UNIVERSIDADE DO SAGRADO CORAÇÃO

SIMONE DE CÁSSIA FERNANDES MORETO

COMPARATIVO DE FERRAMENTAS OPEN SOURCE PARA GERENCIAMENTO DE REDE

BAURU
2015

SIMONE DE CÁSSIA FERNANDES MORETO

COMPARATIVO DE FERRAMENTAS OPEN SOURCE PARA GERENCIAMENTO DE REDE

Trabalho de conclusão de curso apresentado ao Centro de Ciência Exatas e Sociais Aplicadas da Universidade do Sagrado Coração, como parte dos requisitos para obtenção do título de bacharel em Ciência da Computação, sob orientação do Prof. Me. Henrique Pachioni Martins.

BAURU
2015

Moreto, Simone de Cassia Fernandes

M845c

Comparativo de ferramentas open source para gerenciamento de rede / Simone de Cassia Fernandes Moreto. -- 2015.

67f. : il.

Orientador: Prof. Me. Henrique Pachioni Martins.

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade do Sagrado Coração – Bauru – SP.

1. Gerenciamento de rede. 2. Ferramenta de gerenciamento. 3. Open source. I. Martins, Henrique Pachioni. II. Título.

SIMONE DE CÁSSIA FERNANDES MORETO

COMPARATIVO DE FERRAMENTAS OPEN SOURCE PARA GERENCIAMENTO DE REDE

Trabalho de conclusão de curso apresentado ao Centro de Ciência Exatas e Sociais Aplicadas da Universidade do Sagrado Coração, como parte dos requisitos para obtenção do título de bacharel em Ciência da Computação, sob orientação do Prof. Me. Henrique Pachioni Martins.

Banca examinadora:

_____
Prof. Me. Henrique Pachioni Martins
Universidade do Sagrado Coração

_____
Prof. Dr. Elvio Gilberto da Silva
Universidade do Sagrado Coração

_____
Prof. Me. Patrick Pedreira Silva
Universidade do Sagrado Coração

Bauru, 07 de dezembro de 2015.

DEDICATÓRIA

Dedico este trabalho à minha mãe, ao meu falecido pai e aos meus tios.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus por permanecer presente em minha vida e ter me dado a oportunidade de acordar todos os dias, além de me fortalecer nos momentos mais propícios.

Agradeço à minha mãe por permanecer ao meu lado em todos os momentos, me aconselhar e ser um exemplo de mulher.

Agradeço aos meus colegas de cursos que batalharam juntamente comigo para chegarmos até aqui.

Agradeço ao meu orientador, Henrique Pachioni Martins, pela prontidão em atender-me e sanar minhas dúvidas.

Agradeço aos membros da banca, Elvio Gilberto Silva, Alex Setolin Beirigo (TCC I) e Patrick Pedreira, por terem aceito o convite de participação, além de todas as considerações realizadas.

Por fim, agradeço a todos os professores nos quais tive aula e que puderam me repassar um pouco do conhecimento de cada um.

“O sucesso nasce do querer, da determinação e persistência em se chegar a um objetivo. Mesmo não atingindo o alvo, quem busca e vence obstáculos, no mínimo fará coisas admiráveis.” (José de Alencar).

RESUMO

Após a evolução tecnológica e a produção de computadores em larga escala, o mesmo tornou-se indispensável no cotidiano do ser humano. Atualmente, existe em um ambiente empresarial inúmeros dispositivos que compõem a rede, e com isso, seu controle e gerência torna-se fundamental. Através do protocolo padrão de gerenciamento de rede, SNMP, essa tarefa pode ser simplificada. Portanto, tomando ciência da necessidade de se realizar a implementação de uma ferramenta de gerenciamento de rede em um ambiente empresarial, foram selecionados três softwares open source que possibilitassem implementar, comparar e identificar os pontos relevantes de cada um deles. Para essa comparação foram utilizados o Zabbix, Cacti e The Dude. Dentre as características avaliadas estavam a facilidade de download da ferramenta, a acessibilidade da documentação, o grau de dificuldade da implementação, a disponibilidade em diversas plataformas, o recurso de busca automática de dispositivos e mapa da rede, a diversidade dos relatórios e meios de notificação, além de sua interface gráfica. Sendo assim, foi possível verificar que, apesar de cada uma das ferramentas terem suas particularidades, as três obtiveram um bom desempenho. Portanto, o que irá realmente determinar a escolha de uma delas para a implementação em uma corporação, é a necessidade da empresa de acordo com cada detalhe minucioso que a ferramenta pode lhe proporcionar.

Palavras-Chave: Gerenciamento de rede. Ferramenta de gerenciamento. Open source.

ABSTRACT

After the technological evolution and the production of large-scale computers, these devices had became indispensable in the daily lives of human beings. Currently, there can be found in a business enviroment inumerous devices that make up the network, and with it, its control and management becomes critical. Through the network management standard protocol, SNMP, this task can be simplified. Therefore, in light of the need to carry out the implementation of a network management tool in an enterprise environment, there has been selected three open source softwares that made possible implement, compare and identify relevant points of each. For said comparison was used Zabbix, Cacti and The Dude softwares. Among the characteristics evaluated were, the ease of download each tool, documentation accessibility, implementation difficulty, availability on multiple platforms, automatic search function devices and network mapping, diversity of reports and notification measures and graphical interface. Thus, it has been found that although each of the tools had their peculiarities, all of them performed well. So what will really determine the choice between them for use in a corporation, is the need of the company according to every minute detail that the tool can provide.

Keywords: Network Management. Management tools. Open source.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ASN – Abastract Syntax Notation

BER – Basic Encoding Rules

CGI – Common Gateway Interface

CPU – Central Processing Unit

DNS – Domain Name System

GNU/GPL – General Public License

ICMP – Internet Control Message Protocol

ISO – International Organization for Standardization

ISP – Internet Service Provider

LAN – Local Area Networks

MAN – Metropolitan Area Networks

MIB – Management Information Base

MRTG – Multi Router Traffic Grapher

PHP – Hypertext Processor

PING – Packet Internet Network Grouper

PDU – Protocol Data Unit

POP3 – Post Office Protocol

RRD – Round Robin Database

SLA – Service Level Agreement

SMI – Structure of Management Information

SMS – Short Message Service

SNMP – Simple Network Management Protocol

TCP/IP – Transmission Control Protocol/Internet Protocol

TI – Tecnologia da Informação

URL – Universal Resource Locator

WAN – Wide Area Networks

SUMÁRIO

1 INTRODUÇÃO

Após o surgimento dos microcomputadores e sua produção em larga em escala, o mesmo tornou-se um componente fundamental tanto na vida pessoal como na profissional do ser humano. Com isso, surge também a necessidade de se interligar esses dispositivos a fim de compartilhar recursos físicos ou lógicos, nascendo assim, a rede de computadores. Hoje em dia, o nome rede de computadores, envolve, não apenas o computador em si, mas também todos os dispositivos que possam compartilhar, de alguma maneira, informação ou recurso.

Sendo assim, uma empresa pode conter inúmeros dispositivos em sua rede administrativa, e se faz necessário o gerenciamento dos mesmos, a fim de se resguardar de eventuais problemas. Ou seja, uma empresa tem a necessidade de "[...] monitorar e controlar os elementos da rede (sejam eles físicos ou lógicos), assegurando um certo nível de qualidade de serviço." (LOPES; SUAVÉ; NICOLLETTI, 2003, p. 17). Essa prática de gerenciamento é pouco utilizada nas empresas, porém, quando as mesmas usufruem desse recurso, são inúmeros os benefícios conquistados, como, por exemplo, a pró-atividade diante de um problema em um dos componentes da rede. Portanto, com o gerenciamento de rede é possível detectar, diagnosticar e prevenir ocorrências de falhas, promover segurança e registrar a ocorrência de eventos.

Para se garantir essa gerência, existe um protocolo chamado SNMP que é considerado o protocolo padrão de gerenciamento de rede. Sua evolução é composta por três versões, até o momento, sendo que nesta última foi aprimorada principalmente a questão de segurança.

Portanto, o SNMP está presente nas ferramentas de gerenciamento de rede promovendo o monitoramento do ambiente de trabalho, além de uma visão crítica sobre os ativos da rede. E dentre essas ferramentas estão as de domínio público, as quais proporcionam à empresa a possibilidade de personalização mediante suas necessidades e perfis, além de toda a confiabilidade oferecida.

Considerando este cenário, esse trabalho tem a proposta de apresentar um gráfico comparativo entre algumas dessas ferramentas open source, visando oferecer às empresas a possibilidade de um gerenciamento de rede de qualidade, levando-se em consideração a relação custo/benefício.

1.1 OBJETIVO GERAL

Implantar e comparar o nível de desempenho e satisfação de ferramentas open source no gerenciamento de uma rede empresarial.

1.2 OBJETIVOS ESPECÍFICOS

a) estudar e compreender o contexto relacionado ao gerenciamento de redes;
b) efetuar um levantamento bibliográfico sobre as ferramentas open source;
c) relacionar os elementos considerados importantes para uma melhor gerência de rede;
d) criar critérios de avaliação;
e) estruturar e configurar uma pequena rede;
f) instalar e configurar as ferramentas open source;
g) verificar se os elementos relacionados estão presentes nas ferramentas que foram estudadas;
h) elaborar um comparativo entre as ferramentas.

.

2 REFERENCIAL TEÓRICO

Apresenta-se, nesta seção, os tópicos considerados relevantes em relação ao tema. A mesma é composta pela introdução às redes computadores abrangendo os três principais tipos de redes, pelo gerenciamento de rede tratando sua importância, as áreas que o compõem, além dos protocolos utilizados, contém detalhes sobre o mundo open source e conteúdo sobre as ferramentas que se enquadram neste contexto.

2.1 REDES DE COMPUTADORES

Atualmente, é imprescindível o uso de computadores para a realização dos mais diversos afazeres, e surge, com isso, a necessidade de trocas e atualizações de informações de maneira rápida, eficiente e segura. (FRANÇA, 2010).

Segundo Mendes (2007), as redes de computadores consistem na interligação dos computadores afim de compartilhar recursos físicos ou lógicos. Dentre os mesmos estão as informações, os softwares, as impressoras, scanners e outros.

As informações de uma empresa, sendo considerada um dos principais recursos a serem compartilhados, consiste em bancos de dados, onde, algum funcionário, em algum lugar, precisa acessá-lo remotamente. A esse modelo, chamamos de cliente-servidor, onde os servidores são os responsáveis pelo armazenamento dos bancos de dados. (TANENBAUM, 2003).

Sendo assim, as redes podem ser classificadas, basicamente, em três tipos a partir dos equipamentos utilizados e distância entre eles.

2.1.1 Redes Locais (Local Area Networks – LAN)

As redes locais, também chamadas de LANs, são redes caracterizadas pelas curtas distâncias entre os dispositivos. Podem ser facilmente encontradas em prédio de escritório de pequeno, médio e grande porte. (STALLINGS, 2005).

Segundo Forouzan (2008), as primeiras redes LANs tinham taxas de transmissão de 4 a 16 megabits por segundo, hoje normalmente são de 100 a 1000 Mbps.

E por atingirem essa velocidade, as tradicionais LANs cometem pouquíssimos erros e contém baixo retardo na transmissão. (TANENBAUM, 2003).

2.1.2 Redes Metropolitanas (Metropolitan Area Networks – MANs)

As redes metropolitanas, também chamadas de MANs, são redes que interligam os dispositivos dentro de uma área geometricamente limitada, como uma cidade, um campus universitário, ou seja, de acordo com Stallings (2005), é o campo intermediário entre as LANs e WANs.

De acordo com Dantas (2002), as MANs oferecem serviços de interligação de centrais telefônicas, transmissão de sinais de televisão, dados e voz.

Portanto, possuem características similares as redes LANs, porém, com uma maior abrangência.

2.1.3 Redes Geograficamente Distribuídas (Wide Area Networks – WANs)

As redes geograficamente distribuídas, também chamadas de WANs, são as redes que abrangem uma grande área geográfica, interligando países ou até mesmo continentes. Surgiram com a finalidade de interligar as empresas que são localizadas em diversos países.

Segundo Mendes (2007, p. 33) “[...] uma WAN sempre é formada pela interligação de no mínimo dois modens, os quais devem ser ligados a roteadores.”.

Uma rede WAN necessita de um grande investimento em infraestrutura, já que as redes compõem-se de fios, cabos, centrais comutadoras, cabos submarinos, sistemas de rádio terrestre ou de satélite.

2.2 GERENCIAMENTO DE REDES

Com a evolução tecnológica e complexidade das ações de gerência de rede, surgiu a necessidade de se criar soluções satisfatórias entre os equipamentos monitorados e quem os gerencia, independentemente de localização e distância. (ESTEVES; ALVES JUNIOR, 2013).

O ato de gerenciar/monitorar está presente corriqueiramente no cotidiano do ser humano. Pode-se tomar como exemplo os sistemas automobilísticos, onde exibem diversas notificações aos motoristas, como nível de combustível, de temperatura, bateria a fim de evitar qualquer imprevisto. (TEIXEIRA; TEIXEIRA; SILVA NETO, 2014).

Sendo assim, esse conteúdo também se refere ao gerenciamento de rede, podendo ser conceituado, segundo Forouzan (2008, p. 873) como:

> [...] monitoramento, teste, configuração e diagnóstico de componentes de rede para atender a um conjunto de exigências definidos por uma organização. Entre essas exigências, temos a operação estável e eficiente da rede que fornecem a qualidade predefinida de serviços a seus usuários. Para cumprir essa tarefa, um sistema de gerenciamento de rede utiliza hardware, software e pessoas.

Portanto, o gerenciamento de rede tem como principais objetivos detectar, diagnosticar e prevenir ocorrências de falhas, garantir segurança, além de registrar a ocorrência de eventos.

2.2.1 Áreas de Gerência

Foram criadas pela ISO (International Organization for Standardization) cinco categorias de gerência para se obter uma separação funcional entre os processos de gerenciamento, conhecida como FCAPS:

F – “Fault Management” (Gerência de falhas): Divide-se em dois subgrupos – gerência de falhas reativo e gerência de falhas proativo.

O primeiro é o responsável pela detecção, isolamento, ocorrência e registro de falhas. (FOROUZAN, 2008). Falha não é o mesmo que erro. É considerado falha uma condição anormal causada por operações incorretas ou um alto número de erros sendo necessárias ações de gerenciamento para recuperá-los. Já o erro ocorre esporadicamente e pode ser tratado numa rotina automática. (SPECIALSKI, 2001).

Seguindo, portanto, os passos para a recuperação da falha, primeiramente é necessário localizá-la e posteriormente isolá-la, com o intuito de minimizar a quantidade de usuários afetados e notificá-los, informando-os qual a previsão para a resolução.

Após o isolamento, é feita a reparação, podendo ser a substituição ou reparo do componente defeituoso.

Por fim, é necessário registrar todas as etapas processadas para que sejam documentadas e utilizadas no futuro, podendo agir com mais rapidez na manutenção do mesmo problema ou obter dados estatísticos utilizados no gerenciamento de desempenho.

O segundo, tem como foco agir, de acordo com Abreu e Pires (2014, p. 1) “[...] na antecipação de falhas, onde rotinas de diagnóstico são executadas em períodos de tempo pré-definidos [...].”.

C – “Configuration Mangement” (Gerência de configuração): Também divide-se em dois grupos: reconfiguração e documentação.

O primeiro é composto pelos ajustes realizados nos componentes e características da rede, sendo dividido em três tipos: reconfiguração de hardware, software e contas de usuário. (FOROUZAN, 2008).

Na reconfiguração de hardware envolve todas as possíveis mudanças necessárias em relação aos hardwares. Já as de software abrange todas relacionadas aos softwares. E as reconfigurações de contas de usuários envolve tanto a adição e eliminação de usuários num sistema como também os privilégios relacionados a tais usuários.

A documentação é responsável pelo registro da configuração da rede original e todas as mudanças realizadas posteriormente. Envolve, portanto, a reconfiguração, a documentação de hardware, software e contas de usuário.

Assim, podemos dizer que esse gerenciamento tem como característica o controle de identificação de todos os componentes da rede. (DANTAS, 2002).

A – “Accouting Management” (Gerência de registros, logs ou bilhetes): Está relacionado ao uso dos recursos da rede por parte dos usuários afim de gerar tarifas. “Envolve o rastreamento e geração de relatórios da utilização dos recursos da rede por cada usuário ou grupo de usuários, a fim de estabelecer métricas, verificar cotas, determinar custos e cobrar usuários.” (MELCHIORS, 1999, p. 42).

Como exemplo de utilização podem ser citados os provedores de acessos (ISPs) para que os serviços sejam tarifados, como: acesso discado, frame-relay, entre outros. (ABREU; PIRES, 2014).

P – “Performance Management” (Gerência de performance): Está associado, segundo Stallings (2005), ao monitoramento e controle, os quais permitem o

acompanhamento das atividades da rede e propõem ajustes no desempenho da mesma. E para que esses ajustes ocorram são comparados os níveis de capacidade, tráfego, throughput e tempo de resposta obtidos através de coletas de informações da rede, com um conjunto inicial de valores que estabelecem um bom padrão de desempenho.

Sendo assim, pode-se resumir que a função dessa gerência é garantir que a rede esteja trabalhando com a máxima eficiência. (FOROUZAN, 2008).

S – “Security Management” (Gerência de segurança): É o responsável pela segurança das informações e por detalhar tentativas, de sucesso ou não, de invasão na rede, também estabelece políticas de uso, chaves criptografadas, logs do acesso à rede, procedimentos de investigação a acesso não autorizado, detecta e previne vírus de computadores. (LEWIS, 1995 citado por MELCHIORS, 1999).

Portanto, segundo Dantas (2002, p. 227), essa área se resume ao emprego de “[...] uma abordagem de coleta, armazenagem e verificação de arquivos de segurança de eventos.”.

2.2.2 Protocolo SNMP

De acordo com Black (2008), no final da década de 1980, as redes baseadas na arquitetura e protocolos TCP/IP, começaram a se expandir, porém a gerência das mesmas era basicamente inexistente devido à falta de soluções destinadas a esse protocolo. Até que um grupo de engenheiros desenvolveram uma solução temporária, o Simple Network Management Protocol (SNMP). Ao final da década de 1990, a solução SNMP passou de um protocolo temporário ao padrão de gerência de redes de computadores.

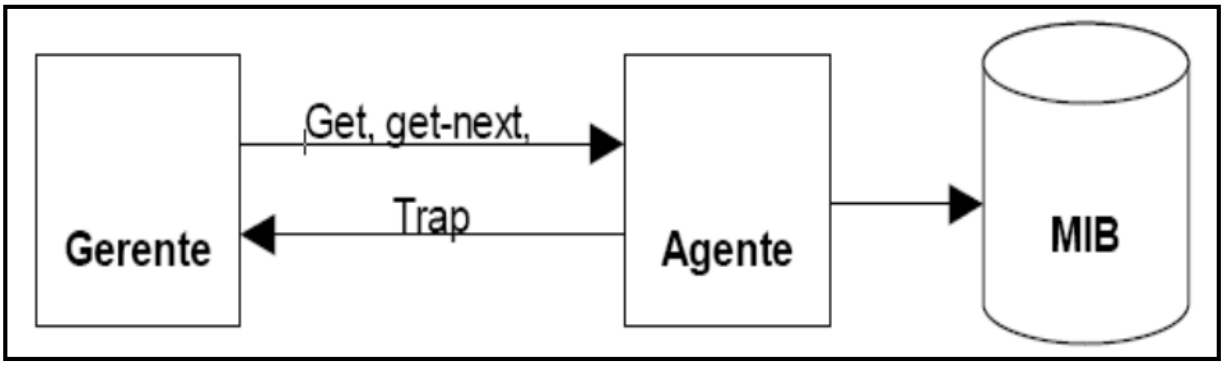
Forouzan (2008) define o SNMP como um protocolo que opera na camada de aplicação, utilizando o conceito de gerente e agente, onde os agentes são controlados por um pequeno número de gerentes, com o objetivo de monitorar dispositivos de diferentes fabricantes e em diversas redes físicas.

Considerando, portanto, que o protocolo SNMP utiliza o conceito de gerente e agente, define-se gerente, segundo Stallings (2008), como a interface entre o gerente humano da rede e o sistema de gerenciamento com o propósito de se monitorar e controlar a rede, contém um conjunto de aplicações de gerenciamento para análise de dados, uma capacidade de traduzir as necessidades do gerente, um banco de

dados recorrente das informações capturadas de todos os elementos gerenciados, ou seja, um host onde roda o programa-cliente. Já o agente, pode ser definido como aquele que responde, a partir de uma estação de gerenciamento, às requisições de informações, além de fornecer informações importantes sem serem solicitadas, ou seja, um roteador ou host que executa o programa-servidor SNMP.

Na Figura 1 pode-se observar o funcionamento do SNMP, composto das trocas de operações entre o gerente e o agente, o agente buscando informações ou realizando modificações de uma variável de um objeto na MIB.

Figura 1 - Modelo de gerenciamento SNMP.



Fonte: Mundo TI Brasil (2012).

Forouzan (2008, p. 878), conclui que existem três conceitos básicos para o gerenciamento via SNMP:

> 1 – Um gerente monitora o estado de um agente solicitando informações que refletem o comportamento do agente.
> 2 – Um gerente força um agente a realizar uma tarefa reinicializando valores no banco de dados do agente.
> 3 – Um agente contribui para o processo de gerenciamento alertando o gerente sobre uma situação anormal.

E para se atingir tal gerenciamento existem dois protocolos auxiliares: SMI (Structure of Management Information) e MIB (Management Information Base) os quais serão abordados a seguir, além do SNMP.

2.2.2.1 Structure of Management Information - SMI

O SMI é um protocolo criado para especificar um conjunto de regras utilizadas para definir tipos, nomear e identificar as variáveis MIB. Especifica que as mesmas

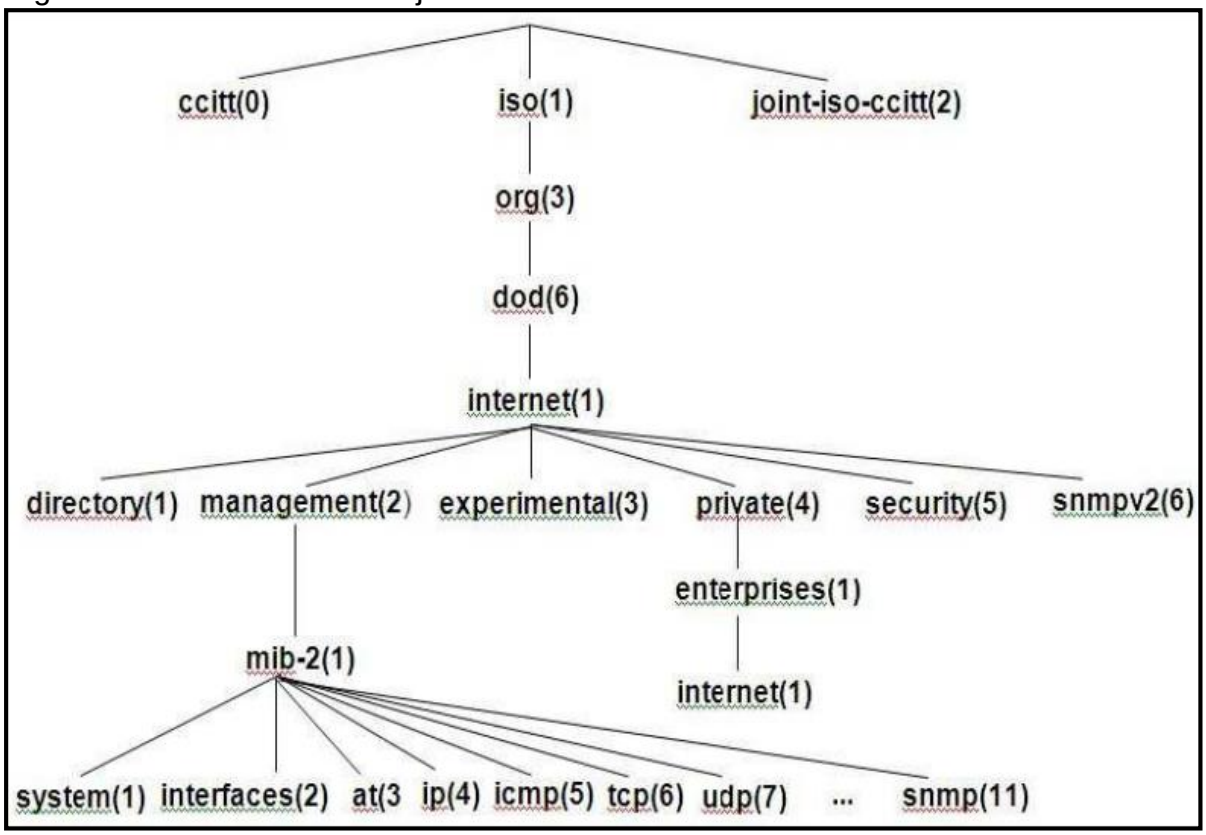
precisam ser definidas e referenciadas usando a ASN.1 (Abastract Syntax Notation), uma linguagem formal que possui uma notação usada em documentos lidos por humanos, e uma representação codificada das mesmas informações utilizadas nos protocolos de comunicação. (COMER, 2006).

De acordo com Forouzan (2008), o SMI, versão 2 (SMIv2), tem como função a nomeação do objeto, definição do tipo de dados que podem ser armazenados no mesmo e sua codificação para a transmissão através da rede.

O SMI requer que cada objeto gerenciado tenha um nome exclusivo e para isso utiliza um identificador global de objeto disposto de maneira hierárquica. (COMER, 2006).

Como pode ser observado na Figura 2, os objetos que são utilizados pelo SNMP estão sempre abaixo do objeto mib-2, portanto, todos iniciarão com 1.3.6.1.2.1 – iso.org.dod.internet.mgmt.mib-2.

Figura 2 - Identificador de objetos.



Fonte: Mundo TI Brasil (2012).

O SMI também especifica os tipos de dados que podem ser armazenados no objeto gerenciado, é considerado, segundo Stalling (2008), um conjunto

razoavelmente restrito de tipos, já que, por exemplo, não são aceitos números reais, porém, atende praticamente todas as necessidades de gerenciamento de rede.

Na Figura 3 pode-se identificar os tipos de dados que são permitidos.

Figura 3 - Tipos de dados.

Tipo de Dados	Descrição
INTEGER	Inteiros na faixa de -2^{31} a $2^{31} - 1$.
UInteger32	Inteiros na faixa de 0 to $2^{32} - 1$.
Counter32	Um inteiro não-negativo que pode ser incrementado em módulo 2^{32}.
Counter64	Um inteiro não-negativo que pode ser incrementado em módulo 2^{64}.
Gauge32	Um inteiro não-negativo que pode aumentar ou diminuir, mas não deve exceder um valor máximo. O valor máximo não pode ser maior que $2^{32} - 1$.
TimeTicks	Um inteiro não-negativo que representa o tempo, módulo 2^{32}, em centésimos de segundo.
OCTET STRING	Strings de octeto para dados binários ou textuais arbitrários; pode-se limitar 255 octetos.
IpAddress	Um endereço de inter-rede de 32 bits.
Opaque	Um campo de bit arbitrário.
BIT STRING	Uma enumeração de bits nomeados.
OBJECT IDENTIFIER	Nome administrativamente atribuido a objeto ou outro elemento padronizado. O valor é uma sequência de até 128 inteiros não-negativos

Fonte: Stallings (2008, p. 419). Adaptada pelo autor.

O método de codificação é definido pelas regras de codificação básicas, BER (Basic Encoding Rules), as quais especificam precisamente os itens de dados e os nomes de uma mensagem. (COMER, 2006).

Segundo Forouzan (2008), os dados são codificados em forma de trinca, contendo: marca, comprimento e valor. Na Figura 4 estão representados os códigos especificados para cada tipo de dado.

Figura 4 - Código para tipos de dados.

Tipos de dados	*Classe*	*Formato*	*Número*	*Marca (Binária)*	*Marca (Hexa)*
INTEGER	00	0	00010	00000010	02
OCTET STRING	00	0	00100	00000100	04
OBJECT IDENTIFIER	00	0	00110	00000110	06
NULL	00	0	00101	00000101	05
Sequence, sequence of	00	1	10000	00110000	30
IPAddress	01	0	00000	01000000	40
Counter	01	0	00001	01000001	41
Gauge	01	0	00010	01000010	42
TimeTicks	01	0	00011	01000011	43
Opaque	01	0	00100	01000100	44

Fonte: Forouzan (2008, p. 885). Adaptada pelo autor.

2.2.2.2 Management Information Base – MIB

A MIB, segundo Forouzan (2008, p. 879), “[...] cria um conjunto de objetos definidos para cada entidade de forma similar a um banco de dados (principalmente metadados em um banco de dados, nomes e tipos sem valores).” Comer (2006), complementa exemplificando uma MIB para um endereço de IP, onde a mesma especifica que um software precisa realizar uma contagem de todos os octetos que chegam pelas interfaces da rede e o software de gerenciamento só pode ler essa contagem.

A MIB versão 2, (MIB2), pode ser dividida em alguns grupos de acordo com suas informações, conforme ilustra a Figura 5.

Figura 5 - Grupos de informações da MIB2.

Grupo	Informação
system (1)	informações básicas do sistema
interfaces (2)	interfaces de rede
at (3)	tradução de endereços
ip (4)	protocolo IP
icmp (5)	protocolo ICMP
tcp (6)	protocolo TCP
udp (7)	protocolo UDP
egp (8)	protocolo EGP
transmission (10)	meios de transmissão
snmp (11)	protocolo SNMP

Fonte: Esteves e Junior (2013, p. 4).

Sendo assim, por exemplo, uma variável MIB sysUPTime está contida no grupo system que tem como significado a amostra do tempo desde a última reinicialização do sistema.

2.2.2.3 Simple Network Management Protocol – SNMP

O protocolo SNMP evoluiu através de três gerações: SNMPv1, SNMPv2 e o atual-SNMPv3, todos, porém, segundo Comer (2006), usam a mesma estrutura e muitos recursos são compatíveis entre as versões.

O SNMPv3, define 8 tipos de pacotes, também nomeados por PDUs, sendo eles: GetRequest, GetNextRequest, GetBulkRequest, SetRequest, Response, Trap, InformRequest e Report. O SNMP PDU é um espaço da mensagem SNMP onde ficam registradas as configurações das mesmas de acordo com o tipo que foi enviada. (ESTEVES; ALVES JUNIOR, 2013).

Uma mensagem SNMP é composta por 4 elementos versão do protocolo, dados de cabeçalho, parâmetros de segurança e dados, onde estão inclusos os PDUs.

As definições de cada PDU, de acordo com Forouzan (2008), podem ser descritas como:

a) GetRequest: É enviado do gerente para o agente para a leitura do valor de uma variável ou um conjunto de variáveis;
b) GetNextRequest: É enviado do gerente para o agente para a leitura do valor de uma variável sem saber seu nome exato;
c) GetBulkRequest: É enviado do gerente para o agente para a leitura de um grande volume de dados;
d) SetRequest: É enviado do gerente para o agente para o armazenamento de um valor em uma variável;
e) Response: É enviado do agente para o gerente como resposta as requisições de leitura;
f) Trap: É enviado do agente para o gerente caso haja alguma anormalidade;
g) InformRequest: É enviado do gerente para outro gerente remoto, são referências a dados de terceiros;
h) Report: Ainda não utilizado, porém foi projetado para alguns tipos de erros entre gerentes.

2.2.3 O Mundo Open Source

Traduzindo ao pé da letra, open source seria código aberto, porém, segundo a Open Source Initiative [2015?], open source não significa simplesmente acesso ao código fonte, para se considerar um software open source, o mesmo deve cumprir os seguintes critérios:

a) Redistribuição livre: A licença não deve restringir de maneira nenhuma a venda ou a distribuição do software, e nem exigir royalty ou qualquer outra taxa;
b) Código fonte: O software deve incluir o código fonte e permitir a distribuição tanto em código fonte quanto em formato compilado;
c) Trabalhos derivados: A licença deve permitir modificações e softwares derivados, além de serem distribuídos sob os mesmos termos da licença do software original;
d) Integridade do código fonte do autor: Para que o código fonte original não seja modificado sem o consentimento do autor, a licença pode exigir que o código modificado seja disponibilizado com um nome ou versão diferente do original;
e) Não à discriminação contra pessoas ou grupos: A licença não pode fazer discriminação de nenhuma pessoa ou grupos de pessoas;
f) Não à discriminação contra fins de utilização: Sua utilização não pode ser vedada a nenhuma finalidade;
g) Distribuição de licença: A licença é válida para qualquer versão redistribuída, não é necessária a execução de uma licença adicional;
h) A licença não pode ser específica para um produto: Os mesmos direitos que são concedidos a distribuição do software original também se concedem a todas as partes para quem o programa é redistribuído;
i) Licença não deve restringir outro software: Um software fechado pode ser distribuído numa mídia juntamente com o open source;
j) Licença deve ser tecnologicamente neutra: Nenhuma clausula da licença deve incluir uma disposição padrão a ser aplicada.

A principal finalidade dessas restrições é a garantia da continuidade do software sempre aberto e disponível para todos que interessem.

Além disso, segundo Pereira, Marinho e Oliveira ([2015?]), um programa desenvolvido na filosofia open source permite a seus utilizadores executar, estudar, modificar, repassar (com ou sem alterações) as possíveis melhorias realizadas. Sendo que a realização desse desenvolvimento se dá em 4 tipos de liberdade aos seus usuários:

a) A liberdade de executar o programa para qualquer propósito;

b) A liberdade de estudar como o programa funciona, e adaptá-lo para suas necessidades;
c) A liberdade de redistribuir cópias de modo que o utilizador possa ajudar o seu próximo;
d) A liberdade de aperfeiçoar o programa, e distribuir os seus aperfeiçoamentos, de modo que toda a comunidade beneficie com isso.

Sendo assim, as ferramentas de gerenciamento de rede detalhadas a seguir se encaixam nesses requisitos.

2.2.4 Ferramentas de Gerenciamento de Rede

Todos os conceitos detalhados nos tópicos anteriores são implantados nas chamadas ferramentas de gerenciamento de rede para que se tenha o controle efetivo de todos os dispositivos da rede

A maioria delas são baseadas no MRTG (Multi Router Traffic Grapher), um script em Perl que utiliza o SNMP para obter dados de tráfego do roteador e um programa em C para logar os dados e criar os gráficos da rede monitorada. (BLACK, 2008).

Sendo assim, as ferramentas vêm sendo evoluídas em relação as novas tendências voltadas para a web, focando a usabilidade e visibilidade do produto.

2.2.4.1 NAGIOS

Levando em consideração as informações de Nagios (c2009-2015), o Nagios é uma ferramenta de monitoramento poderosa, com o objetivo de permitir aos usuários a identificação e resolução dos problemas que possam acontecer na rede antes que gere grandes desconfortos.

Segundo Costa (2008), o Nagios foi desenvolvido por Netsaint, primeiramente atendendo somente o sistema operacional Linux, mas atualmente, já roda em outras derivações do Unix.

Ainda, de acordo com o fabricante, segue-se de um ciclo de funcionamento, onde após a instalação e configuração do Nagios, inicia-se o processo de monitoramento dos componentes da rede, incluindo os serviços, como SMTP, POP3,

ICMP, SNMP, servidores, métricas do sistema, como carga de processador, uso de disco, logs do sistema. Ocorrendo alguma falha e resolução, existe a opção de receber os alertas via SMS, email, pager. Em resposta, a equipe de TI começa um trabalho de investigação. Podendo o mesmo ser intensificado com o uso dos relatórios, afim de garantir o SLA (Service Level Agreement), ou seja, garantir o nível de acordo de serviço estabelecido entre um cliente e um fornecedor de serviços, por exemplo. Caso seja necessário algum reparo, existe a possibilidade de impedir os alertas durante esse período. Com todos esses históricos em mãos, consegue-se realizar um planejamento e realizar as atualizações de infra-estrutra necessárias antes mesmo que ocorra alguma falha.

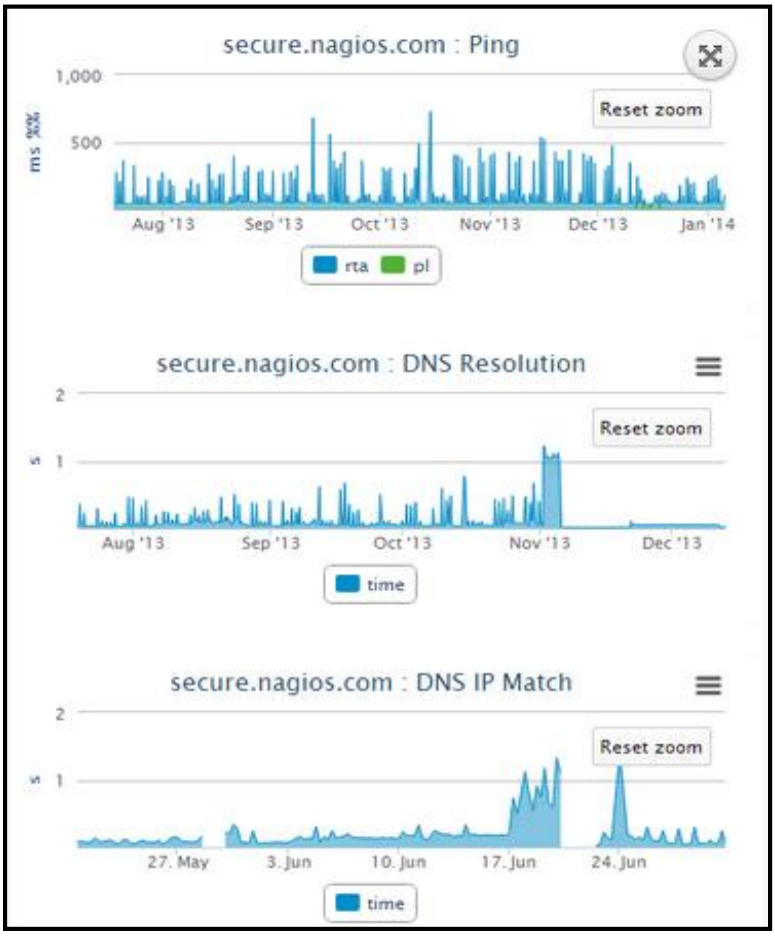
Antes de iniciar o monitoramento da rede através dessa ferramenta, é necessário realizar algumas alterações ou criações em vários arquivos de configurações, como:

a) Arquivo de configuração principal: a esse arquivo dá-se o nome de nagios.cfg, sendo que é composto por diversas diretivas que são lidas pelo seu próprio processamento e pelos arquivos CGIs. O arquivo é criado automaticamente quando se instala o Nagios através de script. (COSTA, 2008);
b) Arquivos de recursos: o arquivo resources.cfg é utilizado para armazenar macros definidas pelo usuário. (BLACK, 2008);
c) Arquivos de configuração de objetos: de acordo com Costa (2008), nesses arquivos, historicamente chamados arquivos de configuração de clientes, são definidos os serviços, clientes, grupos de clientes, contatos, grupos de contatos, comando, períodos de tempo, dependência de serviço, entre outros;
d) Arquivo de configuração de CGI: geralmente localizado em /usr/local/nagios/etc/cgi.cfg, contém várias diretivas que afetam a opção dos CGIs. Um exemplo, segundo Black (2008), de arquivo de configuração de CGI é gerado de maneira automática assim que o “script configure” é executado antes de compilar os binários;
e) Arquivos de configuração de informações estendidas: segundo Costa (2008) são utilizadas para definições opcionais de clientes e serviços as quais serão utilizadas pelas CGIs, com o intuito de prover URLs com

informações extras sobre o serviço ou cliente, formatar os ícones, e desenhar as coordenadas dos gráficos.

Na Figura 6 é possível visualizar a tela de monitoramento de desempenho realizado pelo Nagios.

Figura 6 – Tela de monitoramento de Desempenho.



Fonte: Nagios (c2009-2015).

Sendo assim, o primeiro gráfico demonstra, em relação ao comando PING, de agosto de 2013 a janeiro de 2014, o tempo médio de resposta obtida desde o envio até o recebimento de um pacote (rta) e a porcentagem de perda de pacotes (pl), ou seja, observa-se que nesse período tiveram poucos picos que ultrapassaram a faixa de 500 ms e a porcentagem de perdas de pacotes foi mínima.

2.2.4.2 CACTI

Segundo informações do Cacti (c2004-2012), o Cacti é uma ferramenta capaz de manter gráficos e fontes de dados através da coleta de informações sobre o estado da rede. É uma interface completa para RRDToll (Round Robin Database) com um frontend em PHP. Além de prover suporte para o protocolo SNMP. Foi desenvolvida para, de acordo com Costa (2008), ser flexível ao ponto de se adaptar de maneira fácil a qualquer necessidade, como também ser robusta de utilização. Com ela, é possível fazer o monitoramento dos estados dos elementos da rede e programas além da largura de banda utilizada e uso da CPU.

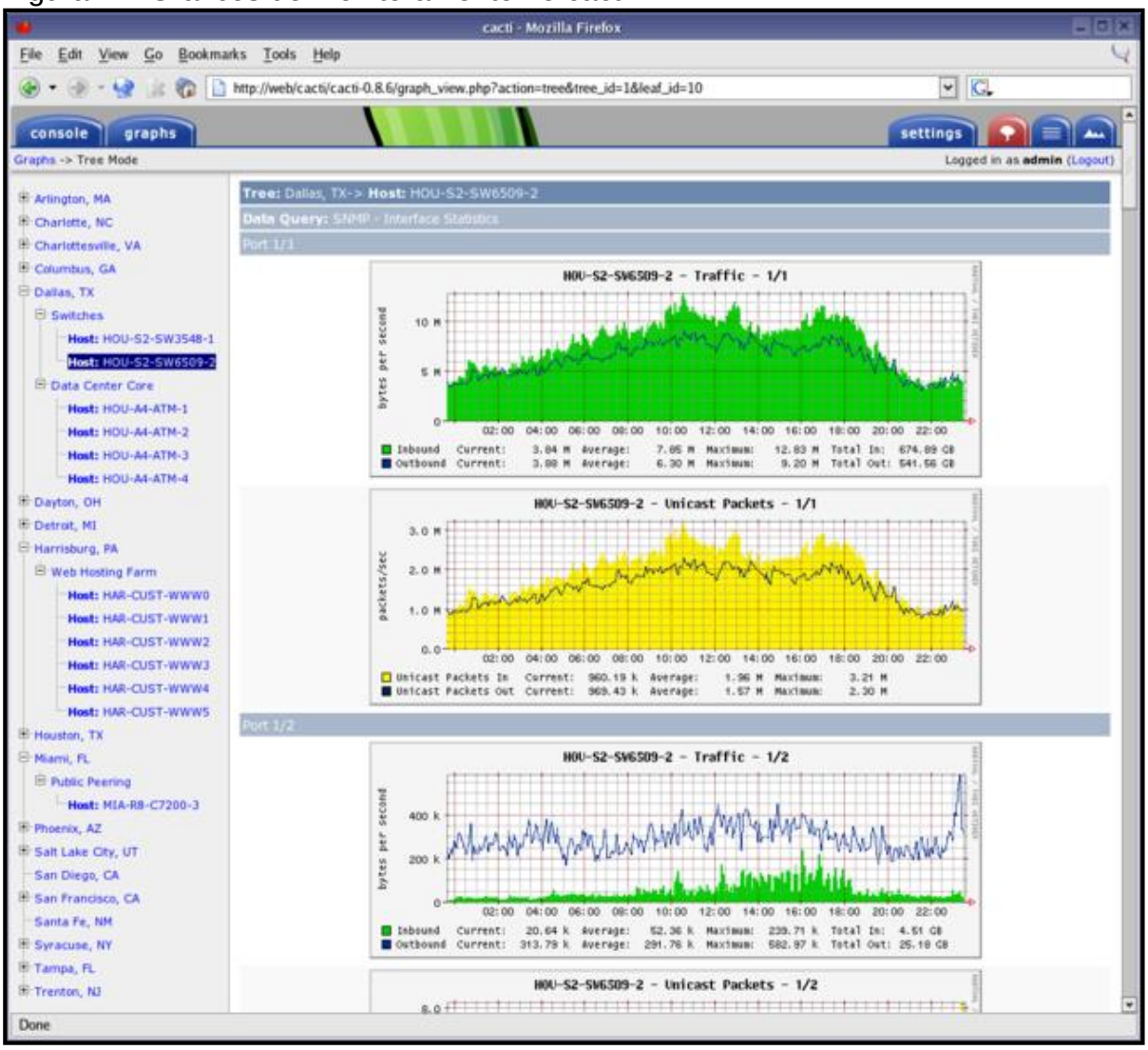
Segundo Black (2008), o RRDToll foi criado por Tobias Oetiker e é um sistema de base de dados Round-Robin sob licença GNU GPL, desenvolvido para armazenar dados sobre o estado de rede de computadores.

Sua arquitetura prevê a possibilidade de expansão através de inúmeros plugins desenvolvidos pela comunidade, sendo que um deles é o PHP Network Weathermap. Com ele é possível mostrar o mapa da rede bem como o estado de cada elemento. (COSTA, 2008).

Também é possível a gerência de usuários, atribuindo a umas suas permissões. Na Figura 7 pode-se observar uma tela de monitoração de link de dados com a utilização do Cacti.

Observa-se, portanto, o tráfego de entrada e saída de dados num período das 02:00 até as 22:00, sendo que o valor máximo de entrada foi de 12,83 MB/s e de saída 9,20 MB/s. Também é possível visualizar o tráfego de pacotes unicast, variando em torno de 2 a 3 M Packets/s.

Figura 7 – Gráficos de monitoramento no cacti.



Fonte: Cacti (c2004-2012).

2.2.4.3 THE DUDE

De acordo com o site Mikrotik ([2015?]), o The Dude é um software gratuito criado pela MikroTik, o qual promove uma drástica melhora no que se diz gerenciamento de rede. Com ele é possível a verificação automática de todos os dispositivos dentro de sub-redes, desenhos e layouts de mapas da rede, controle dos serviços dos dispositivos e execução de ações baseadas em mudanças de estados dos mesmos.

Em relação a plataforma, está disponível para Windows, a partir do Windows 2000, como também para Linux, via Wine e MAC, via Darwine.

Dentre suas características, ainda segundo o próprio fabricante, podemos citar:

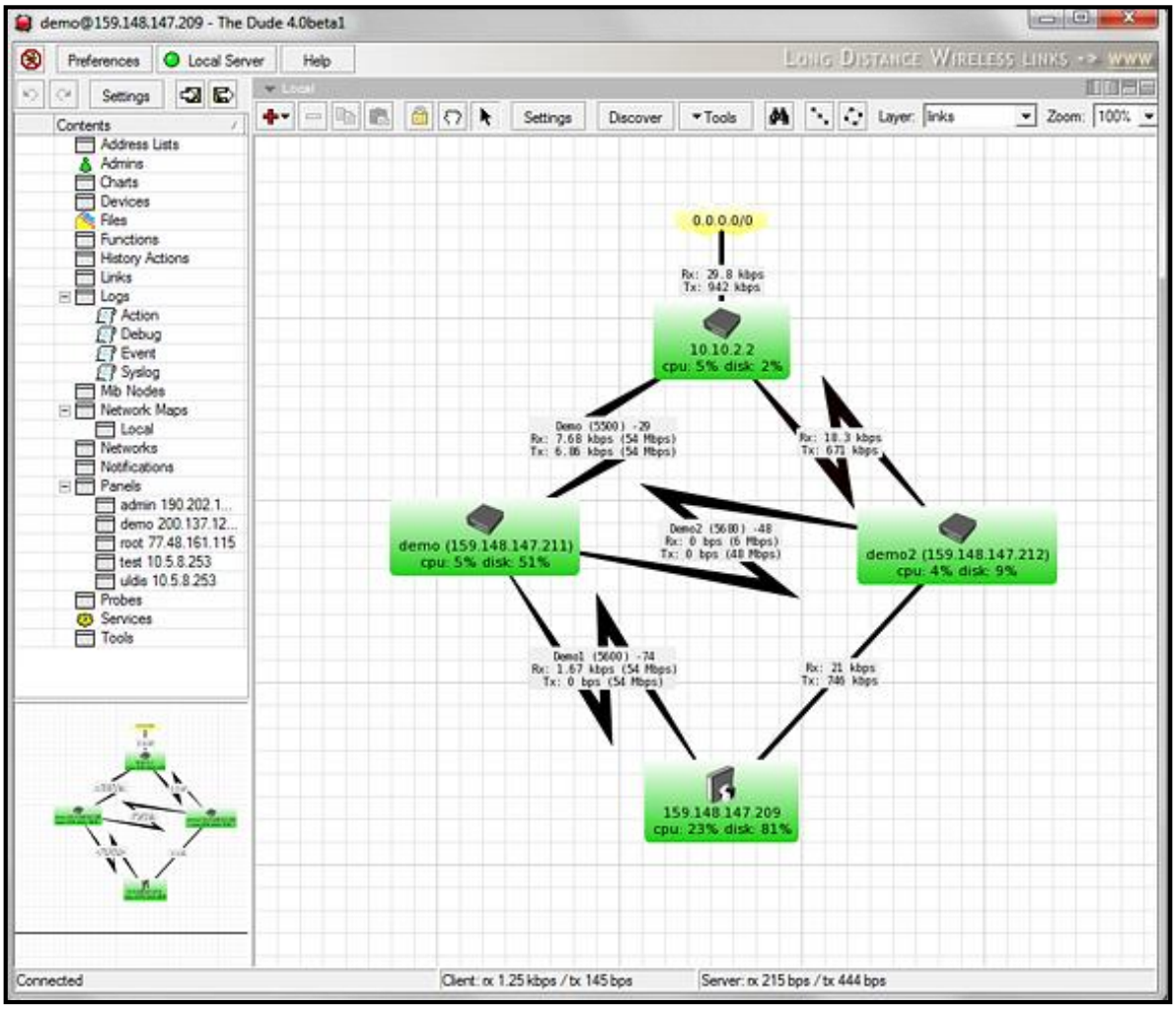
a) descoberta de qualquer tipo ou marca de dispositivo;
b) monitoramento de link, dispositivos e notificações;
c) inclui ícones formato SVG para dispositivos, suporta ícones e fundos personalizados;
d) fácil instalação e uso;
e) permite-lhe desenhar seus próprios mapas e adicionar dispositivos personalizados;
f) suporta SNMP, ICMP, DNS e monitoramento TCP para dispositivos suportados;
g) realiza monitoramento individual de links e gráficos;
h) acesso direto a ferramentas de controle para gerenciamento de dispositivos;
i) suporta servidor remoto Dude e cliente local.

Como um dos destaques da ferramenta, segundo Benini e Daibert (2011), pode ser inserida a maneira como os menus e as janelas estão localizados, tornando sua usabilidade agradável.

Como pode-se observar na Figura 8, os conteúdos da ferramenta encontram-se na lateral esquerda e no centro da tela fica disponível o mapa da rede no qual foi projetado o aplicativo de gerenciamento.

Sendo assim, navegando dentre os itens é possível a manipulação de dados de todos os dispositivos, alterar nome e tipo de ícone. Consegue-se também desenhar o mapa da rede para que seja mais visível sua compreensão. As notificações de interrupções também são editáveis, bem como os serviços nos quais se deseja monitoração. O software também se dispõe a guardar os logs de acessos realizados.

Figura 8 - Interface The Dude.



Fonte: Mikrotik ([2015?]).

2.2.4.4 ZABBIX

De acordo com Zabbix (c2001-2015), o Zabbix é um software projetado para monitoramento dos componentes de infra-estrtura de TI projetado para quem se espera obter disponibilidade e desempenho da gerência empresarial.

Tem sido comumente classificado, de acordo com Black (2008), como uma das melhores ferramentas de gerenciamento, pois tem como foco as lacunas em branco deixadas por outros fabricantes.

Ainda considerando Black (2008), o Zabbix pode ser executado em qualquer distribuição Linux/Unix, requisitando somente a instalação de um servidor de banco de dados, o apache, e o interpretador PHP.

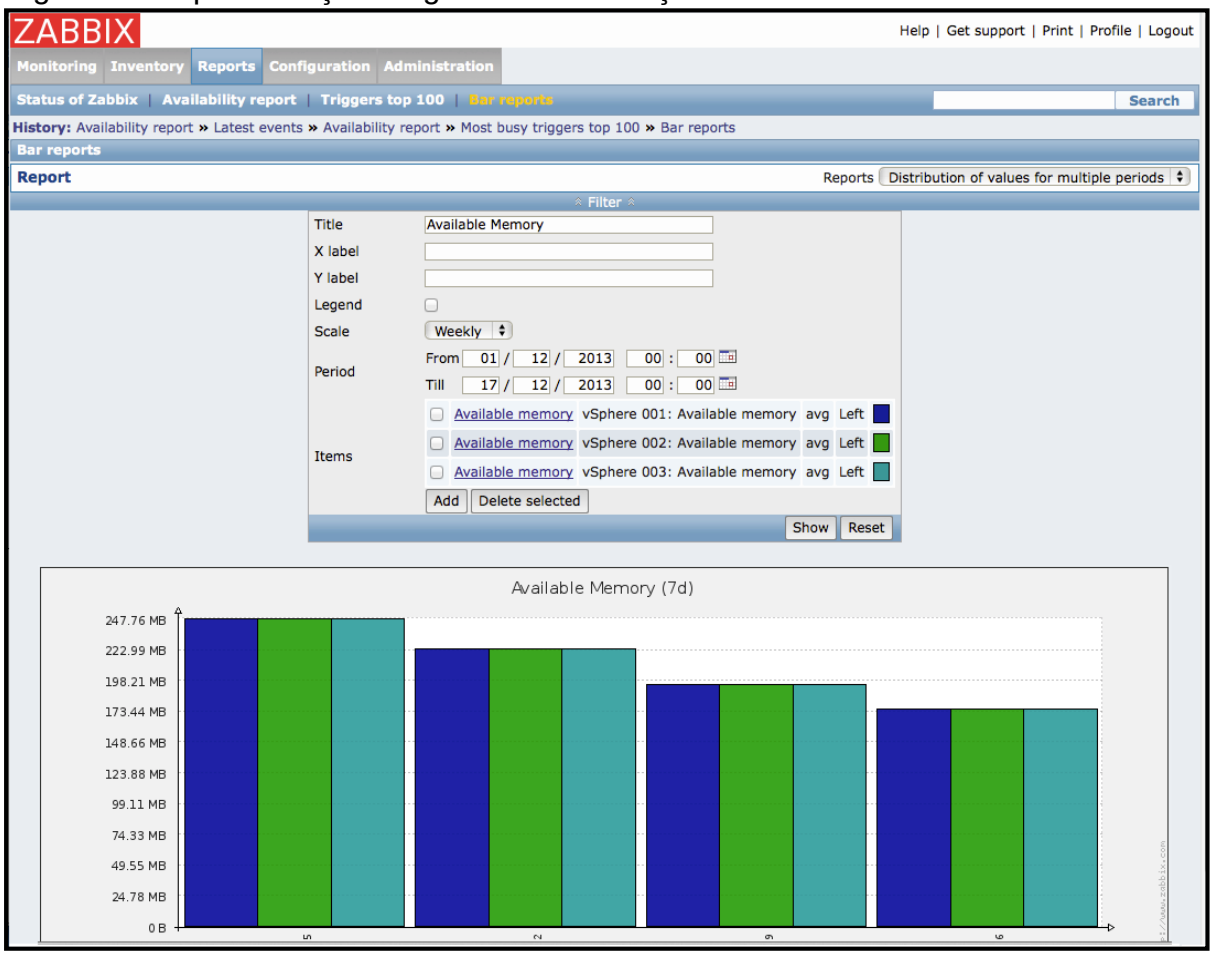
Essa ferramenta oferece, segundo Bonomo (2006), suporte a polling (capturação de dados de tempo em tempo) e trapping (notificação de alarmes), interface web, excelentes relatórios, baixo custo de implantação, serviços de auditoria, monitoramento do SLA, entre outros.

Na Figura 9, pode ser observado um dos gráficos disponíveis no Zabbix em relação a avaliação de memória.

Portanto, nesse relatório obtido pelo Zabbix, em relação a avaliação de memória, pode-se perceber que a utilização da mesma no agente selecionado variou de 247,76 MB a 173,44 MB.

Existe a possibilidade de se definir limites (thresholds) para cada alerta, que são ativados e poder ser enviados aos responsáveis através de SMS, e-mail.

Figura 9 - Representação de gráfico de avaliação de memória.



Fonte: Zabbix (2015).

Dessa forma, o Zabbix oferece facilidade de implantação e configuração destacando-se com sua interface intuitiva e atendendo às expectativas dos usuários.

2.3 TRABALHOS CORRELATOS

A área de rede de computadores é composta por vários tópicos, dentre eles o gerenciamento da mesma. Tópico no qual tem-se uma quantidade de material relevante, tratando principalmente da utilização dos protocolos envolvidos.

Para que haja controle praticamente total dos principais componentes da rede, são implantadas ferramentas de gerenciamento com o objetivo de se resguardar de eventuais problemas.

Sendo assim, é possível encontrar artigos e trabalhos científicos voltados para essa área, geralmente especificando somente uma ferramenta, ou fazendo-se comparações entre algumas ferramentas que não são open source.

Neste contexto se encaixa a monografia intitulada “Gerenciamento e monitoração de redes de computadores utilizando-se Zabbix”, em que aborda um estudo de caso envolvendo a implementação e configuração da ferramenta Zabbix relacionando os itens teóricos, como o protocolo SNMP, sendo que foi a ferramenta disponibiliza inúmeros recursos na ajuda da administração de rede, como gráficos de maior desempenho na coleta dos dados em tempo real e com mais informações, alertas de erros ocorridos nas entidades gerenciadas, configurações, auditoria dos dados. (BONOMO, 2006)

Pode-se citar também a monografia intitulada “Comparação de ferramentas de gerenciamento de redes”, em que aborda o conceito de gerenciamento de rede e seus paradigmas e a comparação entre ferramentas de gerenciamento de rede, open source ou não, sendo que o objetivo principal o auxílio na escolha da ferramenta, de acordo com alguns parâmetros relevantes, sendo a performance, facilidade de utilização e necessidade de recursos tanto de hardware quanto humanos. (BLACK, 2008)

Dessa forma, esse trabalho tem como intuito analisar e comparar algumas ferramentas open source disponíveis no mercado, além de contribuir para trabalhos futuros relacionados ao tema e tornar-se um guia para empresas que visam implementar uma dessas ferramentas.

3 METODOLOGIA

Para se chegar à conclusão deste trabalho, o mesmo foi divido em duas etapas: a primeira com o intuito de identificar os principais temas teóricos e a segunda, uma parte prática onde ocorreu a implementação das ferramentas de rede open source e a análise dos resultados obtidos através do gerenciamento das mesmas.

Sendo assim, na primeira etapa foi realizado um levantamento bibliográfico, sendo que estes conteúdos estavam presentes em livros, artigos científicos e outras fontes disponíveis na internet, contendo referências sobre o que são as redes de computadores, como funciona e os protocolos que compõem o gerenciamento de uma rede, bem como as ferramentas open source.

Após a conclusão dessa etapa, foi iniciada a parte prática, composta pela utilização de três ferramentas open source para o gerenciamento da rede.

As ferramentas escolhidas para a coleta de dados referentes ao estado da rede foram: Cacti, The Dude e Zabbix.

A escolha dessas ferramentas se justificou pelo fato de serem open source e as mais evidenciadas, onde possuem um número relevante de conteúdo sobre, exceto o The Dude que é uma ferramenta menos evidência, mas apresenta, segundo seu referencial, bom desempenho.

A implementação de cada ferramenta foi realizada emulando uma máquina virtual Linux Ubunt 14.04.3, gerenciada pelo software Oracle VM VirtualBox 5.0.0 r101573 em um notebook DELL Vostro 5470, com Windows 10 64 bits, processador Intel Core i7-4510U CPU@2.000 GHz, 8 GB de memória RAM e disco rígido de 500 GB.

Foi configurado o protocolo de gerenciamento SNMP em cada máquina virtual, no notebook DELL, como também em um outro notebook, um POSITIVO Unique, com Windows 7 Ultimate 32 bits, processor Intel Celeron CPU925@2.30 GHz, 2 GB de memória RAM e disco rígido de 500 GB.

Foi necessária a instalação de alguns softwares que são pré-requisitos para o funcionamento das ferramentas, como o MySQL, o servidor Apache, o PHP, e o Wine.

Com isso, as ferramentas implementadas foram configuradas e iniciaram a coleta dos dados.

Para efeito de comparação entre as ferramentas foi utilizada uma tabela, conforme mostra a Figura 10. Sendo assim, nessa tabela, estão descritos alguns

elementos considerados importantes, desde a facilidade da obtenção da ferramenta até a complexidade dos relatórios que possam ser gerados. Foi atribuído, portanto, pesos de acordo com a relevância de cada item, sendo que os itens nos quais foram atribuídos peso no valor de 0,5, se apresentam de maneira menos relevante, já que são destinados ao processo de obtenção da ferramenta, bem como sua interface, portanto, esses itens não interferem, propriamente, no ato de gerenciamento da rede. Diferentemente dos demais, onde foram atribuídos peso no valor de 1, pois são itens considerados mais relevantes para o bom gerenciamento da rede, como o mapa da rede e os meios de notificações que podem ser utilizados.

Figura 10 - Tabela de pesos.

Tabela de associação de pesos e elementos importantes para o comparativo das ferramentas.	Facilidade de download	Documentação Acessível	Facilidade de Implementação	Disponibilidade em diferentes plataformas	Interface amigável	Busca Automática dos dispositivos da rede	Mapa da rede	Diversidade de meios de notificação	Diversidade dos relatórios	Total
Pesos	0,5	1	0,5	0,5	0,5	1	1	1	1	7

Fonte: Elaborada pelo autor.

Cada ferramenta teve sua nota variada numa escala dos números inteiros entre 0 e 4, pois cada item pode ser considerado uma variável qualitativa ou categórica, onde é apresentado um número limitado de valores, classificada em ordinal, seguindo um nível crescente (ordem) entre as categorias. (NORMANDO, TJADERHANE, QUINTÃO, 2010).

Foi realizada uma média ponderada, sendo esta geralmente utilizada quando necessita que um conjunto de conteúdos sejam analisados juntos, através de uma combinação com pesos aos elementos e notas às classes. (DONHA, SOUZA, SUGAMOSTO, 2006). Os pesos e a forma de classificação foram definidos pela própria autora da pesquisa com base em diversas publicações, portanto, caso seja estabelecido algum outro critério de avaliação, possivelmente, as notas destinadas a cada ferramenta, bem como a conclusão final, poderão variar.

Sendo assim, a ferramenta que obteve a nota mais próxima de 4, após a avaliação em todos os quesitos, foi considerada a ferramenta com maiores chances de sucesso após ser implementada em um ambiente empresarial.

3.1 CRITÉRIOS DE AVALIAÇÃO

Os critérios de avaliação, de acordo com cada item, são dispostos em tabelas, apresentados nessa seção.

3.1.1 Facilidade de Download

Para a classificação das ferramentas nesse quesito, foi verificado a quantidade de cliques necessários para chegar até o download da mesma. E, para avaliação, foi utilizada a escala conforme apresenta a Figura 11.

Figura 11 - Tabela avaliativa facilidade de download.

Facilidade download	
Quantidade de Cliques	**Nota**
<= 3	4
4 a 6	3
7 a 9	2
10 a 12	1
> 12	0

Fonte: Elaborada pelo autor.

3.1.2 Documentação Acessível

Para avaliar a disponibilidade da documentação, considerou-se a língua em que a mesma fora escrita bem como a maneira como foi explícito o conteúdo. Sendo assim, foi estabelecida as métricas de acordo com a Figura 12.

Figura 12 - Tabela avaliativa documentação acessível.

Documentação acessível				
Português	**Inglês**	**Conteúdo explicito**	**Falta informação**	**Nota**
X		X		4
	X	X		3
X			X	2
	X		X	1
				0

Fonte: Elaborada pelo autor.

3.1.3 Facilidade de Implementação

Nesse quesito, foi avaliado somente o modo de configuração de novos dispositivos na rede, utilizando o ambiente da ferramenta. Portanto, estabeleceu-se a avaliação, conforme ilustra a Figura 13.

Figura 13 - Tabela avaliativa facilidade de implementação.

Facilidade de implementação		
Ambiente gráfico/ilustrativo	**Ambiente menos ilustrativo**	**Nota**
X		4
	X	3

Fonte: Elaborada pelo autor.

3.1.4 Disponibilidade em diferentes plataformas

Foi considerado para avaliação nesse quesito, a possibilidade de implementação do servidor da ferramenta em plataformas Linux e/ou Windows. Sendo assim, o critério de avaliação foi definido de acordo com a Figura 14.

Figura 14 - Tabela avaliativa diferentes plataformas.

Disponibilidade em diferentes plataformas				
Linux	**Windows**	**Linux Via Wine**	**Linux Ou Windows**	**Nota**
X	X			4
	X	X		3
			X	2
		X		1
				0

Fonte: Elaborada pelo autor.

3.1.5 Interface amigável

Para a avaliação da interface, foi considerado a interface em si da ferramenta, de acordo com sua disposição dos elementos, e a forma lógica de utilização da mesma. Portanto, foi estabelecido o critério de avaliação conforme mostra a Figura 15.

Figura 15 - Tabela avaliativa interface amigável.

Interface amigável				
Ambiente gráfico/ilustrativo	**Ambiente menos ilustrativo**	**Sequência lógica**	**Sem sequência lógica**	**Nota**
X		X		4
	X	X		3
X			X	2
	X		X	1
				0

Fonte: Elaborada pelo autor.

3.1.6 Busca Automática dos Dispositivos

Nesse quesito, foi avaliada a disponibilidade de utilização da busca automática de novos dispositivos da rede, como também a possibilidade de criação de regras de auto busca, avaliadas conforme demonstra a Figura 16.

Figura 16 - Tabela avaliativa busca automática dos dispositivos.

Busca automática dispositivos da rede			
Busca automática	**Regras auto busca**	**Busca via Plugin**	**Nota**
X	X		4
X			3
	X	X	2
		X	1
			0

Fonte: Elaborada pelo autor.

3.1.7 Mapa da Rede

Para avaliação desse elemento, utilizou-se a Figura 17, onde verificou-se a possibilidade de criação do mapa da rede, além da forma como se apresenta, de maneira estática, apenas visualização da rede fisicamente, e dinâmica, com a atualização dos estados dos dispositivos.

Figura 17 - Tabela avaliativa mapa da rede.

Mapa da Rede				
Mapa	**Dinâmico**	**Mapa via Plugin**	**Estático**	**Nota**
X	X			4
X			X	3
	X	X		2
		X	X	1
				0

Fonte: Elaborada pelo autor.

3.1.8 Diversidade dos meios de notificação

Nesse quesito, foram avaliados os diferentes tipos de notificações possíveis, sendo estas as responsáveis pelo alerta ao administrador da rede as eventuais mudanças de estados dos dispositivos. Apresenta-se, na Figura 18, a forma de avaliação do item.

Figura 18 - Tabela avaliativa meios de notificação.

Diversidade meios de notificação	
Tipos diferentes	**Nota**
> =4	4
3	3
2	2
1	1
0	0

Fonte: Elaborada pelo autor.

3.1.9 Diversidade dos relatórios

De acordo com a Figura 19, a diversidade dos relatórios foi avaliada considerando os tipos de gráficos que podem ser gerados de acordo com cada ferramenta, além de ser considerada a possibilidade de detalhamento do dado obtido em determinado dia e horário.

Figura 19 - Tabela avaliativa meios de notificação.

Relatórios			
Tipos diferentes >= 2	**Tipos diferentes < 2**	**Zoom detalhado**	**Nota**
X		X	4
X			3
	X	X	2
	X		1
			0

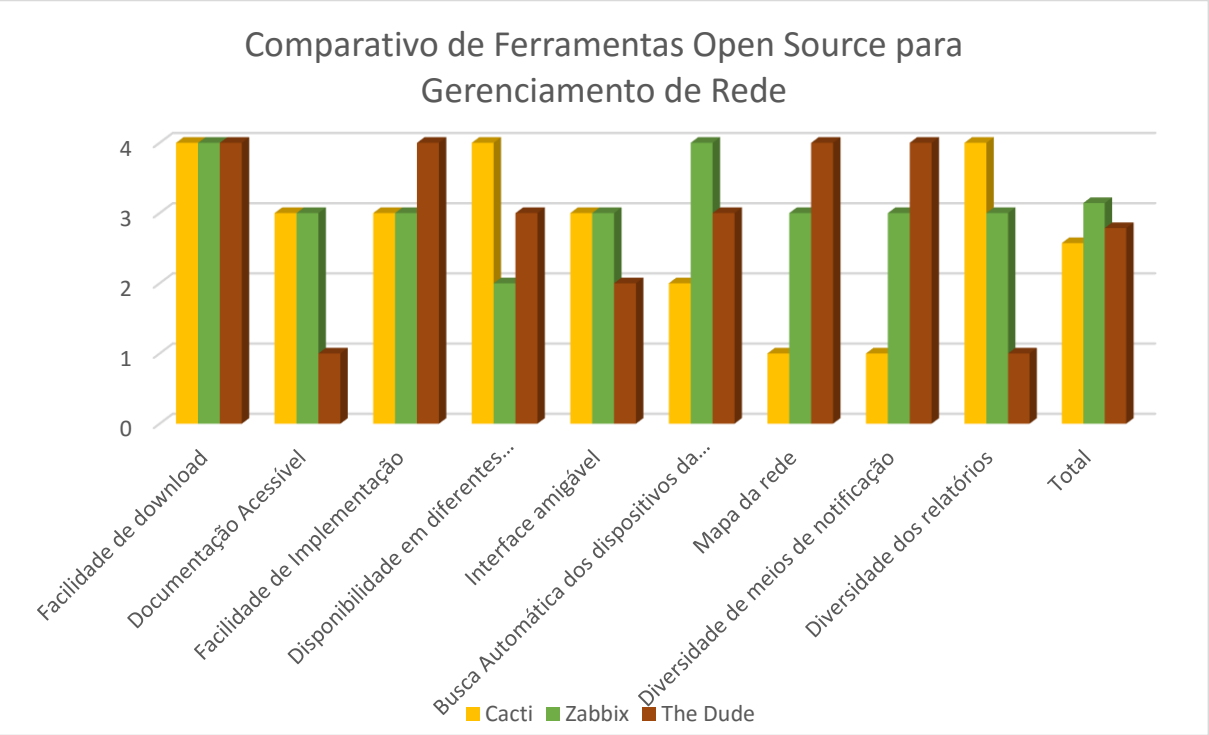
Fonte: Elaborada pelo autor.

4 RESULTADOS

Após a instalação e configuração das ferramentas para gerenciamento de rede, as mesmas foram avaliadas de acordo com cada quesito pré-estabelecido, sendo que obtiveram sua nota variada de 0 a 4. Sendo assim, pode-se perceber que as ferramentas obtiveram um desempenho equilibrado em sua totalidade.

A Figura 20 representa as notas obtidas em cada quesito de acordo com cada ferramenta.

Figura 20 - Comparativo das Ferramentas Open Source.



Fonte: Elaborada pelo autor.

Portanto, observa-se que as ferramentas Cacti e The Dude foram avaliadas praticamente com a mesma nota após a consideração de todos os quesitos. Já a ferramenta Zabbix, obteve uma pequena variação e se sobressaiu frente as demais.

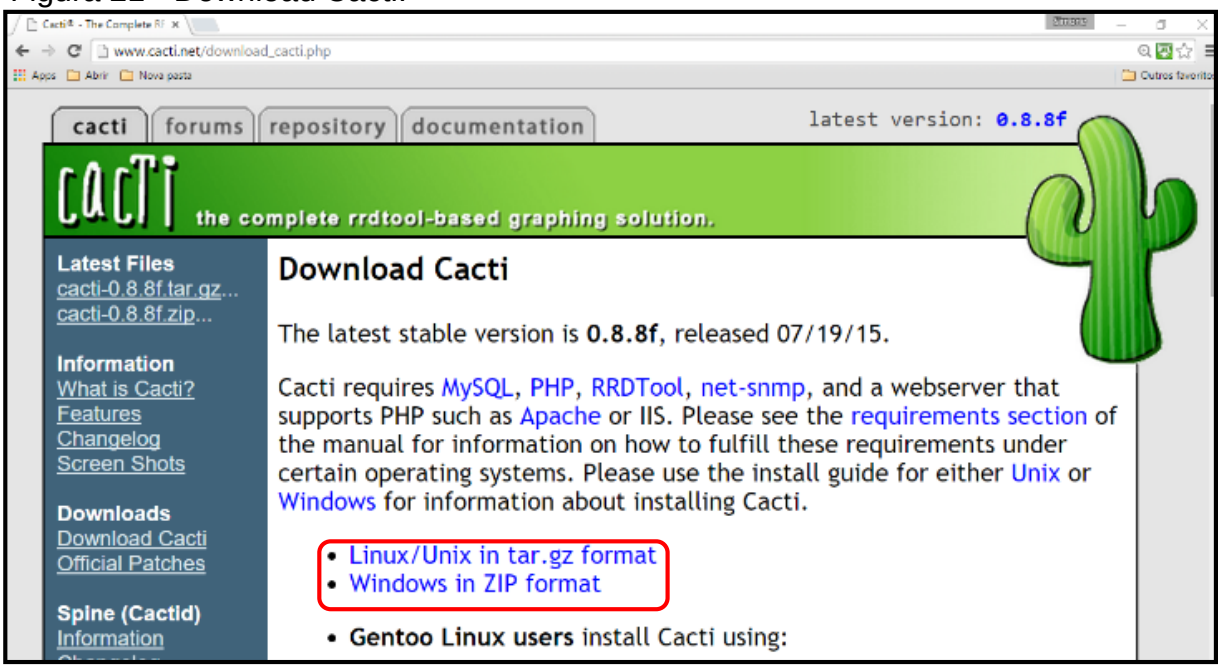
Apresenta-se nos tópicos a seguir as principais considerações de cada ferramenta de acordo com cada quesito avaliado.

4.1 FACILIDADE DE DOWNLOAD

Todas as ferramentas utilizadas possuem a disponibilidade do download da ferramenta no próprio site do fornecedor, sendo assim, consegue-se navegar até a página de download e, através no link disponível, obter a mesma.

Na Figura 21, observa-se a localização do download da ferramenta Cacti.

Figura 21 - Download Cacti.



Fonte: Cacti (c2004-2012). Adaptada pelo autor.

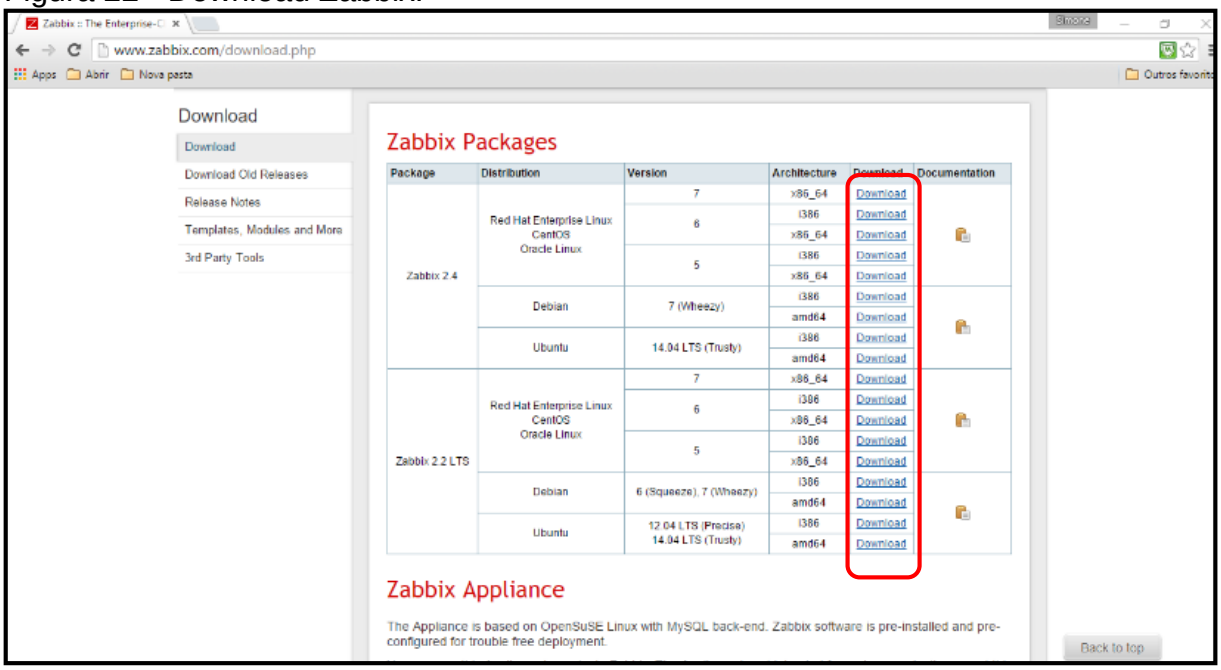
Estão disponíveis para download a versão para Linux e também para Windows, sendo que o tamanho da versão para Linux é de 2,5MB.

Foi utilizado, porém, o download da ferramenta via terminal com o seguinte comando:

apt-get install cacti

Na Figura 22, ilustra-se a página de download da ferramenta Zabbix, sendo que seus pacotes estão disponíveis para distribuições Linux, entre delas, CentOS, Debian e Ubuntu.

Figura 22 - Download Zabbix.



Fonte: Zabbix (2015). Adaptada pelo autor.

Pode-se também perceber que cada download está relacionado, além de sua distribuição, com a arquitetura com a qual a ferramenta será vinculada.

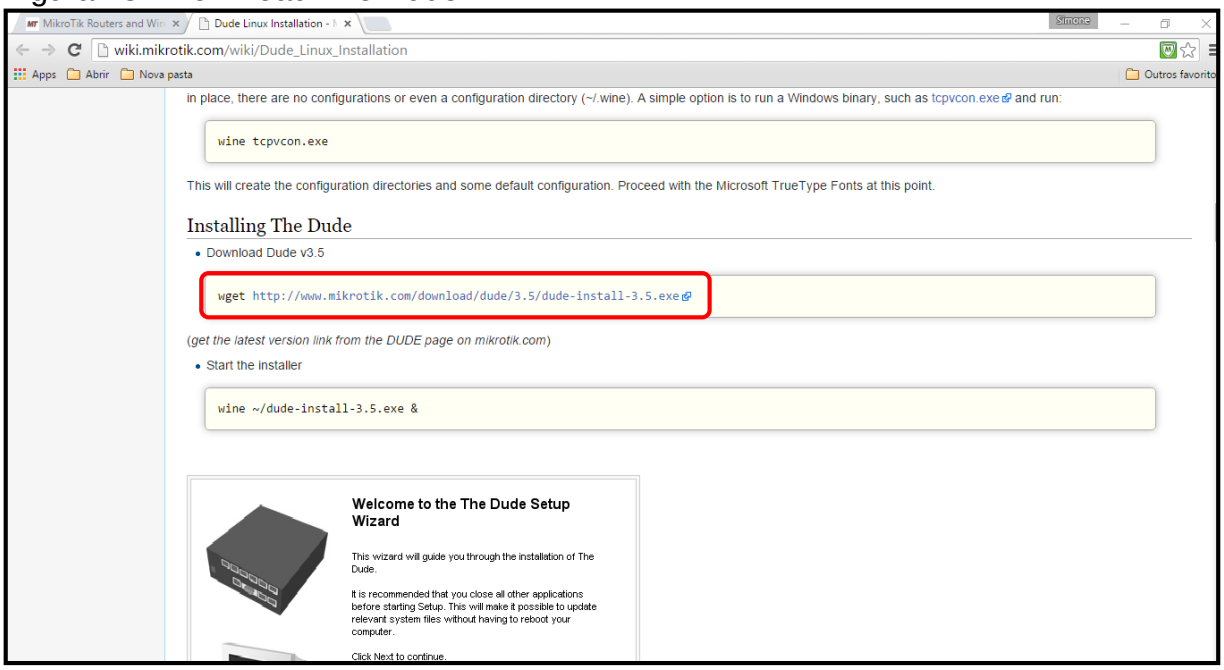
Porém, o seu download também foi concluído via terminal, através do seguinte comando:

wget http://repo.zabbix.com/zabbix/2.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_2.4-1+trusty_all.deb

A ferramenta The Dude, por ser implementada em ambiente Linux via Wine, conta com único link para download, já que o mesmo será indiferente as plataformas devido o modo de instalação. O arquivo para download dispõe-se de um tamanho também pequeno, cerca de 3,5 MB.

Detalha-se portanto, na Figura 23, o link disponível para download da ferramenta The Dude.

Figura 23 - Download The Dude.



Fonte: Mikrotik ([2015?]). Adaptada pelo autor.

Para a conclusão do download, foi utilizado exatamente o mesmo comando no terminal que encontra-se ressaltado:

wget http://www.mikrotik.com/download/dude/3.5/dude-install-3.5.exe

Portanto, pelo fato de que as ferramentas puderam ser obtidas através de comandos via terminal, ou utilizando no máximo 3 cliques navegando em sua própria página, além de possuírem um tamanho razoável, todas foram avaliadas nesse quesito com nota 4.

4.2 DOCUMENTAÇÃO ACESSÍVEL

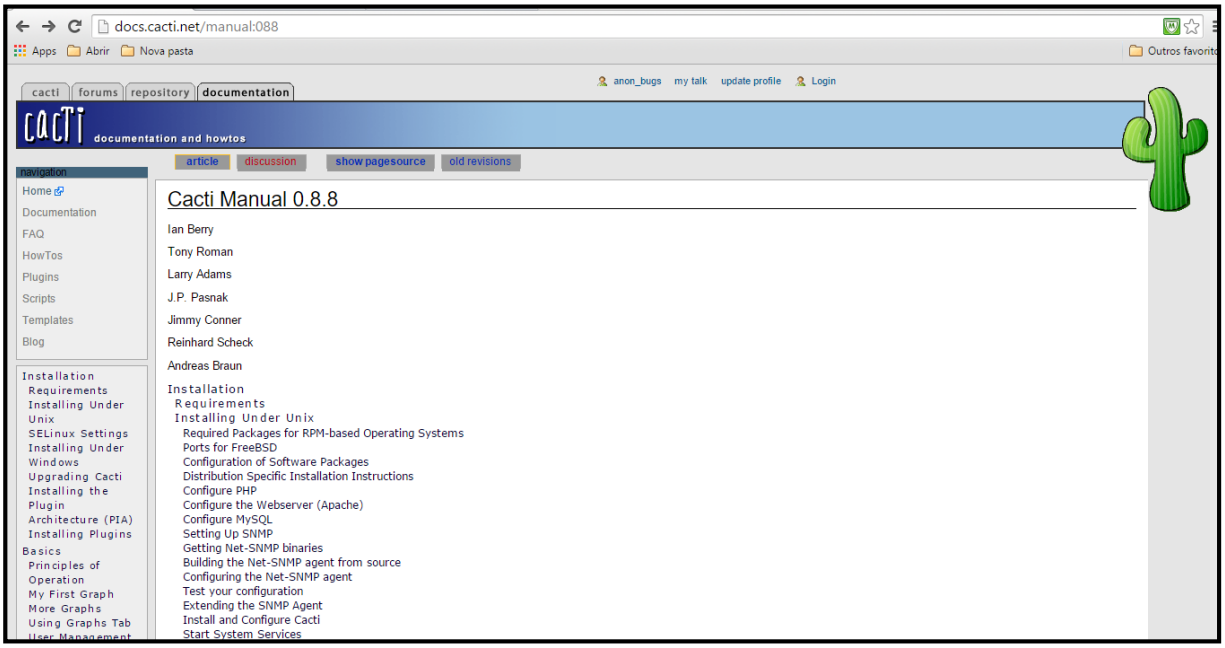
Considerando-se o quesito referente a documentação de cada ferramenta, todas disponibilizam a mesma no próprio site, fazendo com que a instalação e configuração se tornem mais claras.

As ferramentas Cacti, Zabbix discorrem seus conteúdos e aplicações de maneira objetiva, porém, obtiveram a nota 3, pois o Cacti somente disponibiliza a

documentação em versão inglês e o Zabbix, oferece a documentação em português desatualizada.

Na Figura 24, observa-se a página onde a documentação do Cacti está disponível.

Figura 24 - Documentação Cacti.



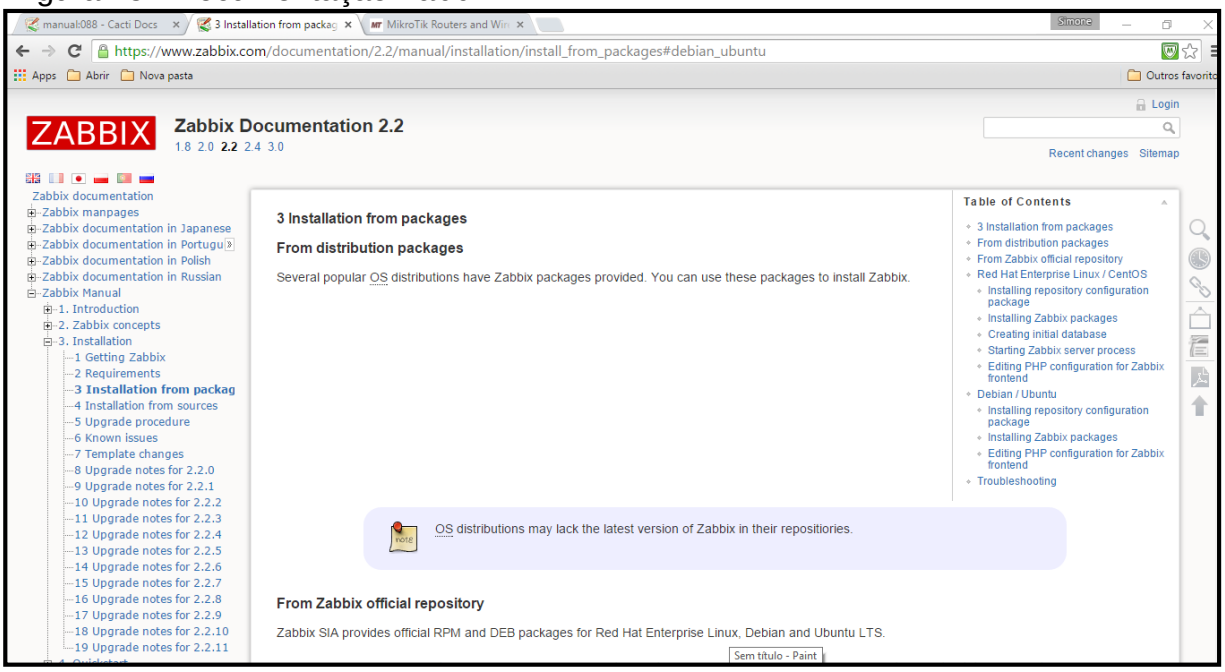
Fonte: Cacti (c2004-2012).

Dentre os tópicos disponíveis da documentação da ferramenta, pode-se consultar desde a instalação e configuração dos seus pré-requisitos, sua configuração básica, além dos tópicos avançados, onde inclui-se a criação de scripts para a recuperação de dados utilizando códigos customizados, como a elaboração de um script utilizando o protocolo ICMP para medir o tempo de uma solicitação ping além de sua disponibilidade.

Considerando a ferramenta Zabbix, sua documentação está disponível de maneira íntegra, sendo que cada aplicação da ferramenta é demonstrada através de exemplos.

Na Figura 25, está demonstrado um trecho da documentação da ferramenta Zabbix.

Figura 25 - Documentação Zabbix.



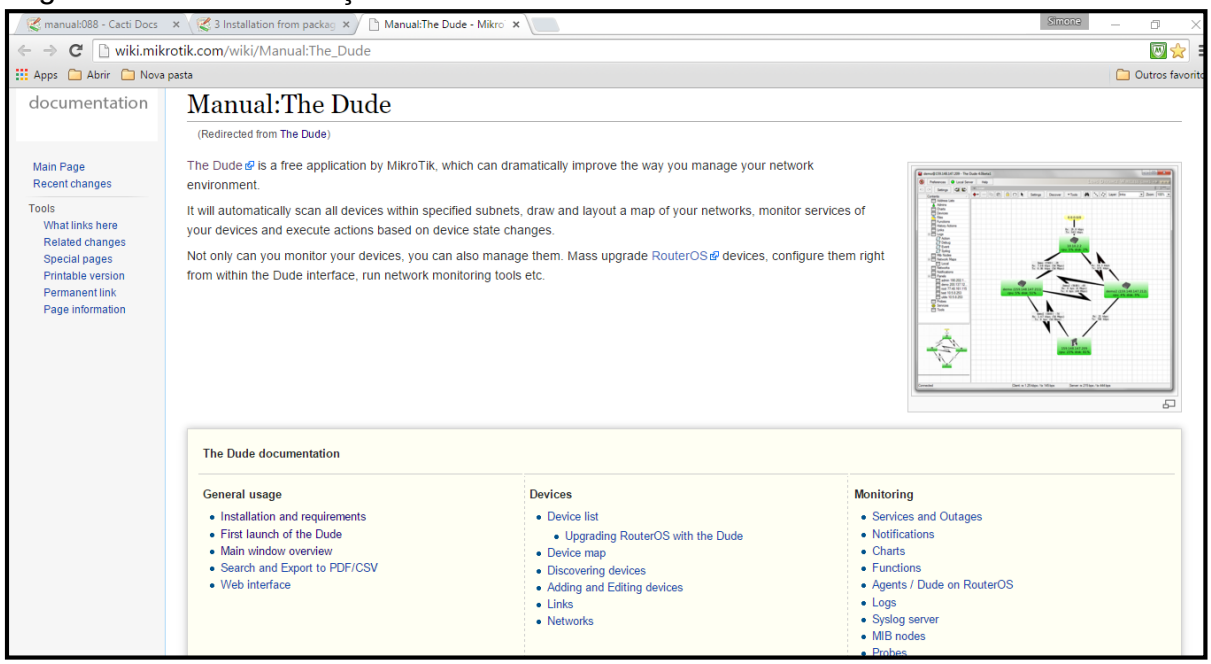
Fonte: Zabbix (2015).

Já a ferramenta The Dude, obteve nesse quesito a nota 1, pois existem funcionalidades da ferramenta que não estão bem definidas e explicadas, como no caso das Probes, onde existe uma explicação sobre o que seria, porém as formas de implementá-la não são tão explícitas, além de toda documentação também estar somente na versão em inglês.

Sua documentação está agrupada com uma visão geral da ferramenta e sua instalação, inclusão dos dispositivos, monitoração, além de configurações de usuários e ferramentas de integração, como o Winbox.

Observa-se, na Figura 26, o manual online disponível pela ferramenta The Dude.

Figura 26 - Documentação The Dude.



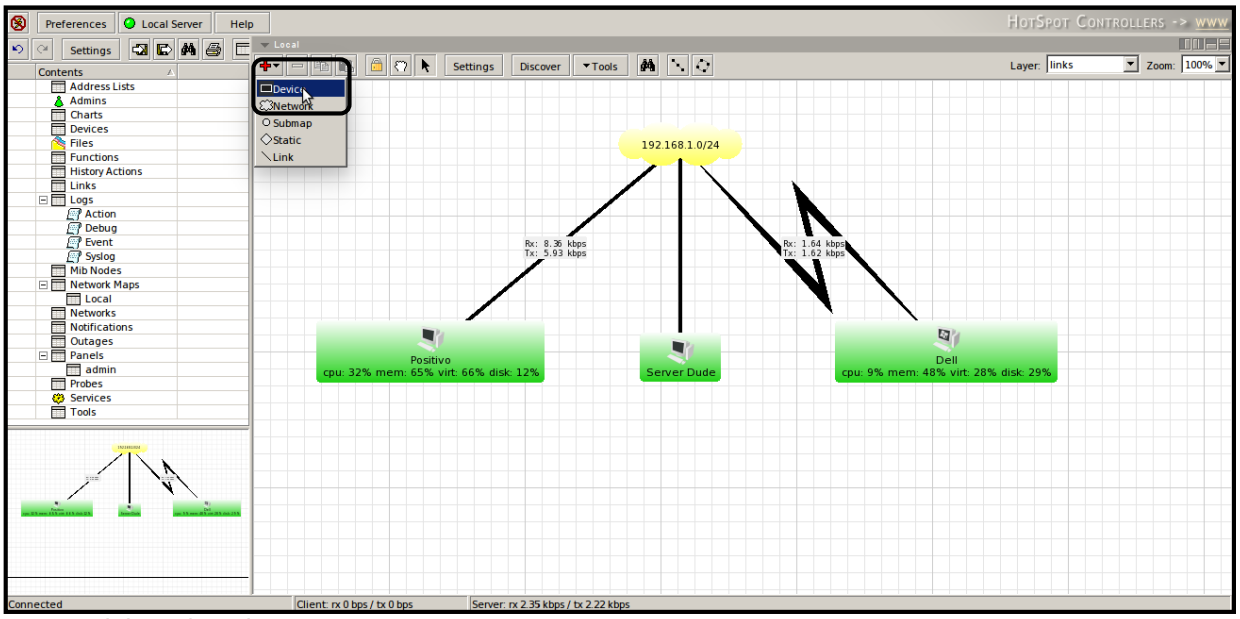
Fonte: Mikrotik ([2015?]).

4.3 FACILIDADE DE IMPLEMENTAÇÃO

Em relação a esse quesito, a ferramenta de destaque foi o The Dude, com nota 4, por apresentar um ambiente mais gráfico e ilustrativo, sua implementação fica subentendida. Em comparação a essa ferramenta, Cacti e Zabbix obtiveram nota 3, a implementação das mesmas não são tão simples quanto, porém também apresentam um alto nível de dificuldade para serem implementadas, já que utilizam praticamente os mesmos conceitos.

Como pode ser verificado na Figura 27, para adicionar o novo dispositivo no The Dude, basta apenas clicar no “+” e selecionar Device.

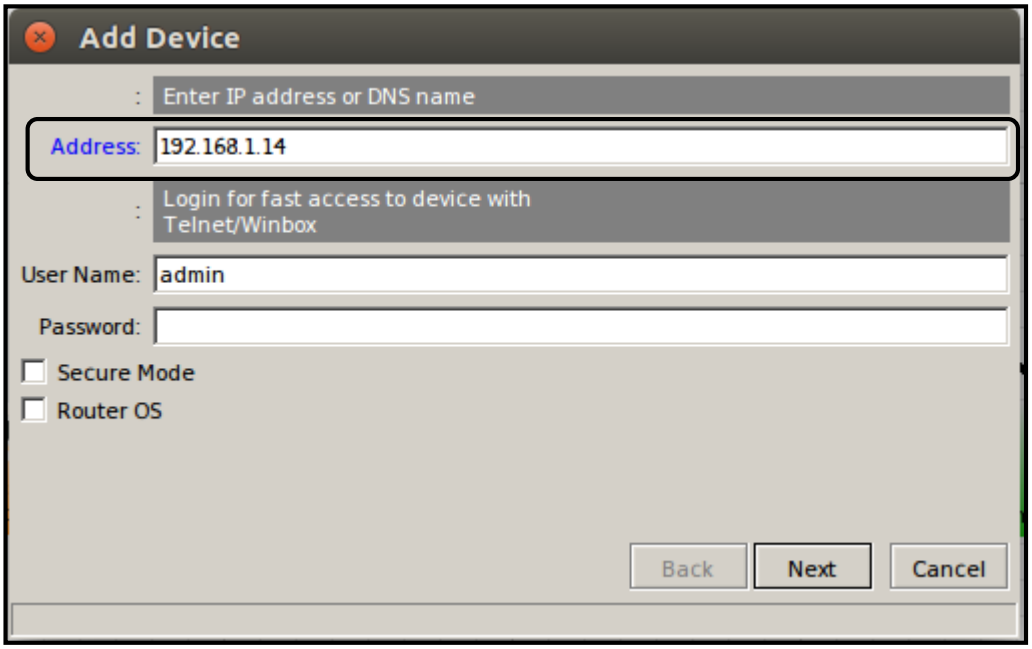
Figura 27 - Novo dispositivo The Dude.



Fonte: Elaborada pelo autor.

Na próxima janela, basta digitar o endereço de IP do equipamento ou o seu domínio, como pode ser observado na Figura 28.

Figura 28 - Adicionando dispositivo The Dude.

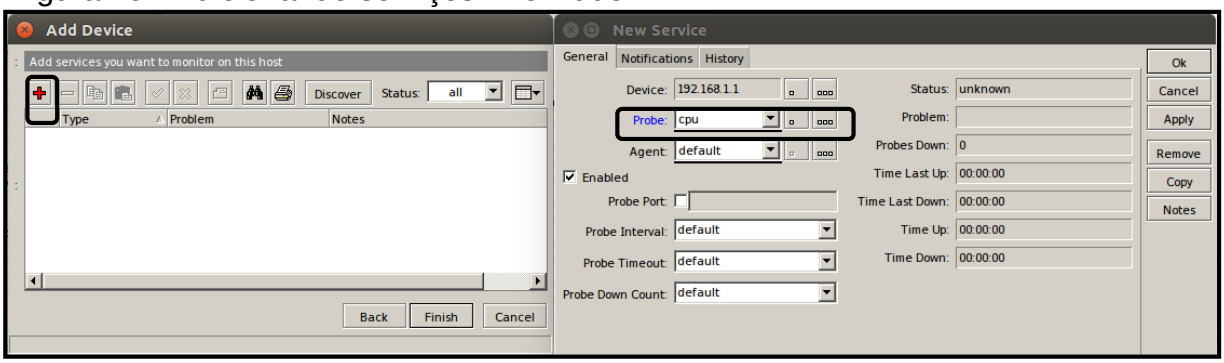


Fonte: Elaborada pelo autor.

Caso esteja adicionando algum dispositivo do fabricante Mikrotik, é interessante acrescentar o nome de usuário e senha pois assim, pode ser facilmente utilizada a ferramenta Winbox, por exemplo, apenas dando um clique com o botão direito e selecionando a ferramenta.

Na próxima tela é possível acrescentar os serviços que serão monitorados, primeiramente clica-se na “+”, e na janela seguinte, seleciona qual o serviço desejado, como pode ser constatado na Figura 29.

Figura 29 - Adicionando serviços The Dude.



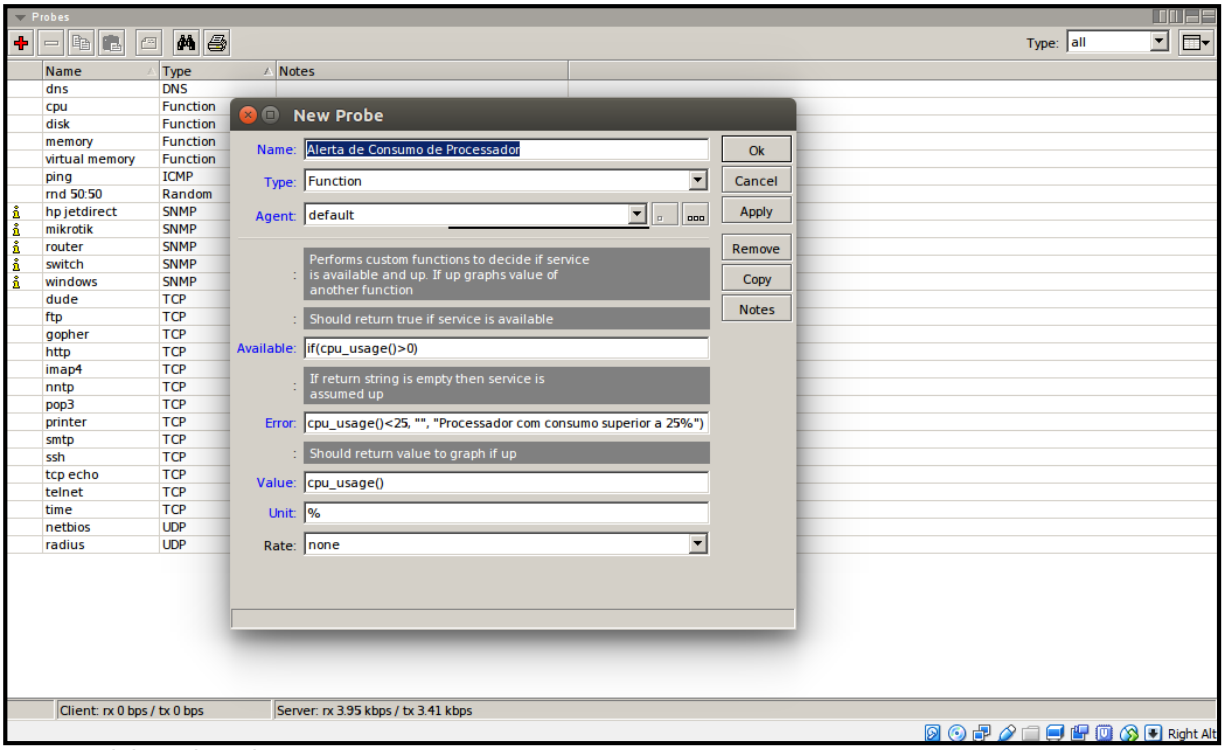
Fonte: Elaborada pelo autor.

Também é possível selecionar um agente, especialmente utilizado quando se deseja monitorar mais de uma rede que não estão num mesmo local físico, quando não selecionado, fica-se como default. Pode-se alterar o tempo de intervalo de pesquisa de dispositivos (Prove Interval), o tempo que deve passar para que o status do serviço fique como timeout (Probe Timeout) e número de vezes em que deve haver falha para um serviço ser considerado indisponível (Probe Down). Por default, essas variáveis assumem os seguintes valores, 30 segundos, 10 segundos e 5, consecutivamente.

Existe a possibilidade de se criar regras de alertas para que os mesmos sejam disparados de acordo com uma condição pré-estabelecida.

Na Figura 30, constata-se a criação de uma função para a definição de um alerta caso o processor atinja um valor acima de 25%, sendo que o valor foi estabelecido para verificar se o serviço realmente seria acionado ao passar dessa porcentagem, já que o processamento do computador em questão estava em torno de 28%. Essa Probe, equivalente a um serviço a ser gerenciado, precisa ser adicionada ao dispositivo desejado para que se tenha efeito.

Figura 30 - Adicionando Probe The Dude.



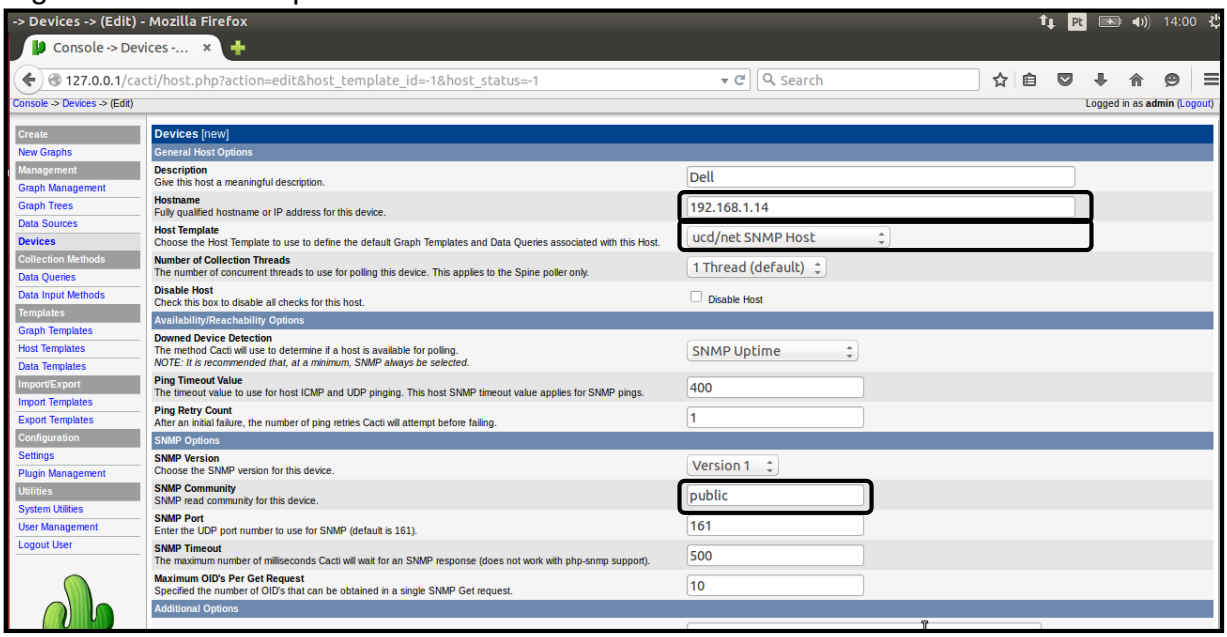
Fonte: Elaborada pelo autor.

Considerando-se a ferramenta Cacti, a adição de novos dispositivos é feita de maneira sequencial, adiciona-se um novo dispositivo, acrescenta-se os dados que serão coletados e posteriormente cria-se o gráfico com tais dados.

Ao clicar em Devices, e em seguida add, será aberta uma janela, e nela, deverá ser especificado o endereço de IP ou nome do host e a forma como será feita a coleta dos dados, além da comunidade SNMP.

Observa-se, na Figura 31, as informações pertinentes para adicionar um novo dispositivo.

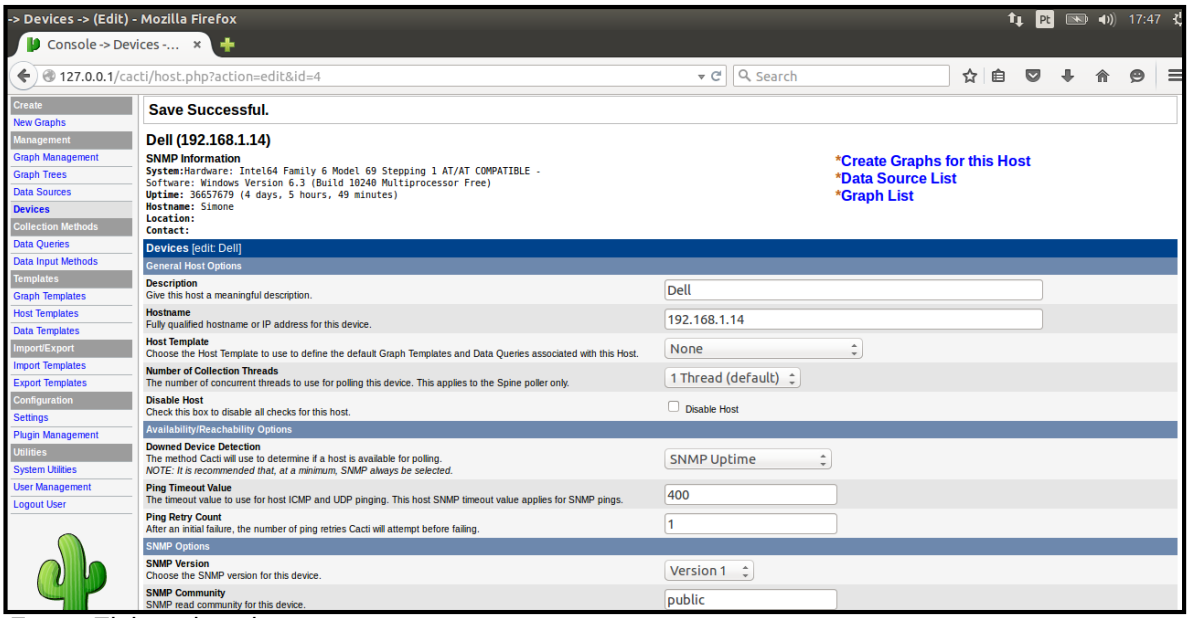
Figura 31 - Novo dispositivo Cacti.



Fonte: Elaborada pelo autor.

Finalizando essa etapa, clica-se no botão localizado no canto esquerdo inferior, Create, e aparecerá na parte superior da tela o retorno à consulta SNMP, conforme mostra a Figura 32.

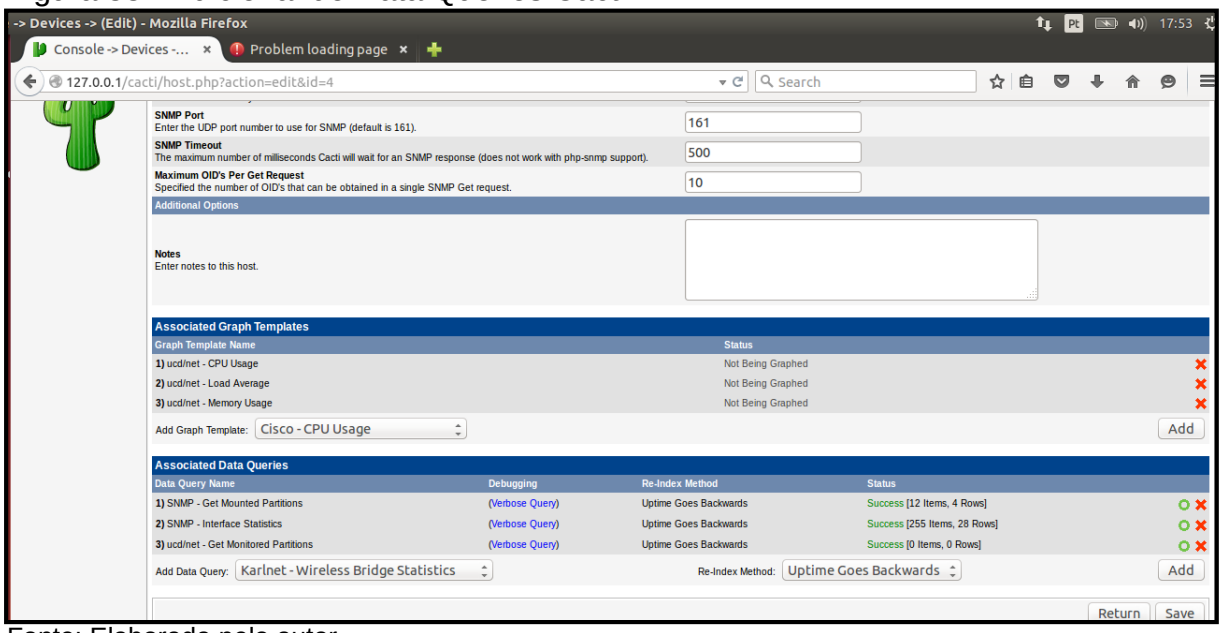
Figura 32 - Retorno à consulta SNMP.



Fonte: Elaborada pelo autor.

Ainda nessa tela, há a possibilidade de adicionar quais os dados que poderão ser associados, como pode ser verificado na Figura 33.

Figura 33 - Adicionando Data Queries Cacti.



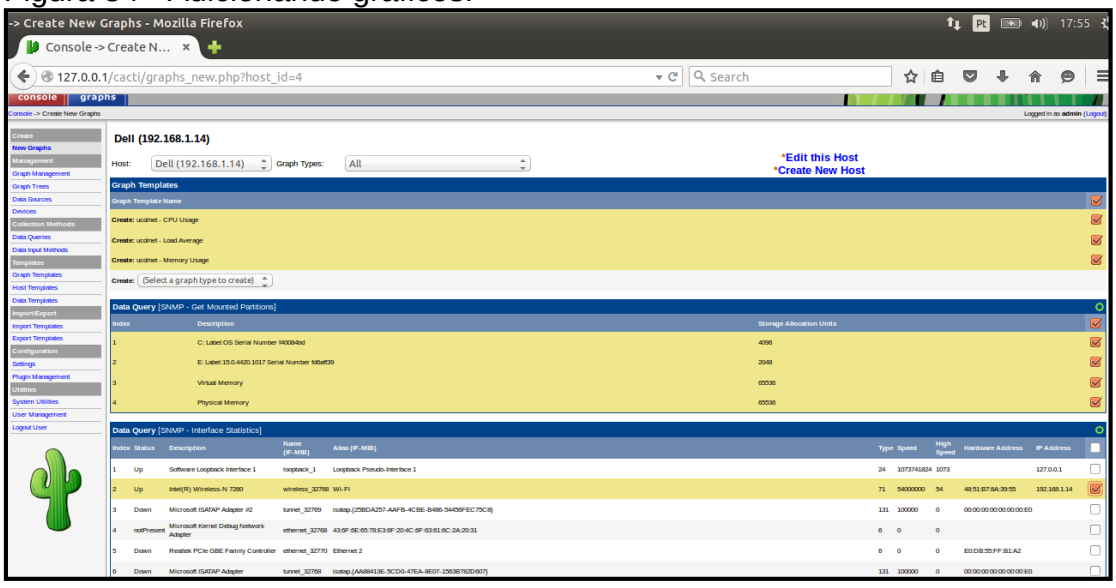
Fonte: Elaborada pelo autor.

Com os dados adicionados, SNMP – Get Mounted Partitions, SNMP – Interface Statistics e udc/net – Get Mounted Partitions, gráficos como, tráfego da placa de rede, e dados referente as partições de disco, já poderão ser montados.

Conforme exibe a Figura 34, os itens selecionados farão parte dos gráficos

.

Figura 34 - Adicionando gráficos.



Fonte: Elaborada pelo autor.

E, para adicionar um novo gráfico, basta clicar em Create Graphs for this host, e na tela seguinte foi selecionado a monitoração de memória, CPU e tráfego de rede.

Posteriormente, cria-se a árvore que será montada no campo de gráficos, onde, por critério de escolha e visibilidade, foram considerados os seguintes critérios:

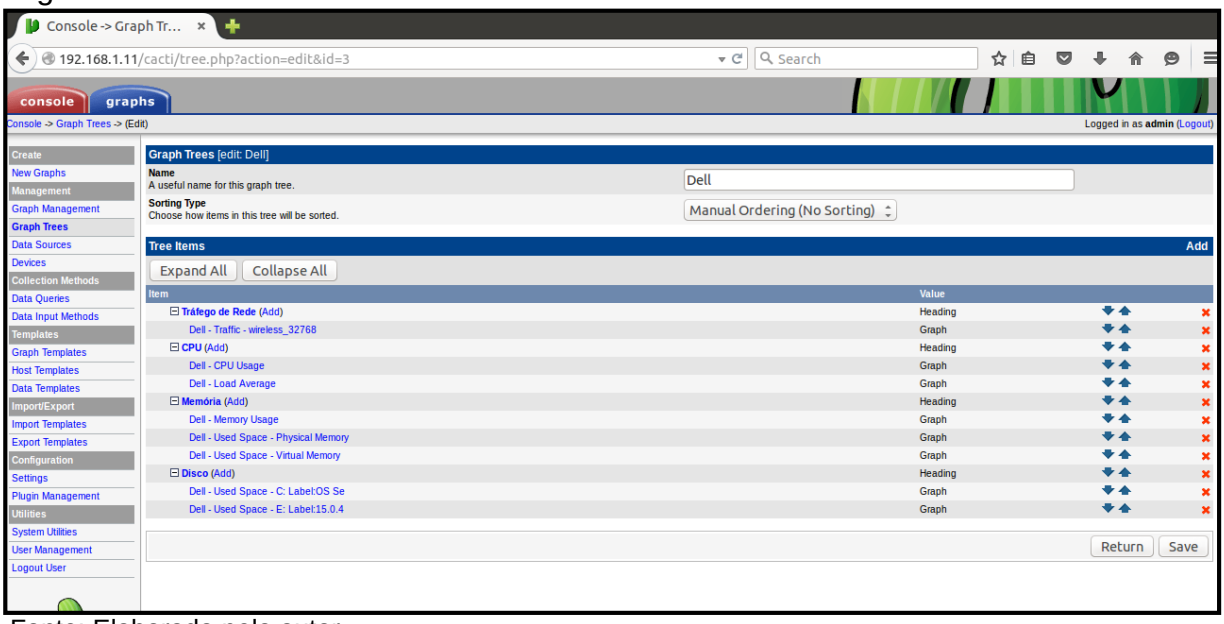
a) uma raiz para cada dispositivo;

b) dessa raiz origina-se os cabeçalhos;

c) dentro desses cabeçalhos estão os itens que serão monitorados.

Conforme Figura 35, existe uma árvore com o nome de um dos dispositivos, Dell, seguido dos cabeçalhos, tráfego de rede, cpu, memória e disco, e dentro de cada cabeçalho, seus próprios itens de monitoramento.

Figura 35 - Árvore de Gráficos.



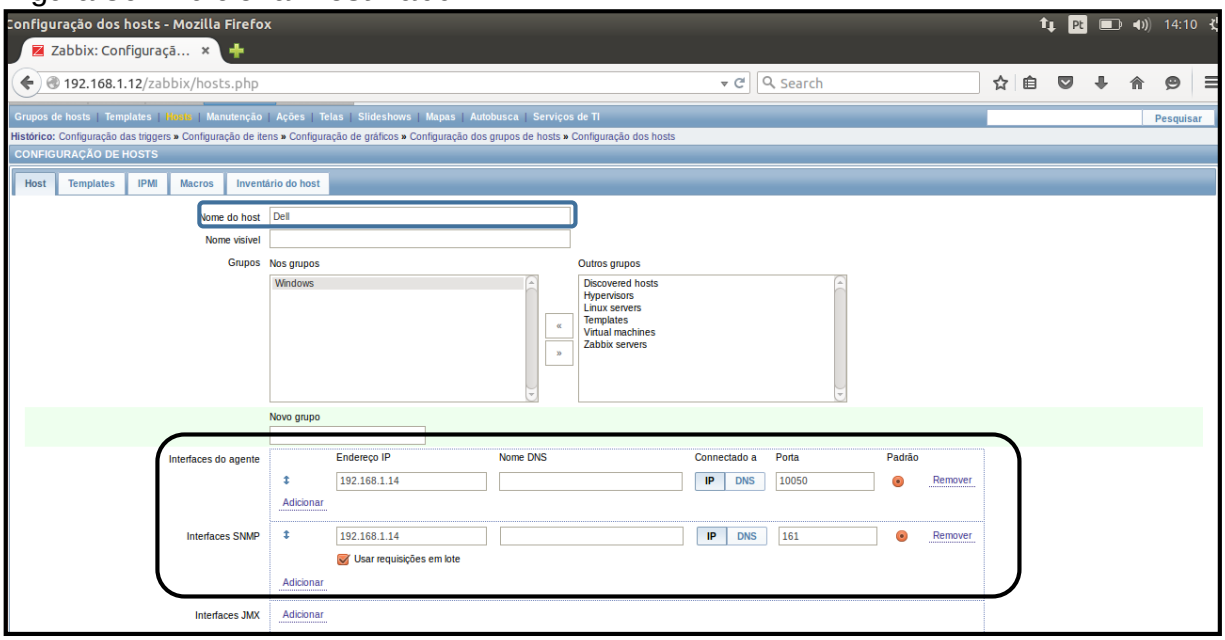
Fonte: Elaborada pelo autor.

Para se fazer um uso mais amplo do Cacti necessita-se a instalação de Plugins, como, por exemplo, o Thold, responsável pela notificação dos hosts off-line, o Weathermap, responsável pela geração do mapa da rede, como também o Monitor, responsável pela classificação dos estados dos hosts.

Já a ferramenta Zabbix, onde sua utilização é bem parecida com o Cacti, a configuração de seus dispositivos também é feita de maneira sequencial. Sendo assim, ao clicar na aba configuração e em seguida hosts, pode-se adicionar um novo dispositivo clicando na parte superior esquerda em Criar host.

Será aberta em seguida a tela de configuração de host, de acordo com a imagem apresentada na Figura 36.

Figura 36 - Adicionar host Zabbix.



Fonte: Elaborada pelo autor.

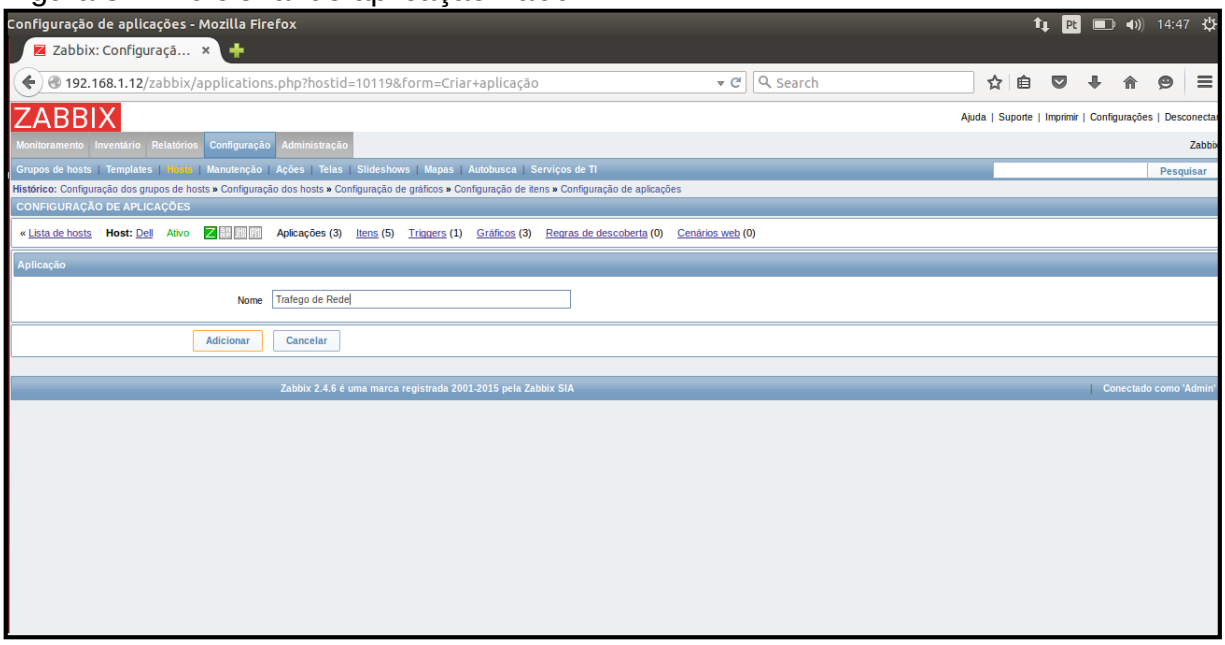
Assim como nas outras ferramentas, o importante dessa etapa e dar um nome ao host e especificar o seu endereço de IP, além de adicionar a interface do agente e/ou SNMP.

Seguindo as abas, pode-se associar o host a um Template pré-definido, como por exemplo o do Windows, onde ele mesmo já deixa estabelecido as aplicações, itens e até mesmo alguns gráficos. Essa opção porém, é opcional. Pode-se também, portanto, estabelecer manualmente as métricas desejadas. Posteriormente, basta clicar em Adicionar, no inferior da tela.

Após adicionar o host, são necessárias as alterações em suas aplicações, nome genérico que irão receber os itens. Os itens são aqueles que realmente irão coletar os dados, de acordo com a chave utilizada.

Portanto, para criar uma nova aplicação, basta selecionar aplicação e clicar em Criar aplicação no canto superior esquerda. Ao realizar esse procedimento, será aberta uma tela, conforme mostra a Figura 37, onde deverá ser especificado o nome da aplicação.

Figura 37 - Adicionando aplicação Zabbix.



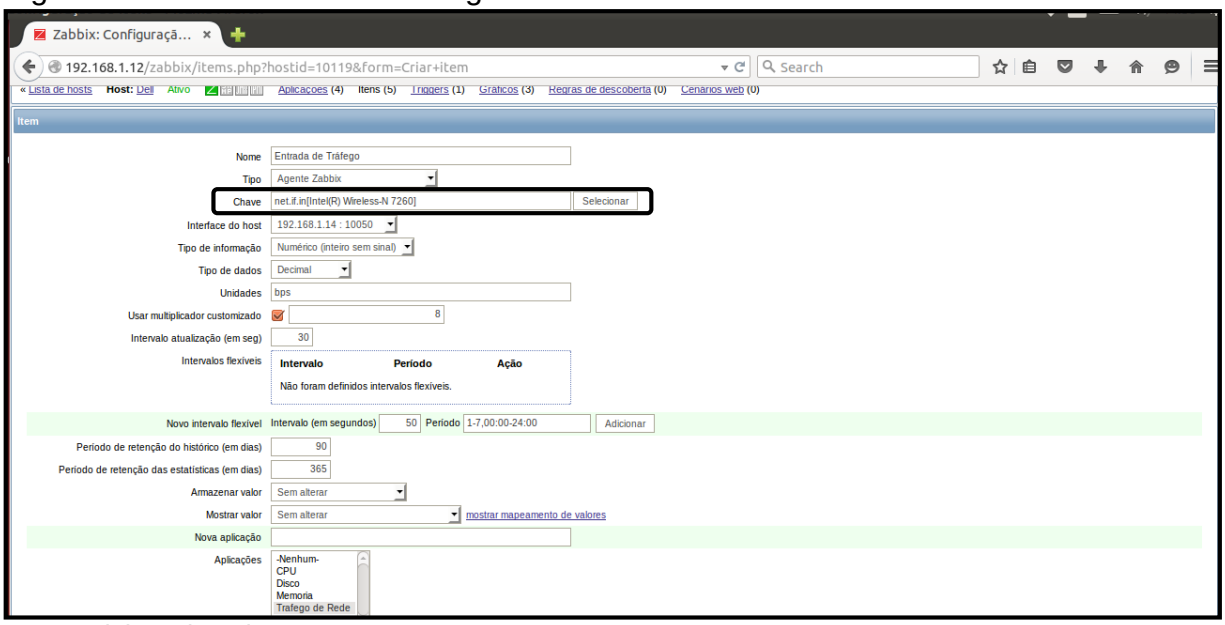
Fonte: Elaborada pelo autor.

Feito este procedimento, clicando em Adicionar, a aplicação já estará criada. Agora basta adicionar os itens dentro da aplicação. Como está sendo criada a aplicação Tráfego de Rede é importante colocar o item responsável pela identificação de entrada de dados pela placa, como também o de saída.

Conforme anteriores, clica-se na aba em que se deseja alterar e cria-se o objeto escolhido.

De acordo com a Figura 38, estabelece-se um novo item de Entrada de Tráfego.

Figura 38 - Item entrada de tráfego Zabbix.



Fonte: Elaborada pelo autor.

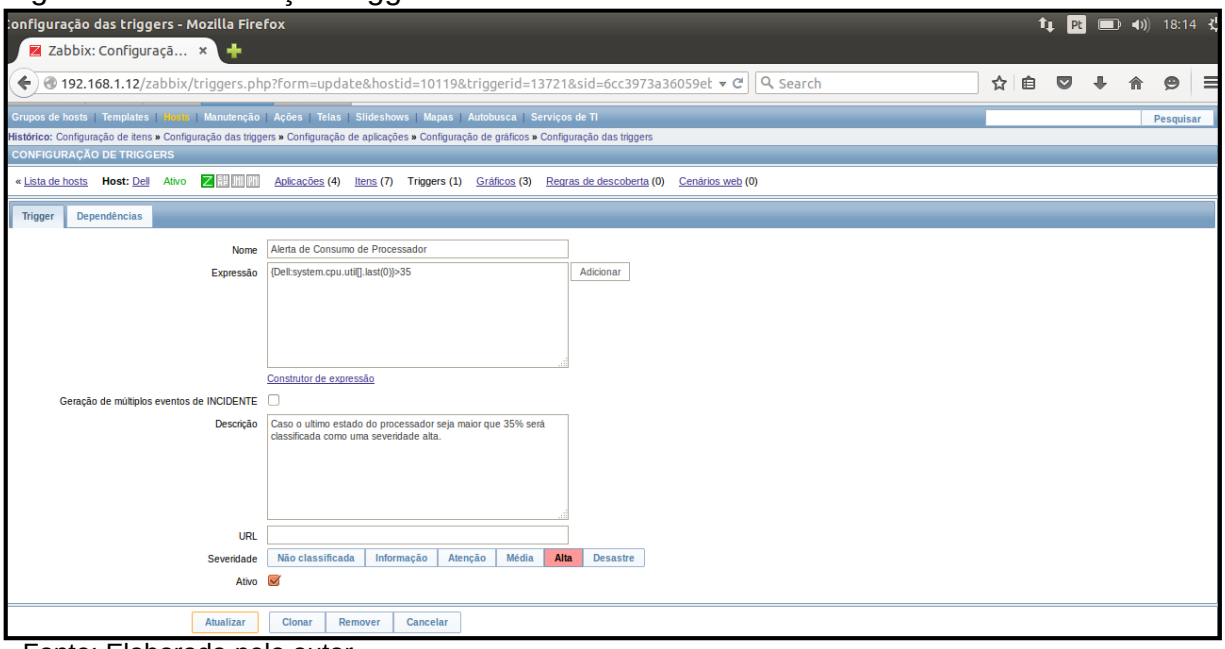
O mais importante ao criar um novo item é a seleção da chave, nesse caso foi utilizada a chave net.if.in[if,<mode>], onde se deve especificar dentro dos colchetes qual a placa de rede será monitorada.

A próxima etapa, em relação as Triggers, são expressões que podem ser geradas de acordo com alguma anormalidade que pode estar ocorrendo no sistema.

Pode-se verificar na Figura 39 a construção de uma trigger para o estado de um processador.

Nessa trigger criada, será classificada como alta severidade caso o processador assuma um valor acima de 35% da sua utilização, posteriormente pode-se criar uma ação quando ocorrer essa situação.

Figura 39 - Construção triggers Zabbix.

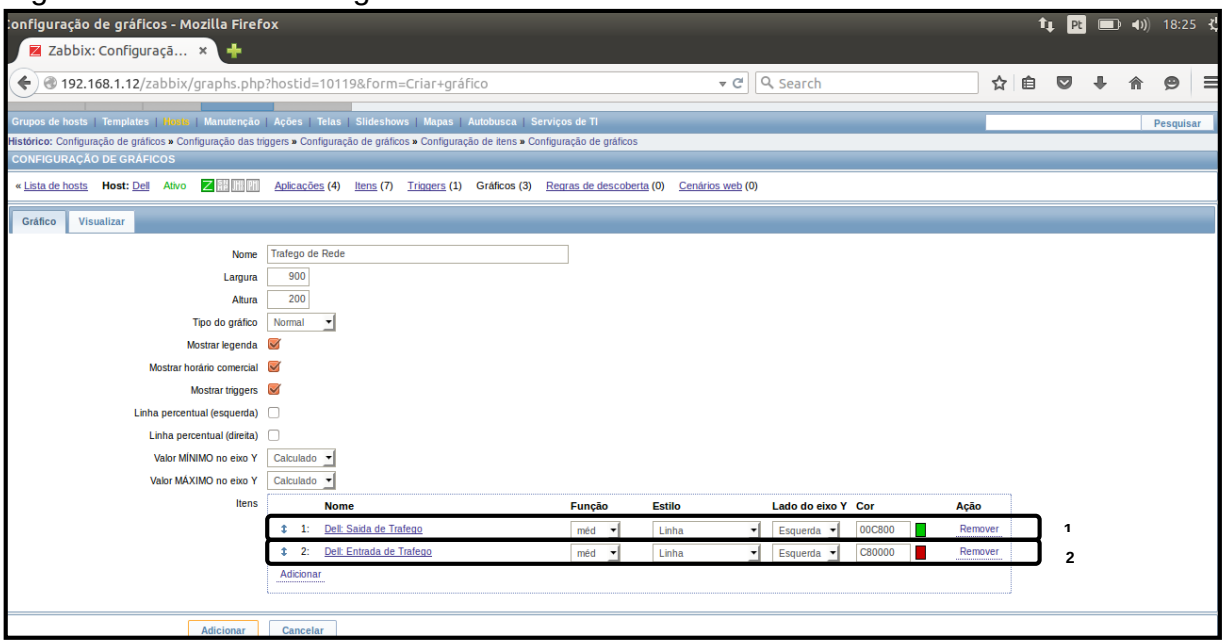


Fonte: Elaborada pelo autor.

Por fim, com os itens devidamente estabelecidos, pode-se criar os gráficos de monitoramento.

Conforme demonstra a Figura 40 é possível verificar a elaboração de um gráfico de tráfego de rede.

Figura 40 - Adicionando gráfico Zabbix.



Fonte: Elaborada pelo autor.

Nesse caso, o gráfico é composto por dois itens, o item 1 responsável pela coleta de dados de saída da placa de rede, já o item 2, pela entrada do tráfego na mesma.

4.4 DISPONIBILIDADE EM DIVERSAS PLATAFORMAS

Considerando o quesito de disponibilidade em diversas plataformas, a ferramenta de destaque foi o Cacti com nota 4. A ferramenta oferece download para as plataformas Linux/Unix como também para Windows.

A ferramenta The Dude, obteve nota 3, também oferece download para as plataformas Linux/Unix e Windows. Porém a versão para Linux/Unix roda a partir, de outra ferramenta, o Wine. Sendo assim, toda vez que se for utilizar a ferramenta The Dude no Linux, deverá ser via Wine.

Já o Zabbix, oferece download somente para a plataforma Linux em seus servidores, porém, seus agentes estão disponíveis em plataformas Linux/Unix e também Windows, portanto, nesse quesito, a ferramenta conquistou nota 2.

4.5 INTERFACE AMIGÁVEL

Considerando que interface amigável pode ser aquela em que o usuário se sente rapidamente adaptado para sua utilização, fazendo que com sua produtividade se torne rentável, a ferramenta The Dude obteve nota 2. Apesar de utilizar um ambiente mais gráfico e intuitivo, a ferramenta apresenta uma disposição dos elementos um tanto confusas.

Diferentemente da ferramenta anterior, Zabbix e Cacti utilizam uma sequência lógica, tomando por base a adição de novos dispositivos, sendo assim, o usuário sabe o próximo procedimento a ser feito assim que terminar a realização do anterior, porém sua interface não é tão gráfica quanto o The Dude, assim, foram avaliadas também com nota 3.

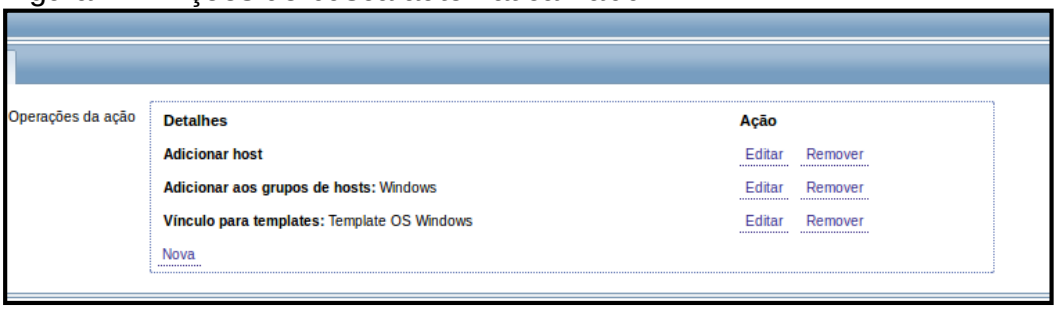
Para tanto, o nível de produtividade na utilização de qualquer uma das ferramentas está diretamente proporcional ao nível de conhecimento do usuário, sendo assim, um usuário totalmente leigo no assunto poderá encontrar maiores dificuldades na utilização das interfaces.

4.6 BUSCA AUTOMÁTICA DOS DISPOSITIVOS DA REDE

A busca automática dos dispositivos da rede faz com que a configuração da mesma se torne mais ágil. Sendo assim, a ferramenta Zabbix foi avaliada com nota 4 nesse quesito, pois com ela é possível a realização da busca de forma eficiente. Também existe a possibilidade de criação de regras de auto busca, onde pode-se especificar as ações que devem ser tomadas caso seja encontrado um tal dispositivo.

Na Figura 41 é possível verificar as ações criadas para a configuração de um novo dispositivo a partir da busca automática dos dispositivos.

Figura 41 - Ações de busca automática Zabbix.



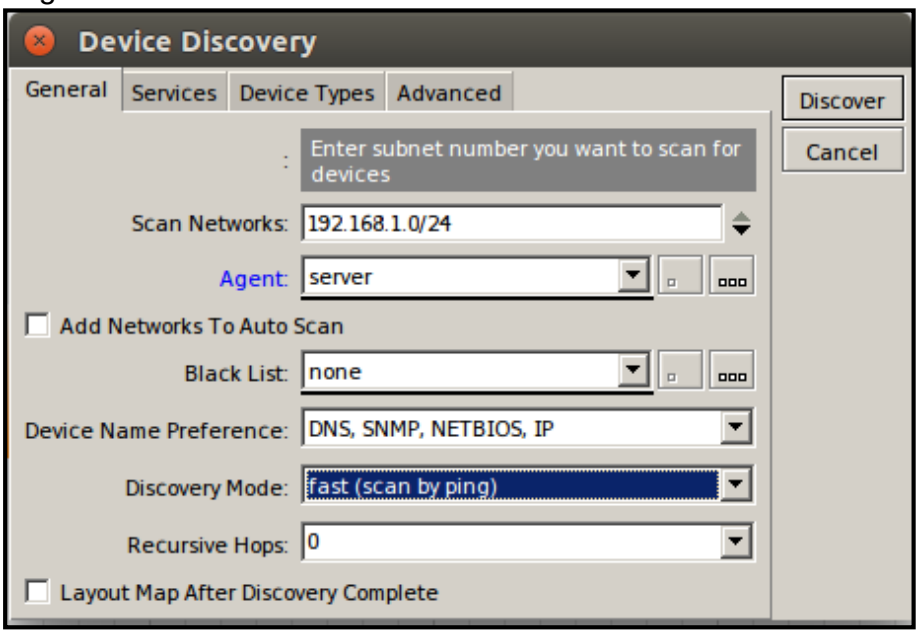
Fonte: Elaborada pelo autor.

Sendo assim, se for encontrado algum dispositivo que utilize o sistema operacional Windows, o mesmo será adicionado, inserido no grupo ‘Windows’, além de ser os templates associados, fazendo com que alguns os itens referentes a memória, processador, disco, sejam habilitados, como também as triggers e alguns gráficos pré-estabelecidos.

Já com a ferramenta The Dude, a busca automática não é composta de tanta flexibilidade, portanto obteve nota 3. É possível determinar quais os serviços serão buscados, de acordo com determinada faixa de IP.

Na Figura 42 ilustra-se a tela de configuração do auto discovery da ferramenta The Dude.

Figura 42 - Busca automática The Dude.



Fonte: Elaborada pelo autor.

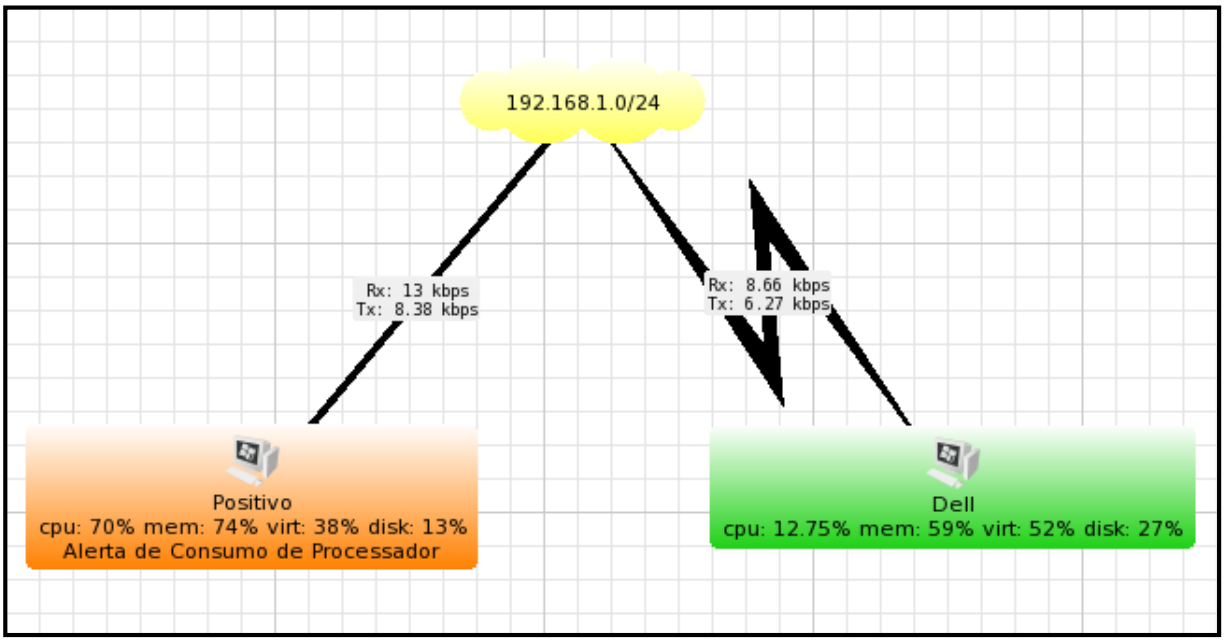
Após o término da busca, a ferramenta propõe um mapa da rede de acordo com os tipos dos dispositivos encontrados e a forma como se encontram interligados.

A ferramenta Cacti, obteve nesse quesito, a nota 2, pois só é necessária a utilização desse recurso através de um plugin chamado Discovery, onde o mesmo promove também regras de auto busca.

4.7 MAPA DA REDE

Ao avaliar as ferramentas nesse quesito, foi possível verificar que na ferramenta The Dude o mapa da rede é bem completo, pois, além de conseguir estruturar a sua rede dentro da ferramenta de forma como ela realmente é fisicamente, possui uma série de opções para facilitar a visibilidade das ocorrências da rede. Como pode ser observado na Figura 43, o mapa da rede é composto pelos elementos que estão sendo monitorados.

Figura 43 - Mapa da rede The Dude.



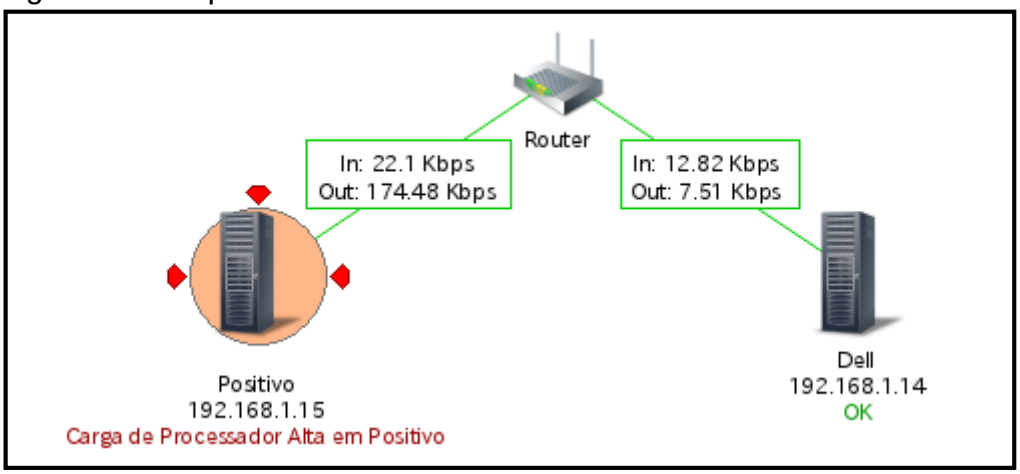
Fonte: Elaborada pelo autor.

Portanto, é possível verificar que além dos dispositivos monitorados, dados como cpu, memória, disco são demonstrados. Assim como a mudança de um estado, onde foi acionado o alerta de consumo de processador, pois seu consumo supera a porcentagem configurada (25%). Ainda é possível constatar o quanto está passando de banda em cada dispositivo. Sendo assim, a ferramenta foi avaliada com nota 4 nesse quesito, pois o mapa da rede é implementado com mais dinâmica.

Já a ferramenta Zabbix, alcançou na avaliação desse quesito, nota 3. É em possível a visualização estrutural da rede, também de forma dinâmica, porém a atualização de seus dados é mais lenta em comparação ao The Dude.

A Figura 44 apresenta o mapa da rede desenvolvido com a ferramenta Zabbix.

Figura 44 - Mapa da rede Zabbix.



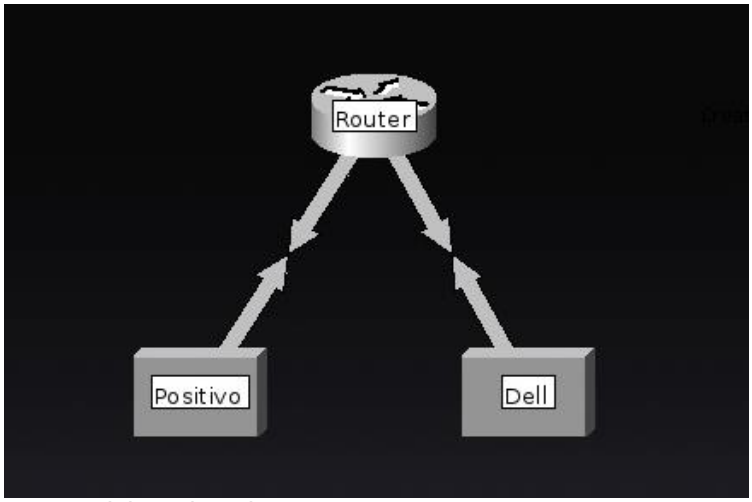
Fonte: Elaborada pelo autor.

Observa-se, portanto, o tráfego de rede de cada dispositivo, como também o acionamento da trigger relacionada a alta carga do processador.

Já a ferramenta Cacti, disponibiliza o plugin Weathermap para a elaboração do mapa da rede. Porém, a interface do mapa e sua implementação, em comparação as ferramentas anteriores, oferece margem às críticas. Sendo que a sua configuração através do editor web do plugin não apresenta suporte para a elaboração completa do mapa.

Pode-se observar, portanto, de acordo com a Figura 45 o mapa elaborado com o editor do Weathermap.

Figura 45 - Mapa da rede Weathermap – Cacti.



Fonte: Elaborada pelo autor.

Sendo assim, a nota do Cacti para esse quesito foi 1, onde pôde-se observar o mapa da rede de forma estática, onde os dispositivos estão interligados ao roteador.

4.8 DIVERSIDADE DOS MEIOS DE NOTIFICAÇÃO

Ao avaliar os diversos tipos de mídia de notificação, a ferramenta The Dude é a ferramenta que mais possui meios de notificação configurados, dentre eles, email, pop-up, importação de áudio e fala com a mudança de status do dispositivo, sendo assim, foi classificado com nota 4.

Já com a ferramenta Zabbix é possível o envio de notificações via SMS, email pré-configurado, além de notificações via criação de scripts customizados, portanto, a ferramenta obteve nota 3.

Para a configuração de envio de notificações pelo Cacti, é necessária a instalação de plugins. Sendo o plugin Thold responsável pelo envio das notificações via Email. Portanto, a ferramenta Cacti obteve nota 1.

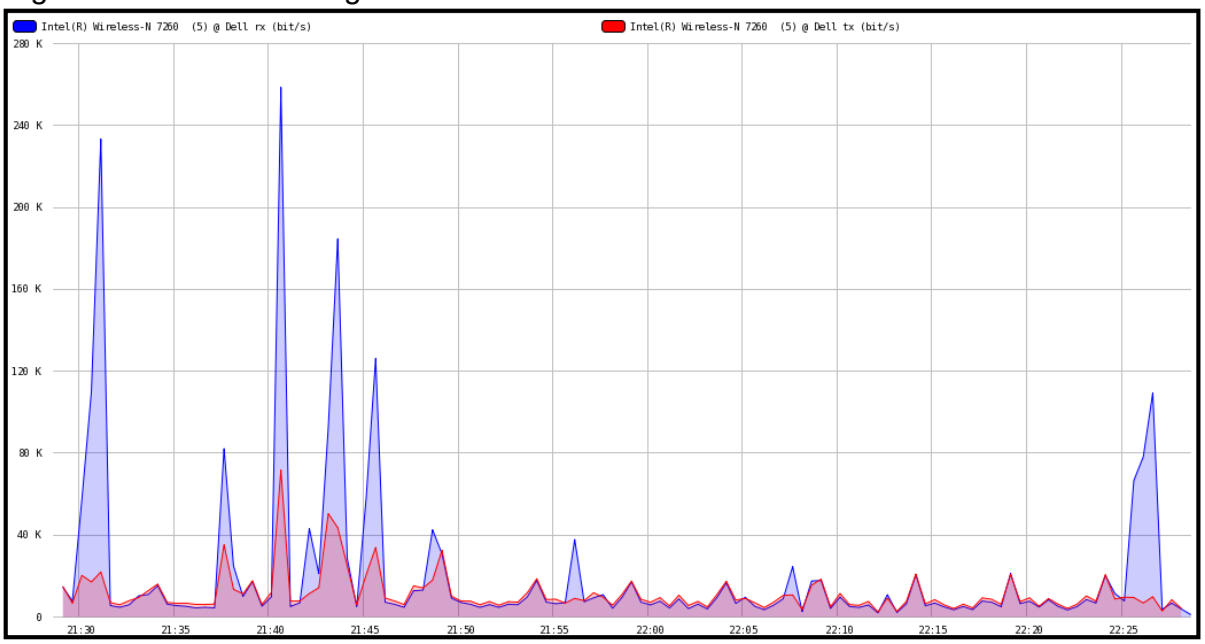
4.9 DIVERSIDADE DOS RELATÓRIOS

Considerando a diversidade dos relatórios gráficos obtidos pela ferramenta The Dude, a mesma foi avaliada com a nota 1, pois apresenta somente a disponibilidade de um modelo gráfico, sendo que o mesmo pode ser elaborado com a cor de preferência, como também a localização da legenda.

Tem a disponibilidade apenas uma caixa de seleção de escala iniciada por hora, seguida de dia, semana, mês e ano e não possui a possibilidade de se selecionar um período para análise. Sendo assim, se for necessário analisar um valor que ocorreu em tal dia e hora, não será possível com o The Dude.

Na Figura 46, observa-se a elaboração de um gráfico referente ao tráfego de rede.

Figura 46 - Gráfico tráfego de rede The Dude.



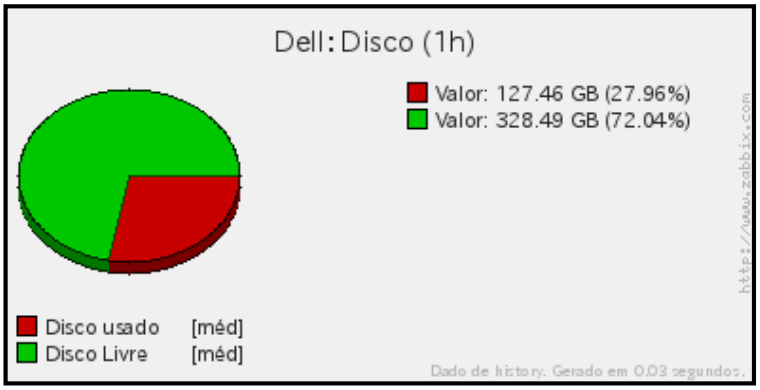
Fonte: Elaborada pelo autor.

Verifica-se, portanto, de acordo com a escala de hora estabelecida, o tráfego de entrada e saída obtidos pelo gerenciamento da placa de rede.

A ferramenta Zabbix, disponibiliza a montagem de quatro diferentes tipos de gráficos, o normal, assim como o The Dude, em formato de pilha, torta e explodido, sendo o último considerado um tipo torta porém com dados espaçados.

A Figura 47 demonstra um gráfico em formato de torta referente ao espaço em disco de um dispositivo, detalhando o valor utilizado e livre.

Figura 47 - Gráfico de disco Zabbix.



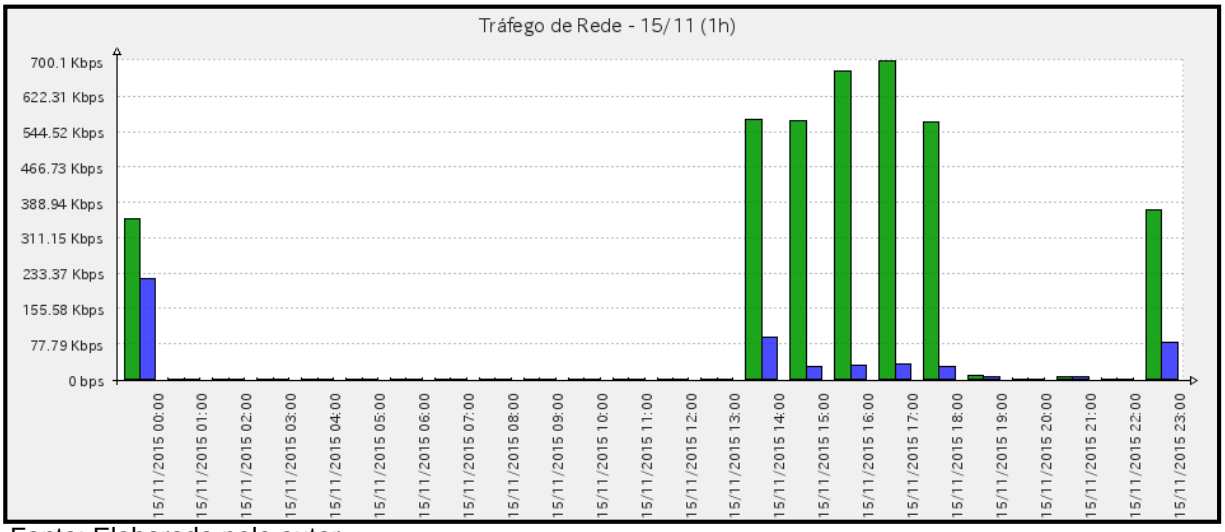
Fonte: Elaborada pelo autor.

Com o Zabbix, é possível também gerar um relatório sobre o período que se deseja analisar, porém, assim como o The Dude, se prende às escalas de hora, dia,

semana, mês e ano, não sendo possível verificar com tanta precisão o valor correspondente a um determinado horário, portanto a ferramenta foi avaliada com nota 3.

Na Figura 48, é possível verificar um relatório emitido referente ao tráfego da placa de rede.

Figura 48 - Gráfico tráfego de rede Zabbix.



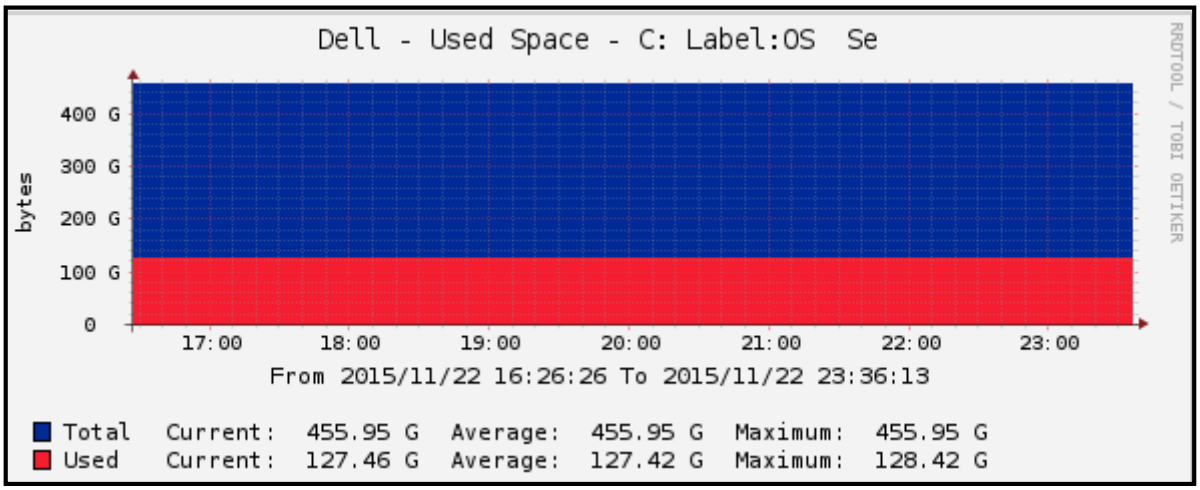
Fonte: Elaborada pelo autor.

Portanto, com a utilização da escala de hora, é possível verificar o tráfego de rede de acordo com cada hora passada.

Já a ferramenta Cacti, apesar de não disponibilizar uma caixa de seleção para a escolha do tipo do gráfico, eles podem ser representados no modelo normal ou no formato de pilha.

Na figura 49, demonstra-se um gráfico referente a quantidade utilizada de disco de um dos dispositivos.

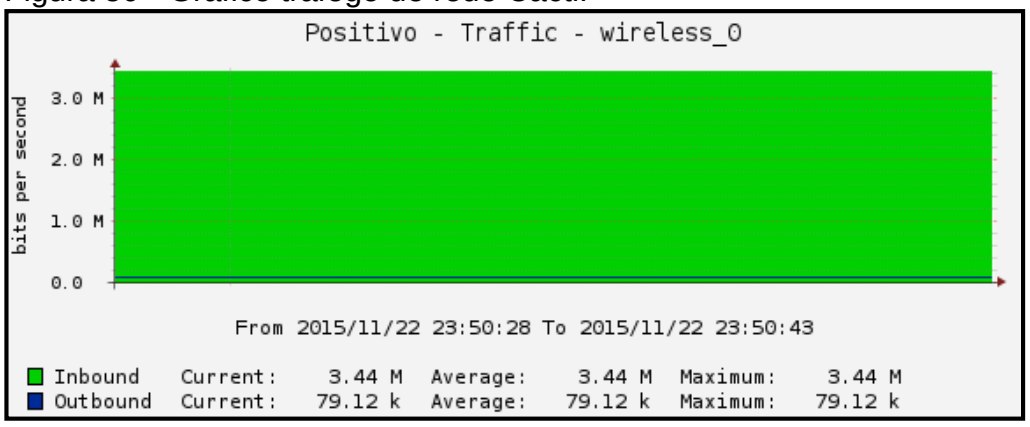
Figura 49 - Gráfico disco Cacti.



Fonte: Elaborada pelo autor.

Diferentemente das demais, a ferramenta Cacti disponibiliza uma aplicação de zoom, onde é possível verificar detalhadamente qual dia e horário pode ter acontecido alguma anormalidade. Como pode ser verificado na Figura 50, o gráfico em relação ao tráfego de rede se apresenta detalhado.

Figura 50 - Gráfico tráfego de rede Cacti.



Fonte: Elaborada pelo autor.

Sendo assim, é possível estabelecer um gráfico relacionado a uma faixa específica de tempo, como no caso, entre 23:50:28 e 23:50:43. Portanto, nesse quesito, a ferramenta Cacti foi avaliada com nota 4.

5 CONSIDERAÇÕES FINAIS

Com a finalização da implantação das ferramentas e atribuições de notas referentes a cada quesito avaliado, foi possível concluir que a ferramenta Zabbix obteve um pequeno diferencial frente as demais.

No entanto, ao estabelecer, verificar e compreender a importância do gerenciamento de rede, principalmente em um ambiente corporativo, a escolha da ferramenta, vai depender necessária e exclusivamente da necessidade do mesmo, buscando adequar a ferramenta que melhor se encaixe de acordo com o que procura.

Se a necessidade da empresa estiver relacionada com a urgência de implementação de um gerenciamento, a ferramenta The Dude pode ser considerada uma boa iniciativa.

Agora se a necessidade for estabelecida na precisão de valores referentes a um dado período, a ferramenta Cacti se adequa perfeitamente, além de contar com uma comunidade muita ativa com o desenvolvimento de vários plugins.

Já a ferramenta Zabbix, com a regularidade obtida nos diversos quesitos, promove um gerenciamento completo e já possui as funcionalidades incorporadas.

Sendo assim, as três ferramentas demonstraram que, com a implementação de qualquer uma delas, o administrador de rede poderá ter uma visão melhor de tudo o que está ocorrendo na rede, além de poder ter parâmetros para a realização de alguma manutenção. Com isso, poderá agir pró-ativamente diante de qualquer eventualidade que possa acontecer. E ainda, o gerenciamento será realizado em sua totalidade de maneira gratuita, já que são ferramentas open source.

Por fim, espera-se que as considerações aqui realizadas, contribuam, de alguma maneira, na definição da escolha de uma dessas ferramentas para gerenciamento de rede.

REFERÊNCIAS

ABREU, F. R.; PIRES, H. D. Gerência de Redes. **Mídia Com**, 2014. Disponível em: <http://www.midiacom.uff.br/~debora/redes1/pdf/trab042/SNMP.pdf>. Acesso em: 26 abr. 2015.

BENINI, R. A.; DAIBERT, M. S. Monitoramento de Rede de Computadores. **DevMedia**, 2011. Disponível em: <http://www.devmedia.com.br/websys.5/webreader.asp?cat=62&artigo=3510&revista=inframagazine_1#a-3510>. Acesso em: 08 mar. 2015.

BLACK, T. L. **Comparação de ferramentas de gerenciamento de redes**. 2008. 64 f. Monografia (Especialização em Tecnologias, gerência e segurança de redes de computadores) – Instituto de Informática; Universidade Federal do Rio Grande do Sul, Porto Alegre, 2008. Disponível em: <http://www.lume.ufrgs.br/bitstream/handle/10183/15986/000695315.pdf>. Acesso em: 29 abr. 2015.

BONOMO, E. **Gerenciamento e Monitoração de Redes de Computadores utilizando-se Zabbix**. 2006. 62 f. Monografia (Especialização em Administração de Rede Linux) – Departamento de pós-graduação, Universidade Federal de Lavras, 2006. Disponível em: <www.ginux.ufla.br/files/mono-EsleyBonomo.pdf>. Acesso em: 25 fev. 2015.

CACTI. **The Cacti Group**, c2004-2012. Apresenta downloads e informações sobre a ferramenta. Disponível em: <http://www.cacti.net>. Acesso em: 06 maio 2015.

COMER, D. E. **Interligação de Redes com TCP/IP**. Tradução: Daniel Vieira. 5. ed. Rio de Janeiro: Elsevier, 2006. v. 1.

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

DANTAS, M. **Tecnologias de Redes de Comunicação e Computadores**. Rio de Janeiro: Axcel Books, 2002. Disponível em: <http://www.feesc.org.br/site/?pg=trcc>. Acesso em: 21 abr. 2015.

DONHA, A. G.; SOUZA, L.C. de P.; SUGAMOSTO, M. L. Determinação da fragilidade ambiental utilizando técnicas de suporte à decisão e SIG. **Revista brasileira de engenharia agrícola e ambiental**, v. 10, n. 1, p. 175-181, 2006. Disponível em: <http://www.scielo.br/pdf/rbeaa/v10n1/v10n1a26.pdf>. Acesso em: 06 dez. 2015.

ESTEVES, A. M. B.; ALVES JUNIOR, N. O Protocolo SNMP. **Notas Técnicas**, Rio de Janeiro, v. 3, n. 1, p. 1-14, 2013. Disponível em: <http://revistas.cbpf.br/index.php/nt/article/view/24/31>. Acesso em: 25 abr. 2015

FOROUZAN, B. **A. Comunicação de dados e redes de computadores**. Tradução: Ariovaldo Griesi. Revisão Técnica: Jonas Santiago. São Paulo: McGraw-Hill, 2008.

FRANÇA, M. C. **Redes de Computadores**. Florianópolis: IF-SC, 2010.

LOPES, R. V.; SAUVÉ, J. P.; NICOLLETTI, P. S. **Melhores práticas para a gerência de redes de computadores**. Rio de Janeiro: Campus, 2003.

MELCHIORS, C. **Raciocínio baseado em casos aplicado ao gerenciamento de falhas em redes de computadores**. 1999. 151 f. Dissertação (Mestrado em Ciência da Computação) - Programa de Pós-Graduação em Computação; Universidade Federal do Rio Grande do Sul, Porto Alegre, 1999. Disponível em: <http://penta.ufrgs.br/~cristina/dumbotexto/cristina.pdf>. Acesso em: 26 abr. 2015.

MIKROTIK. Routing the world, [2015?]. Apresenta downloads e informações sobre a ferramenta. Disponível em: <http://www.mikrotik.com>. Acesso em: 04 maio 2015.

MENDES, D. R. **Redes de computadores**: teoria e prática. São Paulo: Novatec, 2007.

NAGIOS. **Nagios Website**, c2009-2015. Apresenta downloads e informações sobre a ferramenta. Disponível em: <http://www.nagios.org>. Acesso em: 06 maio 2015.

NORMANDO, D., TJADERHANE, L., QUINTÃO, C. C. A. 2010. A escolha do teste estatístico - um tutorial em forma de apresentação em PowerPoint. Dental Press Journal of Orthodontics 15 (02), 101 – 106. Disponível em: <http://www.scielo.br/pdf/dpjo/v15n1/12.pdf>. Acesso em: 06 dez. 2015.

OPEN SOURCE INITIATIVE. The Open Source definitione. **Open Source**, [2015?]. Disponível em: <http://opensource.org/docs/osd>. Acesso em: 03 maio 2015

PEREIRA, F.; MARINHO, I.; OLIVEIRA, N. Artigo para a disciplina de Engenharia de Software: Open Source software development. **FEUP**, [2015?]. Disponível em: <paginas.fe.up.pt/~aaguiar/es/artigos%20finais/es_final_11.pdf>. Acesso em: 03 maio 2015.

SPECIALSKI, E. S. Gerência de redes de computadores e de telecomunicações. **FURB**, 2001. Disponível em: <home.furb.br/fabio/redes2/pub/ApostilaGerencia.doc>. Acesso em: 26 abr. 2015.

STALLINGS, W. **Redes e sistemas de comunicação de dados**: teoria e aplicações corporativas. Rio de Janeiro: Elsevier, 2005.

TANENBAUM, A. S. **Redes de computadores**. 4. ed. Rio de Janeiro: Campus, 2003.

TEIXEIRA, M. V.; TEIXEIRA, J. H.; SILVA NETO, P. C. S. A importância do SNMP e do NAGIOS na administração de redes. In: WORKSHOP DE TECNOLOGIA DA REGIÃO FRONTEIRA OESTE, 3., Pontes e Lacerda, 2014. **Anais...** Pontes e Lacerda: IFMT, 2014. Disponível em: <http://anaiswtrfo.plc.ifmt.edu.br/index.php/wtrfo/article/download/52/47>. Acesso em: 25 abr. 2015.

ZABBIX. **Zabbix Website**, c2001-2015. Apresenta downloads e informações sobre a ferramenta. Disponível em: <http://www.zabbix.com>. Acesso em: 04 maio 2015.