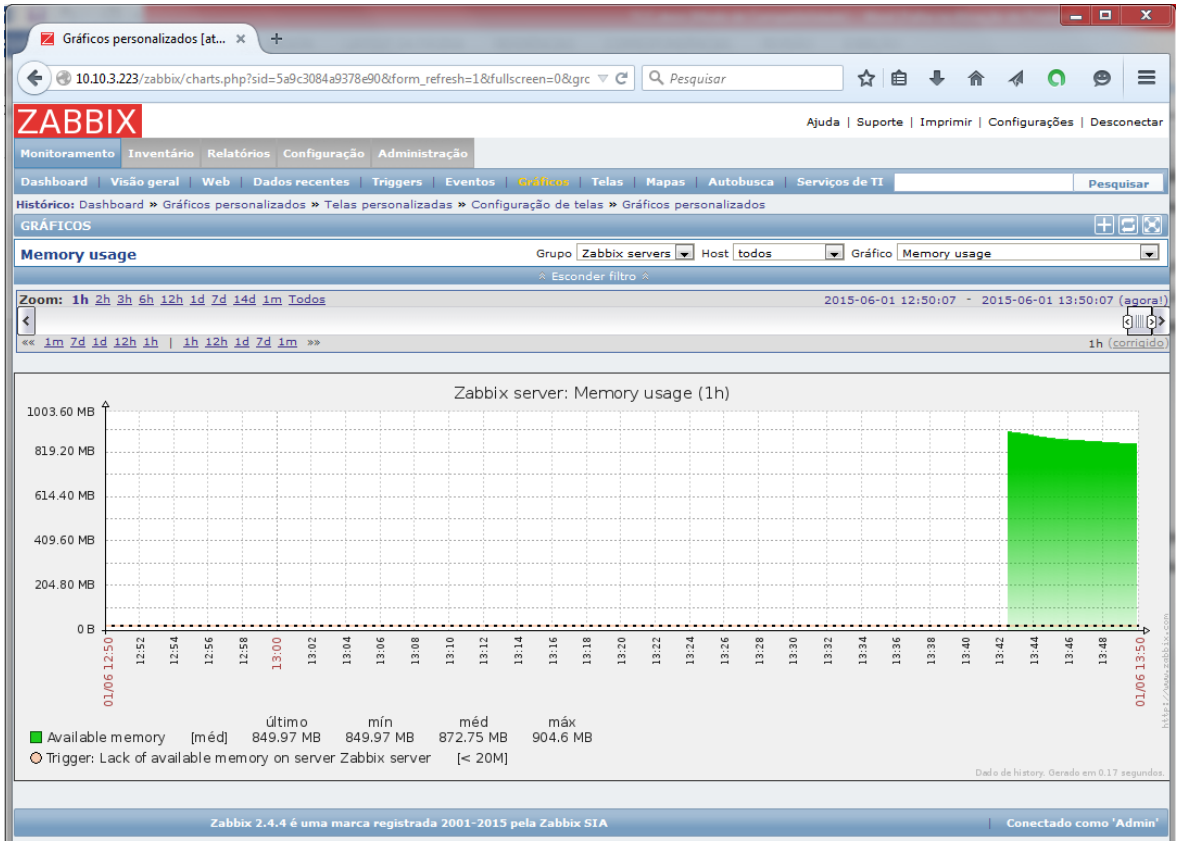

Figura 7 - Interface Web do Zabbix.
Fonte: Acervo pessoal

A Figura 7 ilustra a *Interface Web* do Zabbix, possuindo várias funcionalidades e opções no menu horizontal. Nesta imagem, está selecionado o gráfico referente à utilização de memória em relação ao tempo de execução pelo *Zabbix server* que neste caso, é o nome da máquina virtual que está configurado o módulo servidor do Zabbix.

5 ANÁLISE COMPARATIVA DAS FERRAMENTAS

Seguindo o objetivo a ser alcançado por este estudo, serão realizadas análises das ferramentas MRTG, Nagios e Zabbix desde a configuração dos serviços de gerenciamento e monitoramento, até uma análise mais aprofundada, levando em consideração a forma de tratamento dos dados coletados através dos agentes, assim como a utilização destas informações pelo gerente para geração de gráficos e estatísticas através da *interface Web*. Para a realização desta análise, foram separados alguns assuntos em forma de tópicos a fim de manter uma melhor apresentação dos resultados obtidos, sendo organizados da seguinte forma:

- Configuração das ferramentas para exibição dos gráficos de monitoramento;
- Funcionalidades e usabilidade das interfaces *Web* de gerência;
- Características das ferramentas referentes as tecnologias e linguagens de programação empregadas para gerar os gráficos;
- Capacidade de manipular as ferramentas para que se adequem às necessidades do gerente da rede e do funcionamento da mesma.

5.1 Configuração das ferramentas para exibição dos gráficos de monitoramento

Essa etapa do trabalho busca expor os passos que o administrador da rede necessita realizar até que as ferramentas estudadas consigam trazer as informações sobre a rede em si, assim como as informações sobre o funcionamento dos dispositivos que compõem a rede através dos módulos agentes e gerentes, de forma mais intuitiva através da geração dos gráficos e da geração de alertas para notificação sobre a ocorrência de eventos que fujam da normalidade. Através dos tutoriais e informações presentes nos fóruns e sites relacionados às ferramentas, é possível realizar a configuração das três ferramentas, onde o esforço empregado vai depender diretamente da base de conhecimento de quem está realizando estas configurações.

As ferramentas foram instaladas e configuradas em máquinas virtuais, através do *software* VirtualBox 4.3.26, foram utilizadas máquinas independentes para as três ferramentas

analisadas. A configuração destas maquinas e versões do MRTG, Nagios e Zabbix são as seguintes:

- Sistema operacional: Ubuntu server 14.04.2 LTS i386;
- Memória: 1024 MB;
- Disco rígido: 20 GB;
- MRTG 2.17.4;
- Nagios 4.0.8 + pnp4nagios 0.6.21;
- Zabbix 2.4.

O MRTG possui uma *interface Web* que exibe os gráficos oriundos do monitoramento de forma nativa, necessitando basicamente a alteração de dois arquivos, onde um se refere a própria configuração do MRTG e outro é a criação de um *Alias* para o diretório /var/www/mrtg na configuração do Apache (configurações disponíveis no item 8.3 do apêndice). O objetivo inicial do desenvolvimento desta ferramenta era monitorar um *link* de internet, e por isso necessita que sejam adicionados *scripts* para o MRTG realizar o monitoramento e gráficos referentes a outros serviços, como por exemplo, uso de memória, CPU e espaço de disco ocupado.

O Nagios por sua vez, como citado anteriormente na seção 3.2, é uma ferramenta que possui um grande número de *plug-ins* que permitem adicionar inúmeras funcionalidades além da função de gerência e monitoramento possibilitados pela instalação do pacote de instalação inicial. O Nagios inicialmente não permite a visualização de gráficos referentes às estatísticas geradas pelo monitoramento dos ativos da rede, possibilita apenas informações e estatísticas em “modo texto” grifados em cores diferenciadas indicando o status dos serviços onde: verde (*OK*), amarelo (*Warning*), laranja (*Unknown*), vermelho (*Critical*) e cinza (*Pending*), conforme a Figura 8.

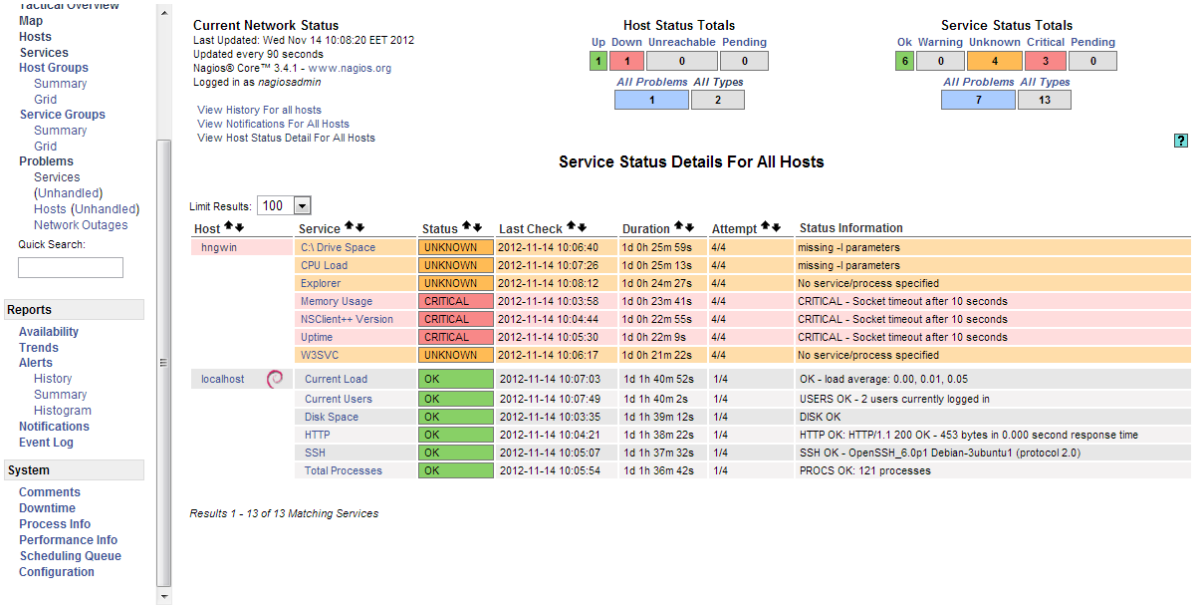

Figura 8 - Status de serviços Nagios Core
Fonte: https://awaseroot.wordpress.com/2012/11/23/monitoring-windows-with-nagios/

Para gerar estatísticas graficamente, foi utilizado o plug-in PNP4Nagios 0.6.21, que necessita do *download*, instalação e configurações adicionais em alguns arquivos do Nagios para que a ferramenta possa utilizar este *plug-in* através do seu arquivo de configuração (configurações disponíveis no item 8.2 do apêndice).

A ferramenta Zabbix, assim como o MRTG, já traz incluída na *interface Web* os gráficos gerados através das estatísticas e informações coletadas através do *Zabbix Agent*. Necessita a alteração de apenas dois arquivos, onde um encontra-se no *Zabbix server* referente a configuração da *Timezone* (fuso horário), e outro é a alteração de um arquivo no *Zabbix agent* para inclusão do IP do servidor e o nome do cliente (configurações disponíveis no item 8.1 do apêndice). Para que os gráficos sejam mostrados na página *Web*, necessita ainda o cadastro do ativo a ser monitorado através do IP e nome deste dispositivo.

5.2 Funcionalidades e usabilidade das interfaces *Web* de gerência

Neste item será analisada a facilidade com que o usuário destas ferramentas consegue visualizar as informações referentes aos dispositivos gerenciados, assim como a capacidade

de navegar entre as opções trazidas por estas interfaces. Primeiramente serão visualizadas informações e características do MRTG, do Nagios e após do Zabbix.

5.2.1 MRTG

A ferramenta MRTG não oferece nenhuma funcionalidade ao administrador da rede, a não ser a visualização dos gráficos gerados a partir das informações extraídas dos dispositivos gerenciados e os alertas via *e-mail*. Por ser uma das pioneiras no cenário de gerência e monitoramento, onde o criador tinha como objetivo apenas exibir graficamente as informações referentes ao tráfego da rede, houve apenas adição de novos módulos de monitoração, ou seja, passou a ser capaz de gerar gráficos sobre utilização de memória, processador, entre outros. Tanto para adição desses módulos como qualquer alteração nas configurações, é necessário que sejam feitas alterações diretamente nos arquivos de configurações da ferramenta.

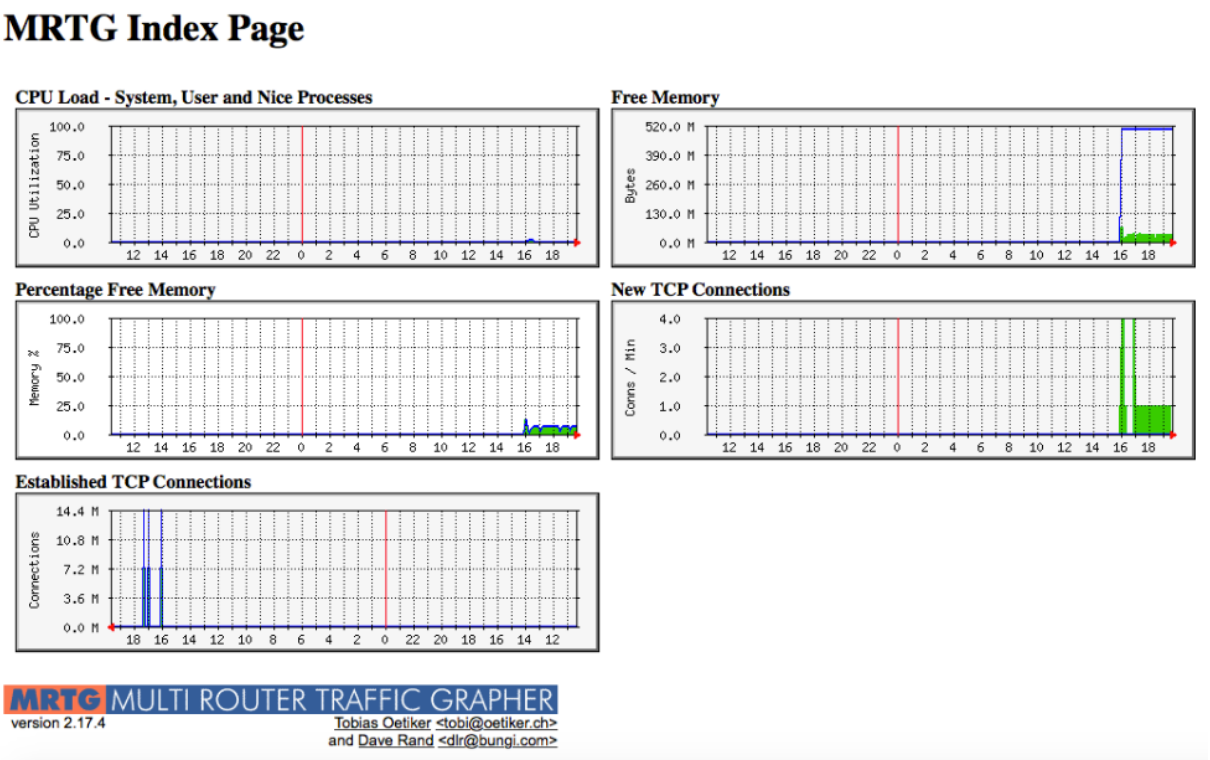

Figura 9 - Interface Web MRTG
Fonte: Acervo pessoal

Como foi possível perceber na Figura 9, a *interface Web* do MRTG foi desenvolvida apenas para exibir os gráficos referentes ao monitoramento, não possuindo funcionalidades adicionais em sua interface. Por outro lado, o Zabbix e o Nagios apresentam uma interface bastante amigável e repleta de funcionalidades interessantes, a diferença está em pequenos detalhes, como por exemplo, apenas o Zabbix oferece a opção de adicionar os ativos a serem monitorados através da *interface Web*, não necessitando alterar arquivos manualmente.

5.2.2 Nagios

Ao analisar a interface do Nagios, apesar exibir apenas informações textuais, pode-se perceber que ela é bastante amigável, onde, através do menu lateral pode-se visualizar informações de forma tática ilustrada na Figura 10, ou seja, esta aba permite visualizar a situação atual contendo várias informações em uma única tela. Esta aba traz informações sobre interrupções no funcionamento da rede, o status de funcionamento dos *hosts* (*Down, Unreachable, Up* e *Pending*), o status dos serviços em funcionamento nos *hosts*, além de informações sobre os recursos de monitoramento. Ainda possibilita a visualização destes itens separadamente através dos itens: *Map, Hosts, Services, Host Groups, Service Groups e Problems*.

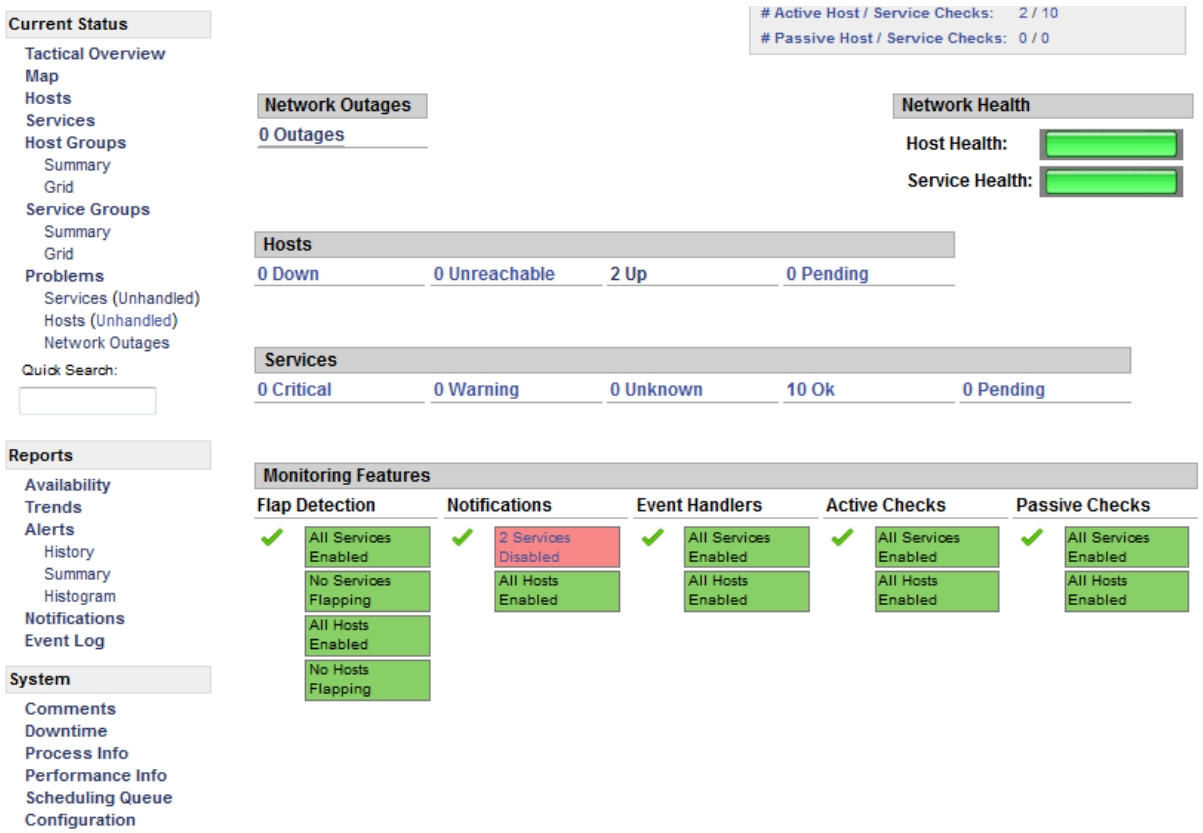

Figura 10 - Tactical Overview Nagios.
Fonte: Acervo pessoal

Ainda presente no menu lateral, conforme a Figura 10, é possível visualizar através da criação relatórios, informações sobre a disponibilidade (serviços, *hosts*, grupo de serviços ou grupo de *hosts*), informações sobre alertas, configuração de notificações (*e-mail*, SMS (*Short Message Service*), entre outros) além de um registro de eventos contendo informações sobre sua execução. Na mesma página ainda é possível a criação de comentários sobre os *hosts* e serviços, informações sobre os processos e performance, fila de agendamentos que permite ativar e desativar checagem de serviços dos *hosts* e por fim, um item que permite modificar as configurações referentes aos *hosts*, serviços, grupos de *hosts*, grupos de serviços, períodos de tempo e comandos utilizados para obter as informações dos dispositivos gerenciados.

A *interface Web* do *plug-in* PNP4Nagios permite visualizar as informações de forma graficamente, oferecendo ainda opções diferenciadas no detalhamento dos gráficos. Na parte referente as ações, é possível determinar um intervalo de tempo especifico para que apenas neste intervalo sejam exibidas as informações graficamente, permite ainda exportar relatórios para os formatos PDF e XML contendo os gráficos e informações referentes ao

monitoramento, permite a visualização de estatísticas sobre o funcionamento do próprio PNP4Nagios.

O *plug-in* oferece ainda a opção de selecionar o intervalo de tempo desejado para visualização das estatísticas de forma gráfica, sendo estes intervalos: visão global (abrange todos os intervalos), 4 horas, 25 horas, uma semana, um mês ou um ano, podendo ser customizadas variando conforme a necessidade do administrador da rede. Ainda possibilita visualizar todas as informações coletadas sobre um dispositivo (utilização de memória, processador, número de processos, entre outros) ou a visualização de cada informação individualmente. A Figura 11 ilustra a interface do *plug-in* PNP4Nagios:

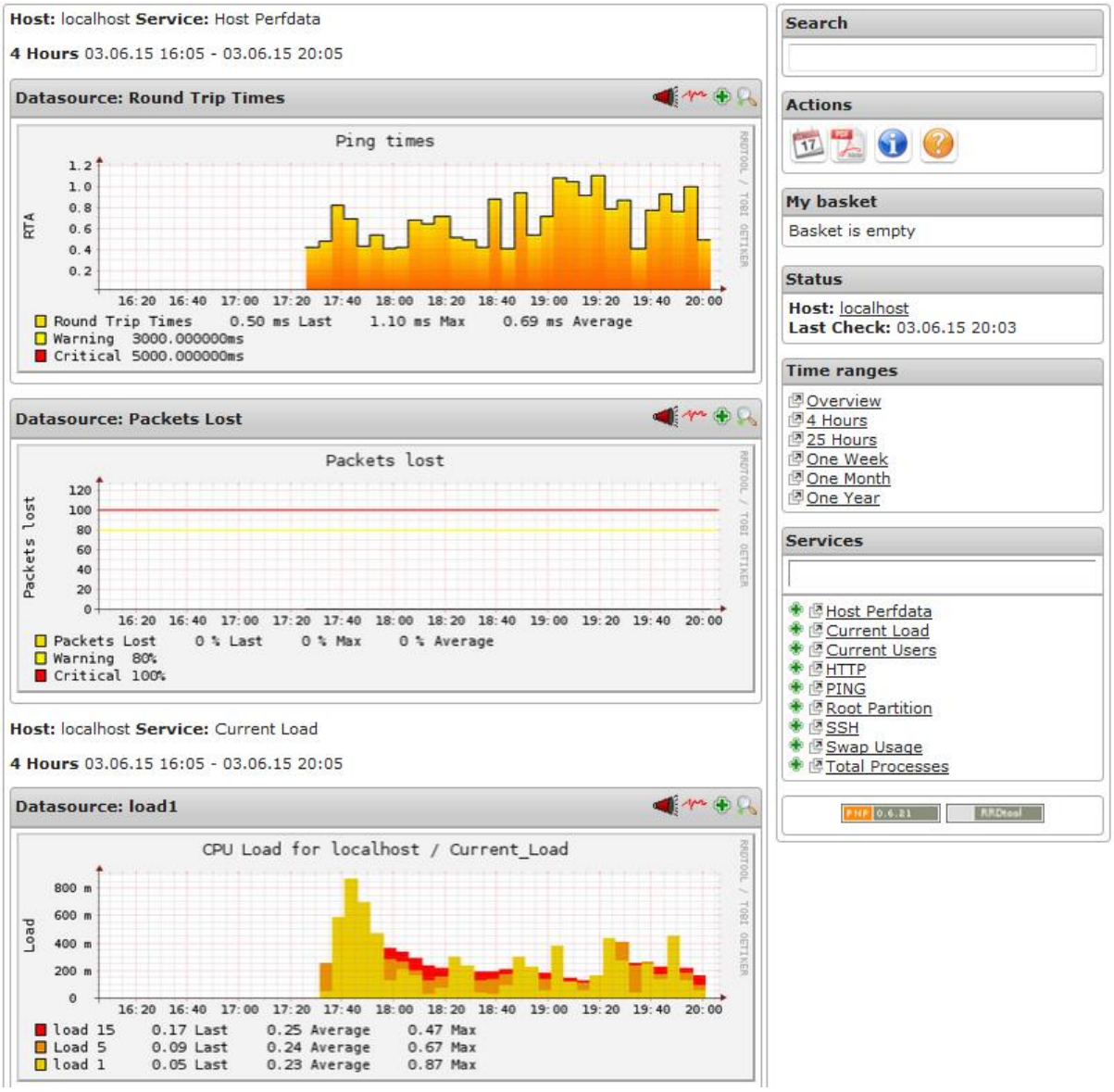

Figura 11 - PNP4Nagios interface Web.
Fonte: Acervo pessoal

5.2.3 Zabbix

A *interface Web* gerada pela ferramenta Zabbix traz inúmeras funcionalidades, sendo também muito fácil de utilizá-la.

A primeira tela após o login é referente a seção de monitoramento, mais exatamente a aba *Dashboard* conforme a Figura 12, onde são mostradas as informações sobre o funcionamento da própria ferramenta, status sobre os *hosts*, grupos de *hosts*, últimos 20 incidentes ocorridos nos dispositivos gerenciados e o número de dispositivos online e desconectados presentes na rede, enfim, um resumo com informações importantes ao administrador. Ainda na seção de monitoramento, é possível ter uma visão geral de grupos de *hosts* e estatísticas sobre os serviços que estão sendo analisados, ainda traz informações como: dados recentes, *triggers*, eventos, mapa da rede local, busca automática de *hosts*, além de gráficos e telas onde pode-se ver os gráficos referentes as estatísticas de monitoramento.

Figura 12 - Página inicial do Zabbix.
Fonte: Acervo pessoal

Na seção Inventário, é possível visualizar informações gerais sobre o inventário dos *hosts*, ou informações detalhadas dos dispositivos monitorados. Na seção Relatórios, é possível gerar relatórios sobre o funcionamento geral do Zabbix, relatórios de disponibilidade

de serviços em monitorados, *triggers* mais utilizadas e relatórios contendo os gráficos selecionados referentes aos dispositivos da rede.

O Zabbix possibilita também a configuração de grupos de *hosts*, *templates*, *hosts*, ações (criação de *triggers*), possibilita alterar a tela de gráficos que é exibida em formato de matriz (linhas X colunas), configuração de mapas e de descoberta automática, tudo isso com nível de dificuldade muito baixo. A figura 13 ilustra a tela de configurações de novos *hosts* a serem monitorados.

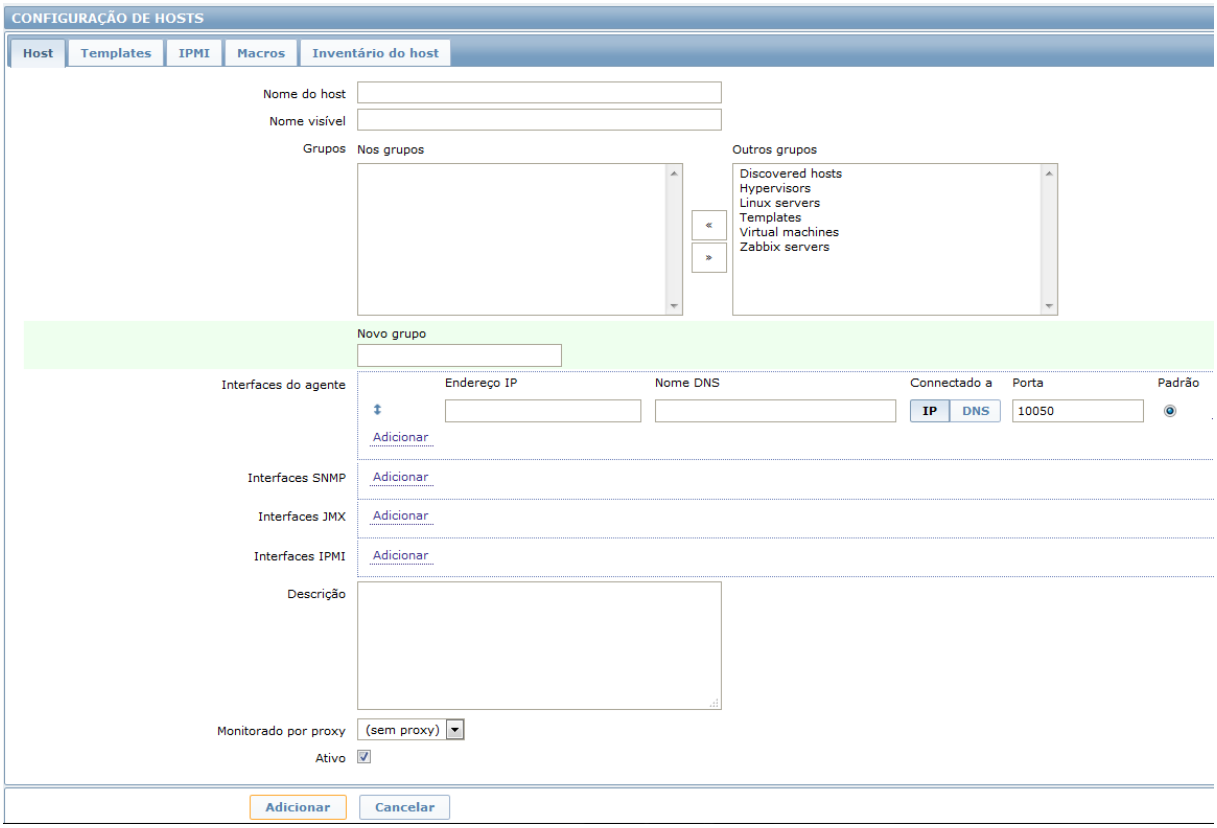

Figura 13 - Tela para adição de novos dispositivos.
Fonte: Acervo pessoal

Na figura 13 é possível adicionar um novo *host* contendo o mínimo de informações sobre o dispositivo, por exemplo, basta ir até a aba *Hosts*, selecionar a opção de criar *host*, informar basicamente o nome do cliente, IP e selecionar um grupo para o mesmo.

Na seção referente à administração, é possível alterar a cor da interface, o tipo de autenticação interna, grupos de usuários, tipos de mídias para envio de alertas, notificações e um guia para a instalação da interface *Web*.

5.3 Características das ferramentas referentes as tecnologias e linguagens de programação empregadas para gerar os gráficos

Para gerar as imagens, todas as ferramentas utilizam a biblioteca *GD Library*, criada por Thomas Boutell, que é uma biblioteca de código-fonte aberto utilizada para gerar imagens dinâmicas. Esta biblioteca pode ser utilizada em várias linguagens de programação, como linguagem C, Perl, PHP, Python, e é capaz de gerar imagens nos formatos PNG, JPEG, GIF, entre outras.

O Nagios, assim como o MRTG utilizam a biblioteca GD em conjunto com a tecnologia CGI (*Common Gateway Interface*), que é responsável por gerar páginas dinâmicas e permitir que um navegador passe parâmetros para um programa alojado em um servidor *Web*. Cabe ressaltar que CGI não é uma linguagem de programação, e sim uma tecnologia associada originalmente à linguagem Perl e depois difundida entre as outras linguagens de programação como PHP, Python, Ruby e ASP.NET.

A ferramenta Zabbix, diferente do Nagios e MRTG, não utiliza propriamente a tecnologia CGI para gerar os gráficos de forma dinâmica, e sim funções escritas na linguagem PHP, juntamente com a biblioteca PHP GD.

5.4 Capacidade de gerar alertas através de diferentes meios de comunicação

A capacidade de gerar alertas é uma das funcionalidades mais importantes presente nestas ferramentas de gerência e monitoramento, isso pelo simples fato de que nem sempre existirá alguém dedicando seu tempo e atenção exclusivamente a ficar analisando os gráficos e estatísticas dos dispositivos que compõem a rede. Pensando nisso, usuários vem desenvolvendo sempre novas configurações de alertas, compartilhando com os membros de comunidades e fóruns voltados ao âmbito de gerência.

Dentre as ferramentas analisadas neste estudo, é possível destacar que o MRTG é a ferramenta que apresenta menos funcionalidades e tipos de alertas, permitindo basicamente envio de alertas através de *e-mail*. Já as ferramentas Nagios e Zabbix possuem comunidades de usuários e colaboradores mais ativas, possuindo mais opções.

O Nagios e o Zabbix possuem as opções de configurar alertas sonoros, alertas via *e-mail*, através de mensagens SMS, através do aplicativo *Yowsup* que é uma tecnologia mais recente desenvolvida utilizando a linguagem Python, funcionando como uma interface em linha de comando capaz de interagir com o *WhatsAPP* necessitando apenas de um número/chip exclusivo para a realização desta função. A ferramenta Zabbix possui ainda a opção de enviar alertas via *Gtalk*.

5.5 Resultados

Através da análise comparativa entre as ferramentas MRTG, Nagios e Zabbix foi possível a obtenção de resultados referentes às funcionalidades e características da *interface Web* de cada uma, no qual os resultados obtidos estão contidos na Tabela 1.

Tabela 1 - Tabela de comparação entre interfaces Web das ferramentas.

	MRTG	**Nagios**	**Zabbix**
Interface Web	Sim	Sim	Sim
Gráficos	Sim	Através de *plug-in*	Sim
Funcionalidades presentes na *interface Web*	Poucas	Múltiplas	Múltiplas
Linguagem de programação utilizada para o desenvolvimento	Perl e C	Perl	C e PHP
Tecnologia para gerar imagens dinâmicas	GD Library	GD Library	PHP GD
Tecnologia para gerar páginas dinâmicas	CGI	CGI	PHP
Alertas	e-mail	Alerta sonoro, *e-mail*, SMS e *Yowsup*	Alerta sonoro, *e-mail*, SMS, *Yowsup* e *Gtalk*

Como visto na Tabela 1, pôde-se perceber que as três ferramentas analisadas possuem diferenças em pontos importantes, onde posso citar a necessidade de *plug-in* para o Nagios gerar imagens referentes aos dispositivos gerenciados, a diferença entre as funcionalidades presentes e tipos de alertas configuráveis nas ferramentas como já citado na seção 5.2.

Pode-se destacar também, que tanto o MRTG quando o Nagios, utilizam a tecnologia CGI para manter as páginas dinâmicas. Esta tecnologia que já não é tão recente, pode trazer algum problema de segurança ou ser suscetível a ataques por permitir que sejam armazenadas informações de uma página diretamente no servidor.

6 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Devido ao grande aumento da utilização da internet, se faz necessário a instalação de equipamentos que suportem a demanda por conexão, mantendo o funcionamento da rede e ativos que a compõe de forma eficiente. Desta forma, surge a necessidade de tornar o gerenciamento e monitoramento uma tarefa menos exaustiva e mais eficaz, utilizando ferramentas que simplifiquem esta tarefa alertando caso ocorram eventos que fujam da normalidade.

Este trabalho teve como objetivo realizar um estudo sobre três destas ferramentas de monitoramento e gerenciamento existentes, sendo elas o Nagios, Zabbix e o MRTG. Além da comparação sobre as funcionalidades, foram avaliadas questões referentes a praticidade de configurar e visualizar os resultados de forma gráfica, através das aplicações *web* de cada uma, assim como a possibilidade de adequar estas ferramentas e os recursos providos pelas mesmas de maneira que o ato de gerenciar e monitorar não seja uma tarefa exaustiva.

Com base no estudo realizado sobre as ferramentas pôde-se perceber que existem muitas semelhanças entre elas, porém o MRTG não teve a mesma continuidade na questão de desenvolvimento e evolução quanto ao Zabbix e o Nagios.

Tanto o Nagios quanto o Zabbix apresentam uma constante no que se refere à evolução das ferramentas, isto se deve consideravelmente às comunidades de desenvolvedores e usuários das ferramentas. Ambas se mostraram bastante completas quando o assunto são as funcionalidades, onde a grande diferença entre elas ficou na questão de usabilidade, necessitando de mais conhecimento e entendimento desde o sistema operacional até os requisitos necessários para a instalação e configuração.

A capacidade de interação entre as ferramentas e administrador da rede é um ponto importante a ser avaliado, levando em consideração à necessidade de a rede estar em correto funcionamento a maior parte de tempo possível. Neste quesito também é importante ressaltar a variedade de opções referentes às tecnologias que podem ser utilizadas para gerar alertas presentes nas ferramentas Zabbix e Nagios.

Com base nas análises realizadas, é possível determinar que o Nagios é uma ferramenta bastante funcional, possuindo diversos *plug-ins* para complementar as funcionalidades dos usuários. O Zabbix, por sua vez, se mostrou bastante útil e mais fácil de utilizar do que o Nagios, por ser também customizável, pode ser modificada conforme for a

necessidade do administrador da rede. Como esperado, o MRTG se mostrou uma ferramenta bastante simples, fácil de utilizar, mas sem nenhuma funcionalidade a não ser a visualização dos gráficos e alertas via *e-mail*, mas realiza supre a necessidade pela qual ela foi desenvolvida.

Posterior a este estudo, pretende-se como trabalho futuro, implementar uma aplicação *Web* para exibir de forma diferenciada os gráficos oriundos do monitoramento, onde por exemplo, os resultados possam ser projetados ou exibidos de maneira que não seja necessário visualizar os gráficos somente em monitores. Com este trabalho, pretende-se utilizar novas tecnologias, como por exemplo, HTML5 e CSS3 para tornar esta aplicação mais responsiva e customizável, podendo ser ajustada conforme for a preferência ou as necessidades do administrador da rede.

7 REFERÊNCIAS

COSTA, F. **Ambiente de redes monitorados com Nagios e Cacti**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

SAUVÉ, J. P; LOPES, R.V; NICOLLETTI, P.S. **Melhores práticas para a gerência de redes de computadores.** 1. ed. Rio de Janeiro: Campus.

BLACK, T. L. **Comparação de ferramentas de gerenciamento de redes**. Porto Alegre: Universidade Federal do Rio Grande do Sul, 2008.

BRAGA, J. O. **Estudo sobre o protocolo SNMP e comparativo entre ferramentas**. Coritiba: Universidade Tuiuti do Paraná, 2011.

VASQUEZ, A. L. B. **Gerenciamento de redes**. [São Paulo]: Universidade Estadual de Campinas, 2005.

PINHEIRO, S. M. S. **Gerenciamento de redes de computadores** versão 2.0, Ago. 2002. Disponível em: <http://www.allnetcom.com.br/upload/GerenciamentodeRedes.pdf>. Acesso em: 04 Mar. 2015.

BONOMO, E. **Gerenciamento e monitoração de redes de computadores utilizando-se Zabbix**. Minas Gerais: Universidade Federal de Lavras, 2006.

KUROSE, J. F.; ROSS, K. **Redes de computadores e a internet**. 5. Ed. Pearson, 2010.

MAJEWSKI, R. **Sistemas de monitoração de rede**. Curitiba: Pontifícia Universidade Católica do Paraná, Nov. 2009.

TANENBAUM, A. S. **Computer networks**. 4. Ed. Pearson, 2011.

CANDIDO, W. L. **Gerenciamento de redes**. Paranaguá: Instituto Federal do Paraná, 2011.

SOARES, A. S.; et al. **Simple Management Network Protocol**. UFRJ. Disponível em: <http://www.gta.ufrj.br/grad/10_1/snmp/versoes.html>. Acesso em: 20 Mar. 2015.

SALVO, R. **SNMP - Introdução**. 2011. Disponível em: <http://www.ti-redes.com/gerenciamento/snmp/intro/>. Acesso em: 27 Mar. 2015.

ABREU, F. R.; PIRES H. D. **Gerência de redes**. Universidade Federal Fluminense. Disponível em: < http://www.midiacom.uff.br/~debora/redes1/pdf/trab042/SNMP.pdf>. Acesso em: 02 Abr. 2015

VMWARE.com. **Virtualization Basics**. Disponível em: <http://www.vmware.com/virtualization/virtualization-basics/how-virtualization-works>. Acesso em: 17 Mai. 2015.

PIRES, A. S. **Tutorial de instalação do agente Zabbix**. João Pessoa. Out. 2010. Disponível em: <http://zabbixbrasil.org/files/Tutorial_de_instalacao_do_agente_Zabbix.pdf>. Acesso em 10 Abr. 2015.

Zabbix LLC. **What is Zabbix**. Disponível em: <http://www.zabbix.com>. Acesso em: 10 Abr. 2015.

Zabbix SAI. **Zabbix documentation 2.4**. Disponível em: <https://www.zabbix.com/documentation/2.4/>. Acesso em: 10 Abr. 2015.

COSTA, F. A. B. **Trabalho sobre Nagios**. Disponível em: < http://pt.slideshare.net/ComandosLinux/nagios-15176062>. Acesso em: 20 Abr. 2015.

SILVA, A. d. V.; CUNHA, L. F. T. **Administração de sistemas relatório Projecto - Nagios**. Disponível em: <http://pt.slideshare.net/avarias1/nagios-11164918>. Acesso em: 20 Abr. 2015.

OETIKER, T. **Tobi Oetiker's MRTG – The Multi Router Traffic Grapher**. Disponível em: <http://oss.oetiker.ch/mrtg/>. Acesso em: 22 Abr. 2015.

QUIM, L. **CGI: Common Gateway Interface**. Disponível em: <http://www.w3.org/CGI/>. Acesso em: 30 Mai. 2015.

GUNDAVARAM, S. **CGI Programming on the World Wide Web**. Disponível em: <http://www.oreilly.com/openbook/cgi/ch01_01.html>. Acesso em: 30 Mai. 2015.

8 APÊNDICE

8.1 Instalação da ferramenta Zabbix

 # wget http://repo.zabbix.com/zabbix/2.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_2.4-1+trusty_all.deb
 # dpkg -i zabbix-release_2.4-1+trusty_all.deb
 # apt-get update
 # apt-get install zabbix-server-mysql zabbix-frontend-php zabbix-agent snmpd php5-mysql php5-curl

- Definir senha do mysql

 # sudo vi /etc/apache2/config-enabled/zabbix.conf

- Alterar linha 17: Descomentar e alterar Timezone para America/Brasilia

 # service apache2 restart
 # service zabbix-server restart

Para fazer login na interface Zabbix através do endereço http://ipDaMaquina/zabbix:

- User: admin
- Password: zabbix

8.2 Instalação da ferramenta Nagios + PNP4Nagios

 # cd /var/tmp
 # wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz
 # wget http://nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz
 # useradd nagios
 # groupadd nagcmd
 # usermod -a -G nagcmd nagios
 # usermod -a -G nagcmd www-data

 # usermod -a -G nagios www-data

 # tar zxf nagios-4.0.8.tar.gz

 # tar zxf nagios-plugins-2.0.3.tar.gz

 # cd nagios-4.0.8

 # ./configure --with-nagios-group=nagios --with-command-group=nagcmd --with-mail=/usr/bin/sendmail --with-httpd-conf=/etc/apache2/sites-enabled

 # make all

 # make install

 # make install-init

 # make install-config

 # make install-commandmode

 # make install-webconf

 # cp -R contrib/eventhandlers/ /usr/local/nagios/libexec/

 # chown -R nagios:nagios /usr/local/nagios/libexec/eventhandlers

 # /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

 # /etc/init.d/nagios start

 # htpasswd -c -b /usr/local/nagios/etc/htpasswd.users nagiosadmin alex

 # cd /var/tmp/nagios-plugins-2.0.3

 # ./configure --with-nagios-user=nagios --with-nagios-group=nagios

 # make

 # make install

 # ln -s /etc/init.d/nagios /etc/rcS.d/S99nagios

 # iptables -I INPUT -p tcp --destination-port 80 -j ACCEPT

 # apt-get install -y iptables-persistent

 # a2enmod rewrite

 # a2enmod cgi

 # service apache2 restart

- Inicio da instalação e configuração PNP4agios:

 # apt-get install rrdtool perl librrds-perl php5-gd

 # wget http://downloads.sourceforge.net/project/pnp4nagios/PNP-0.6/pnp4nagios-0.6.21.tar.gz

 # tar -xzvf pnp4nagios-0.6.21.tar.gz

 # cd pnp4nagios-0.6.21

 # ./configure

 # make all

 # make install

#make install-webconf

 # make install-config

 # make install-init

 # make fullinstall

 # vim /usr/local/nagios/etc/nagios.cfg (setar process =1 e adicionar)

- Adicionar estas linhas na configuração para que o Nagios utilize o PNP4Nagios:

process_performance_data=1

service_perfdata_file=/usr/local/pnp4nagios/var/service-perfdata

service_perfdata_file_template=DATATYPE::SERVICEPERFDATA\tTIMET::$TIMET$\tHOSTNAME::$HOSTNAME$\tSERVICEDESC::$SERVICEDESC$\tSERVICEPERFDATA::$SERVICEPERFDATA$\tSERVICECHECKCOMMAND::$SERVICECHECKCOMMAND$\tHOSTSTATE::$HOSTSTATE$\tHOSTSTATETYPE::$HOSTSTATETYPE$\tSERVICESTATE::$SERVICESTATE$\tSERVICESTATETYPE::$SERVICESTATETYPE$

service_perfdata_file_mode=a

service_perfdata_file_processing_interval=15

service_perfdata_file_processing_command=process-service-perfdata-file

host_perfdata_file=/usr/local/pnp4nagios/var/host-perfdata

host_perfdata_file_template=DATATYPE::HOSTPERFDATA\tTIMET::$TIMET$\tHOSTNAME::$HOSTNAME$\tHOSTPERFDATA::$HOSTPERFDATA$\tHOSTCHECKCOMMAND::$HOSTCHECKCOMMAND$\tHOSTSTATE::$HOSTSTATE$\tHOSTSTATETYPE::$HOSTSTATETYPE$

host_perfdata_file_mode=a

host_perfdata_file_processing_interval=15

host_perfdata_file_processing_command=process-host-perfdata-file

vim /usr/local/nagios/etc/objects/commands.cfg

- Definir Comandos para execução do PNP4Nagios:

define command{

command_name process-service-perfdata-file

command_line /usr/local/pnp4nagios/libexec/process_perfdata.pl --

}

define command{

command_name process-host-perfdata-file

command_line /usr/local/pnp4nagios/libexec/process_perfdata.pl --

}

 # service apache2 restart

 # service nagios restart

 # service npcd restart

8.3 Instalação da ferramenta MRTG

 # apt-get install snmp snmpd apache2

#vim /etc/snmp/snmpd.conf

- Descomentar a seguinte linha:

  #rocommunity public localhost

 # /etc/init.d/snmpd restart

#apt-get install mrtg

#cfgmaker --global 'workdir: /var/www/mrtg' --output /etc/mrtg.cfg public@localhost

#vim /etc/mrtg/mrtg.cfg

- Editar e adicionar:

  Options[_]: growright, bits

  RunAsDaemon: Yes

  Interval: 5

#indexmaker /etc/mrtg.cfg --columns=1 --output /var/www/mrtg/index.html

#vim /etc/apache2/apache2.conf

- Criar Alias para acesso à interface Web:

```
Alias /mrtg "/var/www/mrtg/"
<Directory "/var/www/mrtg/">
                    Options None
                    AllowOverride None
                    Require all granted
</Directory>
```

#service apache2 restart

#LANG=C /usr/bin/mrtg /etc/mrtg/mrtg.cfg --logging /var/log/mrtg.log