CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Tecnologia em Segurança da Informação

Anderson Ferreira Nobre Cabello

USO DO CACTI PARA GERENCIAMENTO DE REDES

Uma Análise Experimental e Comparativa

Americana, SP

2015

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Tecnologia em Segurança da Informação

Anderson Ferreira Nobre Cabello

USO DO CACTI PARA GERENCIAMENTO DE REDES

Uma Análise Experimental e Comparativa

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso de Tecnologia em Segurança da Informação, sob a orientação do Prof. Ms. Henri Alves de Godoy

Área de concentração: Segurança da Informação

Americana, SP

2015

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

	Cabello, Anderson Ferreira Nobre
C113u	Uso do CACTI para gerenciamento de redes: uma análise experimental e comparativa. / Anderson Ferreira Nobre Cabello. – Americana: 2015.
	51f.
	Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
	Orientador: Prof. Me. Henri Alves de Godoy
	1. Redes de computadores 2. Segurança em sistemas de informação I.Godoy, Henri Alves de II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.
	CDU: 681.519 681.518.5

Anderson Ferreira Nobre Cabello

USO DO CACTI PARA GERENCIAMENTO DE REDES: UMA ANÁLISE EXPERIMENTAL E COMPARATIVA

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: Segurança da Informação.

Americana, 26 de Junho de 2015.

Banca Examinadora:

Henri Alves de Godoy (Presidente)
Mestre
Fatec Americana

Benedito Luciano Antunes de França (Membro)
Mestre
Fatec Americana

Rogério Nunes de Freitas (Membro)
Especialista
Fatec Americana

AGRADECIMENTOS

Em primeiro lugar gostaria de agradecer a Deus por conduzir minha vida de forma que tudo ocorra da melhor maneira possível. Gostaria também de agradecer a todos os professores da Fatec Americana, por todo o conhecimento transmitido para nós, alunos. Em especial, gostaria de ressaltar alguns professores que ultrapassaram a linha do ensino e nos ensinaram mais que o plano de ensino do semestre: Profª. Ms. Maria Cristina Luz Fraga Moreira Aranha, Prof. Ms. Henri Alves de Godoy, Profª. Juliane Borsato Beckedorff Pinto, Prof. Rogério Nunes de Freitas e Prof. Ms. Alexandre Garcia Aguado. Por fim, gostaria de agradecer aos alunos Ely Edson Dalbem, Evelyn Miyuki Ota e Ricardo de Paula Cardoso pela ajuda e companheirismo em todos esses anos de estudos.

DEDICATÓRIA

À minha esposa, Elen, por me apoiar e ser mãe e pai de nossos filhos durante esse período de estudos, e aos meus filhos, Alexandre e Henrique, pelo tempo em que não pudemos ficar juntos.

RESUMO

O presente trabalho tem como objetivo mostrar o uso de uma ferramenta específica para o gerenciamento de redes e mostrar toda a sua conexão com o curso de Tecnologia em Segurança da Informação. Para isso foi utilizado um ambiente controlado para prover resultados do monitoramento. Na primeira seção, foi apresentado o conceito de Segurança da Informação e seus principais pilares de sustentação, e como o gerenciamento de redes pode ser diretamente ligado a um desses pilares. Em seguida é iniciada uma seção onde são apresentados alguns conceitos e fundamentos sobre o gerenciamento de redes. Na seção seguinte, foram descritos alguns conceitos básicos sobre a estrutura dos *softwares* de gerenciamento de redes, para melhor compreensão do sistema aqui apresentado. Os conceitos e descrição do aplicativo Cacti foram apresentados em seguida, bem como seu uso. Testes de laboratório foram mostrados apresentando o uso efetivo da ferramenta monitorando um ambiente virtual e outro real, sendo que o primeiro foi desenvolvido somente para esta finalidade e o segundo foi utilizado num ambiente doméstico real. Foram apresentados os resultados desses testes, bem como a conclusão do projeto, com as considerações finais sobre o tema.

Palavras-chaves: Gerência de Redes; Cacti; Monitoramento.

ABSTRACT

This study aims to show the use of a specific tool for managing networks and show all its connection with the course of Technology in Information Security. For this it was used a controlled environment to provide monitoring results. In the first section, the concept of Information Security and its main supporting pillars were presented, and how the network management can be directly connected to one of those pillars. Then begins a section which presents some concepts and fundamentals of network management. In the following section, it was described some basic concepts about the structure of network management softwares, to better understand the system presented here. So, the concepts and description of the application Cacti were presented as well as its use. Laboratory tests were done showing the effective use of the tool monitoring a virtual environment, and other real one, where the first was developed only for this purpose and the second was used in a real home environment. The results of these tests were presented as the project completion, with final remarks on the topic.

Keywords: Network Management; Cacti; Monitoring.

LISTA DE FIGURAS

Figura 1 – Pilares da Segurança da Informação 13
Figura 2 - Exemplos de dispositivos em uma rede 15
Figura 3 - Pacote SNMP 19
Figura 4 – Exemplo de processo Round Robin 22
Figura 5 - Dependências de instalação do Cacti 24
Figura 6 - Definição de senha no MySQL 25
Figura 7 - Seleção do servidor WEB 25
Figura 8 - Seleção de configuração da base de dados 26
Figura 9 - Seleção do tipo de instalação 27
Figura 10 - Primeiro logon no Cacti 27
Figura 11 - Tela de monitoramento do *plug-in* "Monitor" 29
Figura 12 - Gráfico do NTop 29
Figura 13 - Topologia virtual 31
Figura 14 - Topologia de rede doméstica 32
Figura 15 - Teste de *stress* da utilização de CPU 34
Figura 16 - Uso do CPU por usuário 34
Figura 17 - Teste de *stress* da placa de rede 35
Figura 18 - Monitoramento de porta do roteador 36
Figura 19 - Teste de *stress* do disco rígido 37
Figura 20 - Teste de consumo da memória RAM 38
Figura 21 - Uso da memória virtual 38
Figura 22 - Monitoramento de processos no sistema 39
Figura 23 - Monitoramento de disponibilidade de equipamento 40
Figura 24 – Mensagem de aviso de *host off-line* 41
Figura 25 – Mensagem de alerta de disco 42
Figura 26 - Monitoramento de páginas impressas total 43
Figura 27 - Monitoramento de páginas impressas no dia 43
Figura 28 - Monitoramento de consumo de banda pela impressora 44
Figura 29 – Dispositivos que podem ser monitorados 45
Figura 30 - Gráficos visualizados pelo Cacti Viewer 46

LISTA DE ABREVIATURAS, SÍMBOLOS E SIGLAS

CPU	*Central Processing Unit*
FSF	*Free Software Foundation*
FTP	*File Transfer Protocol*
GNU	*Gnu is Not Unix (acrônimo recursivo)*
GPL	*General Public License*
IBM	*International Business Machine*
ICMP	*Internet Control Message Protocol*
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
MB	*Megabyte*
MIB	*Management Information Base*
PDU	*Protocol Data Unit*
PHP	*Personal Home Page*
RAM	*Random Access Memory*
SMI	*Structure of Management Information*
SMS	*Short Message Service*
SNMP	*Simple Network Management Protocol*
TCP	*Transfer Control Protocol*
TI	Tecnologia da Informação
UDP	*User Datagram Protocol*
UPS	*Unit Power Supply*

SUMÁRIO

INTRODUÇÃO 10
1. SEGURANÇA DA INFORMAÇÃO 13
1.1 Confidencialidade 14
1.2 Integridade 14
1.3 Disponibilidade 14
2 . GERENCIAMENTO DE REDES 15
2.1 Motivos para gerenciar uma rede 16
2.2 Áreas para gerenciamento de redes 17
2.3 Estrutura padrão de gerenciamento de redes 18
2.3.1 SNMP 18
2.3.2 SMI 19
2.3.3 MIB 20
3. ESTRUTURA DOS *SOFTWARES* DE GERENCIAMENTO DE REDES 21
3.1 *Round Robin* 21
3.2 RRDTool 22
4 CACTI 23
4.1 Requisitos mínimos de *software* 23
4.2 Instalação do gerente Cacti em uma distribuição Debian 24
4.3 Configuração inicial do Cacti 26
4.3 *Plug-ins* 28
4.4 *Templates* 30
5. ANÁLISE EXPERIMENTAL E COMPARATIVA 31
5.1 Monitoramento de utilização de CPU 33
5.2 Monitoramento de tráfego de rede 35
5.3 Monitoramento de espaço utilizado em disco 36
5.4 Monitoramento de memória 37
5.5 Monitoramento de processos em execução no sistema operacional 39
5.6 Monitoramento de disponibilidade do equipamento 39
5.7 Recebimento de alertas por *e-mails* 40
5.8 Monitoramento de impressoras 42
5.9 *Cacti Viewer* 44
CONSIDERAÇÕES FINAIS 47
REFERÊNCIAS 49

INTRODUÇÃO

Esse trabalho teve como **escopo**, apresentar as técnicas disponíveis para o gerenciamento de redes, utilizando a ferramenta Cacti em um ambiente controlado e as possíveis desvantagens em sua utilização.

O **problema** principal para formulação deste trabalho foi determinar se o *software* Cacti é uma opção vantajosa para o gerenciamento de uma rede de computadores e desta forma, responder a seguinte **pergunta**: A relação custo-benefício da implantação deste recurso o torna uma ferramenta viável para se incorporar num ambiente de trabalho?

O **objetivo geral** deste trabalho foi fazer uma análise do funcionamento de uma rede monitorada, registrando vantagens e desvantagens de se ter esse tipo de implementação.

Como **objetivos específicos** foram definidos:

a) Conhecer o processo de implantação do serviço de monitoração da rede;

b) Realizar testes para comparação de uma rede monitorada *versus* rede sem monitoramento em um ambiente controlado;

c) Exercitar as diversas formas de monitoramento da rede e dos *hosts*;

d) Analisar e discutir os resultados obtidos durante o teste de comparação.

Como **justificativa** para a escolha do tema, foi levado em consideração o aumento das redes de computadores atuais, em função da facilidade e variedade de novos dispositivos que são incorporados a elas. Todavia, quanto mais equipamentos conectados, maiores as chances de algum deles ficar indisponível, ou sofrer alguma ação que coloque em risco a Segurança da Informação. O gerenciamento de redes é uma medida importante para mitigar esses riscos.

Este autor tentou mostrar suas vantagens, baseando-se nos conhecimentos adquiridos durante o curso de Segurança da Informação. A escolha pela aplicação Cacti se deu por não haverem muitas referências ao produto em sistemas de pesquisas de

artigos acadêmicos. Ferramentas como o Nagios (PONTUAL, 2009) e o Zabbix (PUSKA, 2011) detêm um amplo material, sendo até citadas em alguns trabalhos de conclusão também nesta unidade de ensino, tais como o Gerência de Redes com Zabbix, apresentado por Marcos Teodoro da Silva em 2013 e Gerência e Monitoramento de Redes, apresentado por Raquel Ferraz Cunha Santos em 2011.

Como **método**, a pesquisa foi aplicada, com base em procedimentos técnicos comparativos, sendo feita de modo experimental, a fim de exibir com exemplos reais, os resultados dos experimentos, provindos de dois ambientes controlados, onde o primeiro foi desenvolvido de forma virtual com o auxílio da ferramenta VirtualBox, e o segundo foi executado em um ambiente de rede real, onde ambos alimentaram uma base de dados que geraram o conteúdo da pesquisa.

A técnica utilizada foi a de observação e análise de conteúdo, pois pretendeu-se montar um laboratório de testes para gerar os dados necessários da pesquisa e documentá-los apropriadamente. Dois ambientes foram montados, sendo que a) um utilizou máquinas virtuais trabalhando em uma rede e uma máquina gerente e; b) o outro foi feito em um ambiente real, ambos coletando dados de todos os *hosts* da rede, que resultaram em uma pesquisa do tipo qualitativa. Com base no banco de dados gerado, foi avaliada a real utilidade de um gerente de monitoramento de redes, que foi devidamente registrado utilizando o procedimento bibliográfico e documental da pesquisa.

As **hipóteses** fundantes para o estudo foram:

a) O Cacti tem se mostrado um *software* com uma interface simples de instalar e fácil de operar, além de não necessitar de um *hardware* poderoso para monitoramento, mas isso não significa, necessariamente, que seja uma vantagem real.

b) O Cacti tem diversos concorrentes; alguns deles são amplamente utilizados em áreas de TI por estarem há mais tempo no mercado e serem bastante estáveis, portanto

pode ser que tenham as mesmas vantagens ou diferenças mínimas que não justifiquem o uso de um em relação ao outro.

c) O Cacti tem a seu favor, em relação aos seus concorrentes, uma das melhores ferramentas para geração de gráficos, além do desenvolvimento de *plug-ins*, que implementam recursos que ele não traz originalmente.

Como principais fontes de **pesquisa bibliográfica** são citados:

- Kurose e Ross no livro sobre redes de computadores, abordam o tema de gerenciamento de rede de forma bastante didática e nos transmite todo o embasamento técnico para construção de uma rede gerenciada e os motivos que nos leva ao gerenciamento em todos os possíveis tipo de redes (KUROSE; ROSS, 2010).

- Berry, entre outros são autores de um dos mais completos manuais sobre a ferramenta Cacti, além de ser assíduo colaborador na criação de novos *plug-ins* e ferramentas adicionais à distribuição. Seu manual descreve em detalhes todas as funcionalidades para a configuração do sistema Cacti (BERRY *et al*., 2012).

- Lopes, Sauvé e Nicoletti propõem no livro uma metodologia para guiar o responsável pelo gerenciamento de redes, de maneira que se crie uma norma a ser seguida e que se padronize as atividades (LOPES; SAUVÉ; NICOLETTI, 2003).

- Dantas em seu livro discorre sobre os alicerces que definem a Segurança da Informação e os modelos para gerenciamento de riscos e algumas ferramentas (DANTAS, 2011).

1. SEGURANÇA DA INFORMAÇÃO

Atualmente, com o avanço da tecnologia, a informação em formato digital é gerada em quantidade incalculável, a todo momento. As pessoas e as organizações passaram a ter necessidade de proteção de seus dados, pois ela passou a ser item fundamental para o seu desenvolvimento e sucesso. Com base nisto, surgiu a Segurança da Informação, que é a proteção quanto a vários tipos de ameaças, de forma que garanta a continuidade do negócio, minimize os riscos, maximize o retorno sobre o investimento e as oportunidades do negócio (DANTAS, 2011, p.11).

A Segurança da Informação é padronizada pela norma NBR ISO/IEC 27002:2005 (ABNT, 2005) e tem como pilares fundamentais a confidencialidade, a integridade e a disponibilidade. A Figura 1, mostrada a seguir, simboliza este conceito.

Figura 1 – Pilares da Segurança da Informação

Fonte: Autoria própria adaptada da norma NBR ISO/IEC 27002:2005

1.1 Confidencialidade

“É a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso” (ABNT, 2005 *apud* DANTAS, 2011, p.13).

Uma informação importante não teria tanto valor se ela não pudesse se manter em sigilo. Para isso, a Segurança da Informação deve coibir qualquer acesso não autorizado à informação, garantindo sua inviolabilidade.

1.2 Integridade

“É a garantia da exatidão e completeza da informação e dos métodos de processamento” (ABNT, 2005 *apud* DANTAS, 2011, p.11).

A informação quando recebida deve estar íntegra, pois de nada valeria um dado que não é confiável. A segurança da informação deve garantir que a informação realmente é como ela está sendo apresentada.

1.3 Disponibilidade

“É a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário” (ABNT, 2005 *apud* DANTAS, 2011, p.12).

A informação deve estar disponível quando for solicitada. Muito de seu valor seria perdido se uma informação não pudesse ser acessada quando necessária. Por isso, a Segurança da Informação deve garantir que os meios de transmissão dessas informações estejam íntegros e funcionando.

O tema deste projeto está intimamente ligado a este pilar. E a partir desta definição de disponibilidade é que o sistema de gerenciamento de redes tem se tornado algo relevante em redes de computadores, pois tenta evitar que sistemas e dispositivos se tornem indisponíveis.

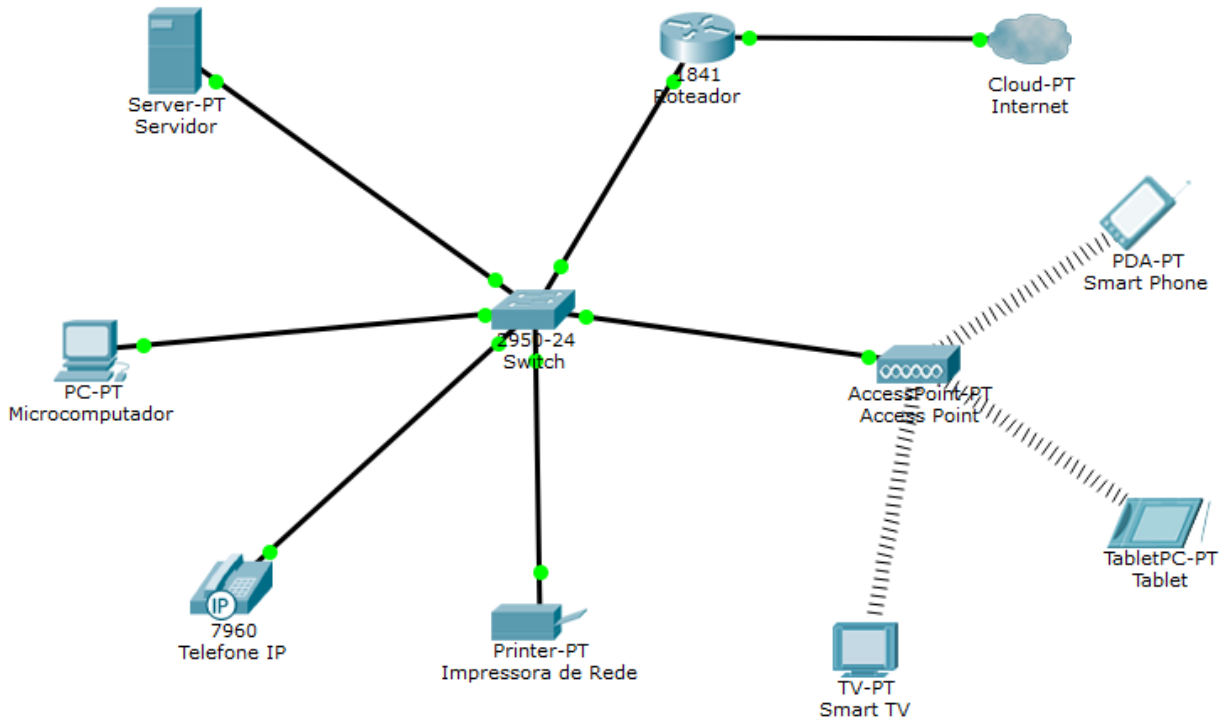
2 . GERENCIAMENTO DE REDES

Atualmente as redes passaram a comportar muito mais dispositivos do que simplesmente computadores. Houve um aumento considerável de tipos de *hosts* nas redes mais básicas, graças ao avanço e barateamento da tecnologia. Ao passo que alguns anos atrás havia basicamente microcomputadores em uma rede local, hoje há impressoras de rede, *switches*, roteadores *wi-fi*, *notebooks*, *smartphones*, *tablets*, *video games* e até televisores, para citar apenas alguns exemplos.

Hoje, um dispositivo quando se torna indisponível em uma rede, pode causar diversos problemas aos negócios, e a partir desta necessidade, passou-se a se dar maior importância à disponibilidade dos dados, desejando-se assim que eles estejam disponíveis a maior parte possível do tempo.

A Figura 2 exemplifica a diversidade de tipos de equipamentos que existem atualmente nas topologias atuais.

Figura 2 - Exemplos de dispositivos em uma rede



Fonte: Autoria própria desenvolvida com uso do *software* Packet Tracer v. 6.1.0.0120

Para Lopes, Sauvé, Nicoletti (2003) a gerência de computadores tem como objetivo controlar elementos físicos e lógicos, e prover um determinado nível de qualidade. Normalmente, para isso, é utilizado um sistema desenvolvido para este propósito.

> 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. (LOPES; SAUVÉ; NICOLLETTI, 2003, p. 17).

Além de conseguir encontrar algum dispositivo que não esteja operacional, o gerenciamento de redes pode mostrar comportamentos anormais na rede, alertando sobre um possível problema, antes que ele ocorra, como, por exemplo, um segmento da rede em que haja muito consumo de banda da rede.

2.1 Motivos para gerenciar uma rede

Segundo Kurose e Ross, entre os principais motivos para que um administrador de redes utilize um *software* de gerenciamento de redes, podem ser:

- Falha em uma interface de redes de um *host:* Os *softwares* de gerenciamento proveem um mapa da rede por meio do qual são mostrados os *hosts on-line* e emitem um alerta indicando os que estiverem *off-line*. Desta forma, é fácil identificar um que venha a perder a conexão com a rede;

- Monitoração de *hosts:* É possível gerenciar periodicamente sistemas sendo executados nos dispositivos da rede, bem como serviços habilitados no sistema operacional e certificar se estão operacionais;

- Monitoração do tráfego de rede: A partir deste recurso, é possível identificar locais de congestionamento, se acontecem em determinado período do dia, e assim tomar as decisões corretas para correção deste tipo de “gargalo” na rede. Isso pode ser útil na tomada de decisões sobre um *upgrade* físico ou de banda, por exemplo.

- Monitoração de tabelas de roteamento: Este tipo de monitoramento é específico para roteadores e *switches* configuráveis e não será abordado seu uso neste projeto, pois necessitaria de equipamentos próprios para esta finalidade. Servem para verificar tabelas de roteamentos, a fim de encontrar falhas de configuração e que podem gerar instabilidades em redes;

- Monitoração de disponibilidade de serviço: Algumas empresas necessitam de informação quanto à disponibilidade de alguns *hosts* da rede, para efeito de acordos de níveis de serviços. Dessa forma, podem-se gerar relatórios que comprovem a eficiência da rede e a real disponibilidade dos equipamentos na rede;

- Detecção de invasão: Tráfego suspeito, acesso às determinadas portas e requisições de pacotes ICMP, são alguns exemplos de dados que um administrador pode verificar via *software* de monitoramento de redes (KUROSE; ROSS, 2010, p. 554-555).

Obviamente, as funções podem ser expandidas, pois praticamente todos os *softwares* de gerenciamento dispõem de integração com outras ferramentas, o que possibilitaria o exercício de outras funções.

2.2 Áreas para gerenciamento de redes

Ainda, segundo Kurose e Ross, a ISO definiu 5 áreas para o gerenciamento de redes:

- Gerenciamento de desempenho: gerencia o desempenho de *hosts* com base em números e informações de análise e controle;

- Gerenciamento de falhas: Igual ao gerenciamento de desempenho, mas aplicado a partir do momento em que uma falha ocorreu;

- Gerenciamento de configuração: Possibilita verificar atualizações de dispositivos;

- Gerenciamento de contabilização: Controla o acesso de usuário e informa o quanto os dispositivos de rede estão consumindo de recursos;

- Gerenciamento de segurança: Controle de acesso aos recursos baseado em centrais de distribuição de chaves (KUROSE; ROSS, 2010, p. 555-556).

Definidas todas as áreas para o gerenciamento de uma rede, cabe ao administrador entender quais serão as utilizadas por ele e definir qual o sistema será utilizado para gerenciar a rede.

2.3 Estrutura padrão de gerenciamento de redes

O gerenciamento de redes segue alguns padrões e estruturas, que normalmente envolvem os equipamentos que terão seus dados coletados, chamados de **agentes**, e uma máquina para coletar e tratar esses dados, que pode ser dedicada ou não para essa função, chamada **gerente** (LOPES; SAUVÉ; NICOLETTI, 2003, p. 17).

Para esse modelo de operação é incorreto chamá-lo de cliente-servidor, pois as máquinas gerenciadas, ora funcionam como servidor, pois fornecem seus dados para a máquina gerente, e ora funcionam como cliente, quando necessitam enviar um alarme para o gerente.

Para que essa operação seja possível, basicamente três protocolos são necessários e a seguir será dada uma breve explicação sobre suas definições e funções.

2.3.1 SNMP

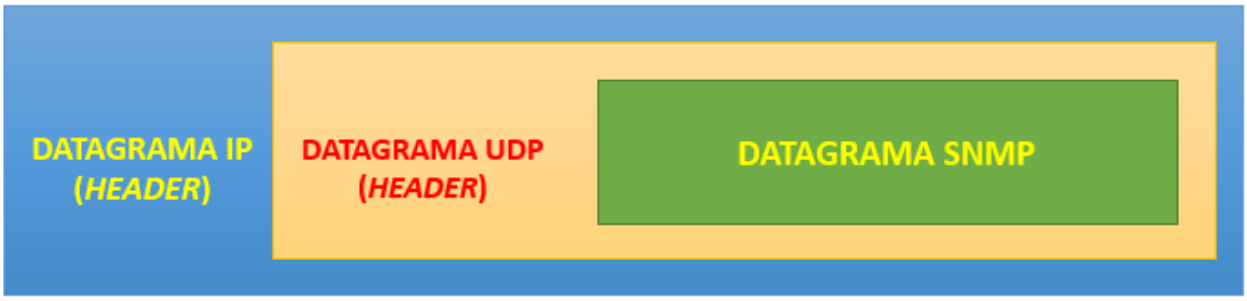
O SNMP é o protocolo padrão para gerenciamento de dispositivos em redes que usem o protocolo IP. Usa a porta 161 por padrão e é responsável pela comunicação entre gerente e agentes. Ele também define o formato e o tipo de pacotes que serão trocados entre os dispositivos. Atualmente, a maioria dos dispositivos em uma rede suporta este protocolo e atua na camada de Aplicação do modelo TCP/IP (RFC 1157, 1990).

O SNMP é anexado em pacotes do tipo UDP, pois desta forma, não têm prioridade no tráfego da rede, evitando assim, congestionamentos causados pelo monitoramento da rede. Esses pacotes UDP são encapsulados dentro de um datagrama IP para serem

transportados pela rede. O pacote tem uma estrutura bem simples, que pode ser verificada na Figura 3.

Dentro do datagrama SNMP é apresentado a versão do protocolo, a comunidade ao qual o protocolo está associado e o PDU que contém os dados a serem transmitidos.

Figura 3 - Pacote SNMP



DATAGRAMA SNMP		
Versão	*Community* – Definida nas configurações do gerente	SNMP PDU – Estrutura de dados e verificação do pacote

Fonte: Autoria própria adaptado de Kurose e Ross (2010, p. 567-570) e NIC (2015)

O tamanho do pacote é variável e seguirá as regras estipuladas na rede para o envio de pacotes IP.

Atualmente, o SNMP está em sua terceira versão, sendo que a segunda versão traz melhorias de performance comparado com a segunda. E a terceira versão funciona com sistema de criptografia como medida de proteção aos dados (RFC 1157, 1990).

2.3.2 SMI

O SMI “é um protocolo que define a estrutura básica das informações que serão coletadas. Uma espécie de *template*, especificando as regras para criação de nomes, tipos e a forma como as informações serão codificadas para ser enviada ao gerente” (NIC, 2015, 3min17s).

Os *templates* de *softwares* de gerenciamento são modelados com base nas informações que o SMI presente nos dispositivos fornece (RFC 1155, 1990).

Para exemplificar de uma forma simples, quando habilitamos o SNMP em um equipamento com o sistema operacional Linux, automaticamente será habilitada uma SMI que irá apontar os itens que podem ser gerenciados naquele sistema, tais como processador, memória, disco rígido, entre outros.

2.3.3 MIB

O MIB “define o conjunto de informações que podem ser coletadas nos agentes sendo estruturada de forma hierárquica” (NIC, 2015, 3min49s).

Numa MIB há vários grupos, com vários objetos em cada um deles. Os grupos são definidos pela SMI, e os objetos são distribuídos em uma determinada ordem para que haja coesão nas informações. Para exemplificar, pode-se ter um grupo chamado *System*, por meio do qual, os dados de um sistema seriam coletados nesta ordem para montar uma tabela: nome e versão; vendedor; última reinicialização; contato; serviços utilizados pelo sistema (RFC 3418, 2002).

Ainda com base no exemplo dado sobre SMI, para cada item possível de gerenciar, haverá MIBs específicas, com as informações de como coletar os dados para cada um desses recursos. Logo, para o disco rígido, por exemplo, haverá uma MIB de como coletar qual a capacidade total do disco. Outra, que consegue calcular quanto do disco rígido está sendo utilizado no momento, e assim por diante.

A MIB tem atualmente duas versões, chamadas MIB e MIB-II e se diferenciam por trazer melhorias de performance na versão mais atual.

3. ESTRUTURA DOS *SOFTWARES* DE GERENCIAMENTO DE REDES

Esta seção tem como principal função apresentar alguns conceitos básicos sobre os *softwares* de gerenciamento de redes, que são os responsáveis por interpretar as informações trocadas entre agentes e gerentes, além de tratar e apresentar esses dados de forma que os administradores de redes possam interpretá-los.

Antes de falar sobre o *software* de gerenciamento de redes, é necessário citar alguns pontos importantes para seu correto entendimento. Quase todos são disponibilizados sob a licença GNU GPL, que basicamente diz que todo sistema disponibilizado sob suas regras, devem ser gratuitos, ter o código-fonte disponibilizado para ser alterado por quem quiser e deve continuar sendo gratuito, independente da alteração sofrida.

A seguir serão abordados como o sistema operacional trata a requisição SNMP e um dos *softwares* que está agregado ao Cacti.

3.1 *Round Robin*

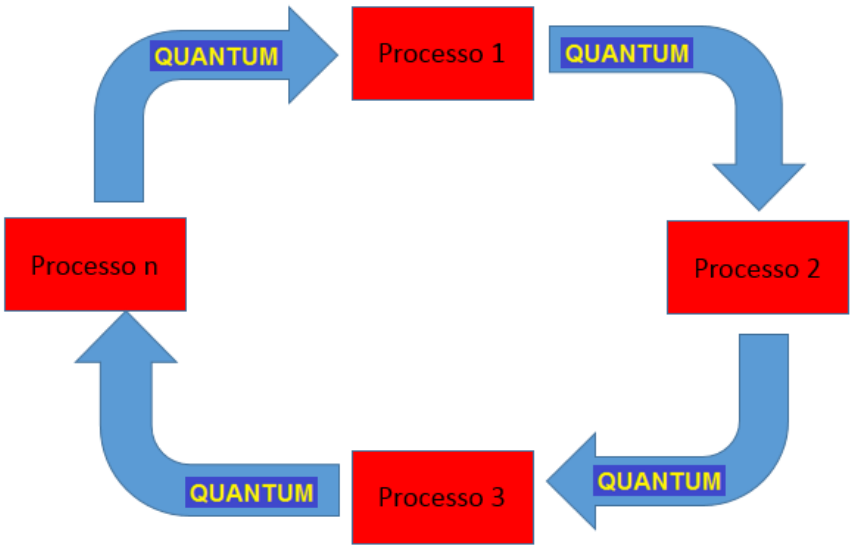
É um algoritmo para agendamento de processos (programa em execução), em que um sistema atribui frações de tempo para cada processo, em partes iguais e de forma circular, não havendo prioridade.

Eles são armazenados em uma fila circular e executados em ordem, e durante um tempo pré-estabelecido pelo sistema, chamado de ***quantum***. Se o processo não for finalizado durante seu *quantum*, volta para o fim da fila e aguarda sua vez novamente para ser executado. Esse processo pode ser visualizado na Figura 4 por meio da qual se mostra que o Processo 1 é executado durante um determinado período de tempo (*quantum*), e após esse período, tendo o processo sido concluído ou não, o Processo 2 será executado, e o Processo 1 aguardará sua vez para ser executado novamente (WIKIPEDIA, 2015).

O SNMP, que é o protocolo necessário para o transporte das informações gerenciadas, utiliza esse processo para ser executado no sistema operacional e enviar

as informações solicitadas e dessa forma, evita que haja travamento do sistema, devido alguma solicitação incorreta (CACTI, 2015).

Figura 4 – Exemplo de processo Round Robin



Fonte: Autoria própria baseado em WIKIPEDIA, 2015

3.2 RRDTool

RRDTool (*Round Robin Database Tool*) é um sistema criado por Tobias Oetiker em 2005, sob licença GNU GPL, que armazena dados numéricos em redes, e que pode ser utilizado para armazenamento de outros tipos de dados, tais como temperatura, uso de CPU, entre outros.É comumente usado, sendo integrado aos outros programas que necessitam de armazenamento de dados (RRDTOOL, 2015).

Por ser leve e simples de se integrar a outros programas, o RRDTool é muito utilizado quando os *softwares* necessitam da função de coleta de dados numa rede. O Cacti é um desses programas.

4 CACTI

Cacti é uma ferramenta *RRDTool* para monitoramento e gerenciamento de redes simples e complexas, produzida pela empresa Cacti Group, Inc. Foi desenvolvida sob a licença GNU de *software* livre e é distribuída de forma gratuita, porém, é possível contribuir com doações pelo site *http://www.cacti.net* (CACTI,2001).

É capaz de monitorar elementos da rede e seus programas, além da banda utilizada e uso do processador. Estes dados são demonstrados através de gráficos em um banco de dados MySQL. A interface é montada sobre PHP[1] e utiliza o protocolo SNMP para a comunicação.

Este trabalho se baseará em seu uso, devido a pouca literatura e projetos de pesquisa disponíveis, fazendo-se uso desta ferramenta.

4.1 Requisitos mínimos de *software*

Atualmente para instalação do *software* Cacti é necessário que, em conjunto, estejam instalados os seguintes *softwares*:

- RRDTool 1.0.49 ou 1.2.x ou superior – para coleta dos dados;
- Banco de dados MySQL 4.1.x ou 5.x ou superior – usado para armazenar os dados recebidos;
- PHP 4.3.6 ou superior, 5.x é altamente recomendado para funções avançadas – usado para criação das páginas *web*;
- Um servidor *web* (Apache, IIS, por exemplo) – para acesso remoto via *browser*.

Os requisitos mínimos de *hardware* devem atender as exigências da distribuição Linux escolhida para receber o Cacti (BERRY *et al*., 2012).

[1] Linguagem de programação

4.2 Instalação do gerente Cacti em uma distribuição Debian

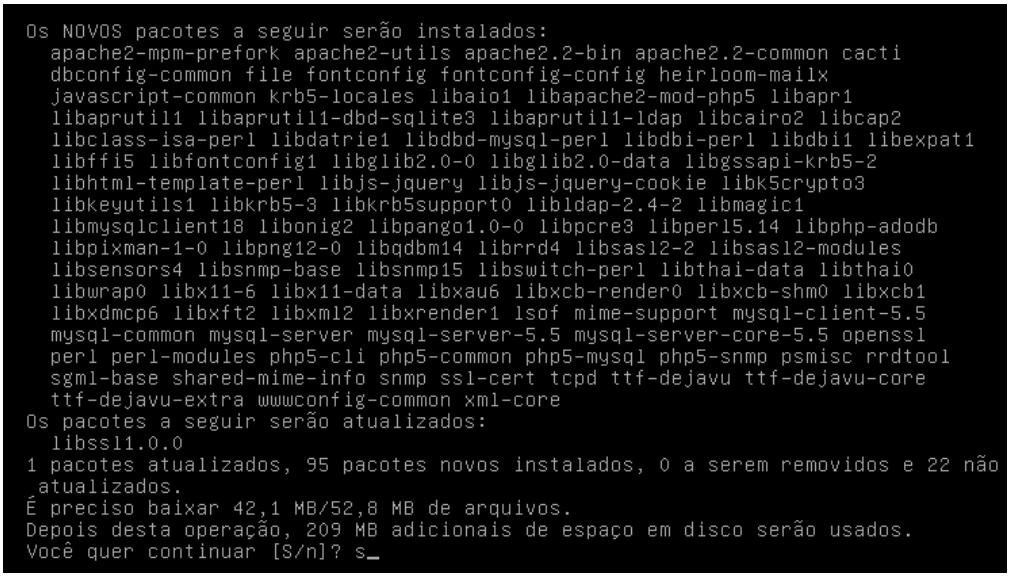
A instalação de um gerente Cacti é simples e quando utilizada em distribuições mais amigáveis, como o Debian ou o Ubuntu, fica mais simples. A seguir serão mostrados os passos para instalação em uma máquina com o sistema Debian 7.

O intuito deste capítulo é mostrar o quão simples é a instalação da ferramenta Cacti. Tendo o sistema em funcionamento e com acesso à Internet, basta executar o comando:

#sudo apt-get install cacti

Conforme mostrado na Figura 5, todas as dependências necessárias para a instalação do Cacti são apresentadas e instaladas automaticamente.

Figura 5 - Dependências de instalação do Cacti

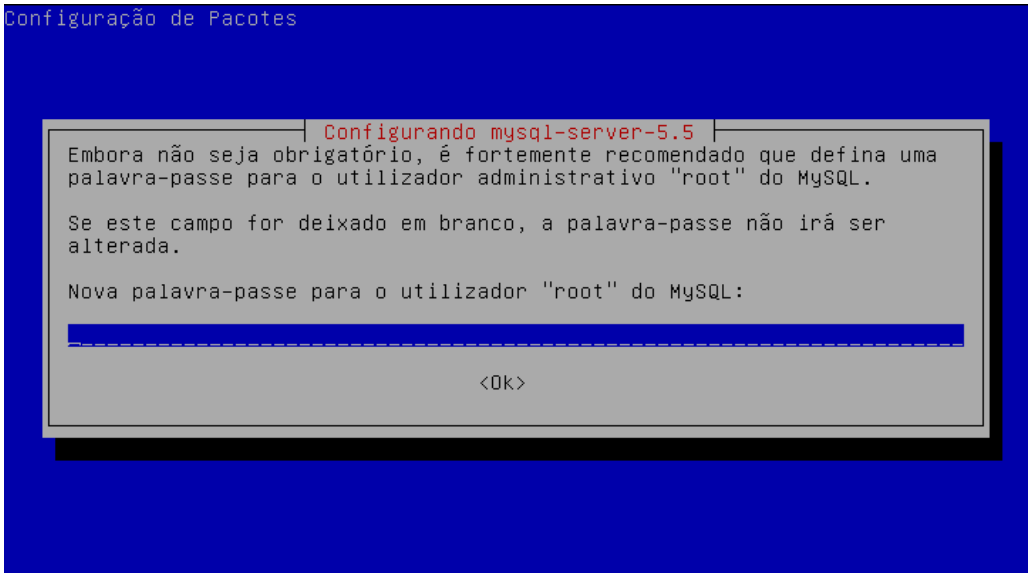


Fonte: Autoria própria. Imagem retirada durante instalação da aplicação.

O Debian se encarrega de instalar todas as dependências, tais como MySQL, Apache, PHP, entre outras.

Junto com a instalação do Cacti se dará a instalação do banco de dados. Será solicitada a definição de uma senha para acesso ao MySQL, conforme apresentada na Figura 6.

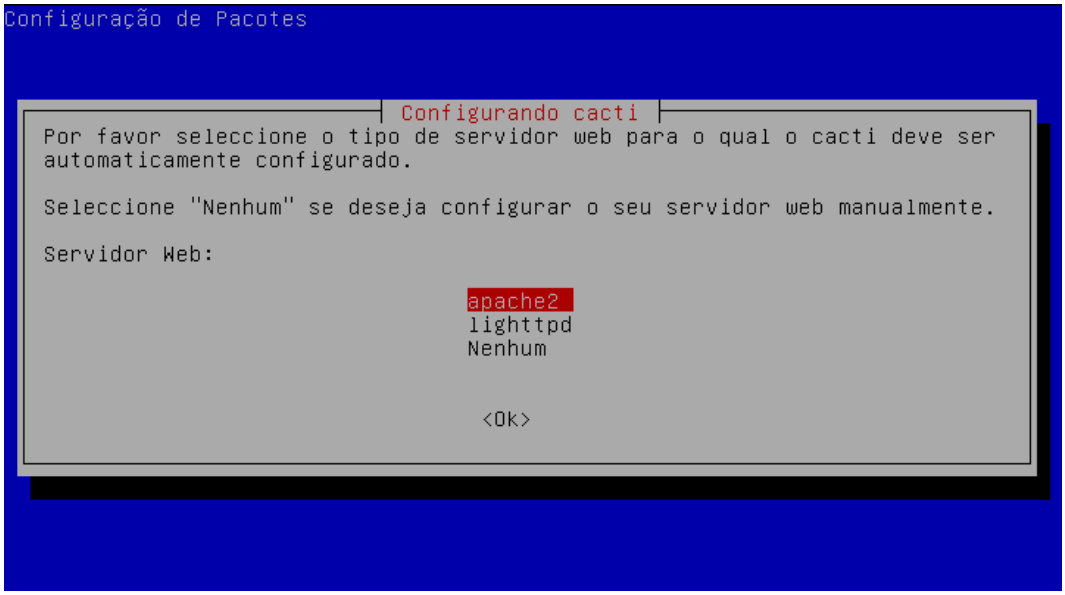
Figura 6 - Definição de senha no MySQL



Fonte: Autoria própria. Imagem retirada durante instalação da aplicação.

O próximo passo é definir o *Web Server* que será utilizado, de acordo com a Figura 7. Neste caso, foi utilizado o Apache2, por ser o mais comumente utilizado.

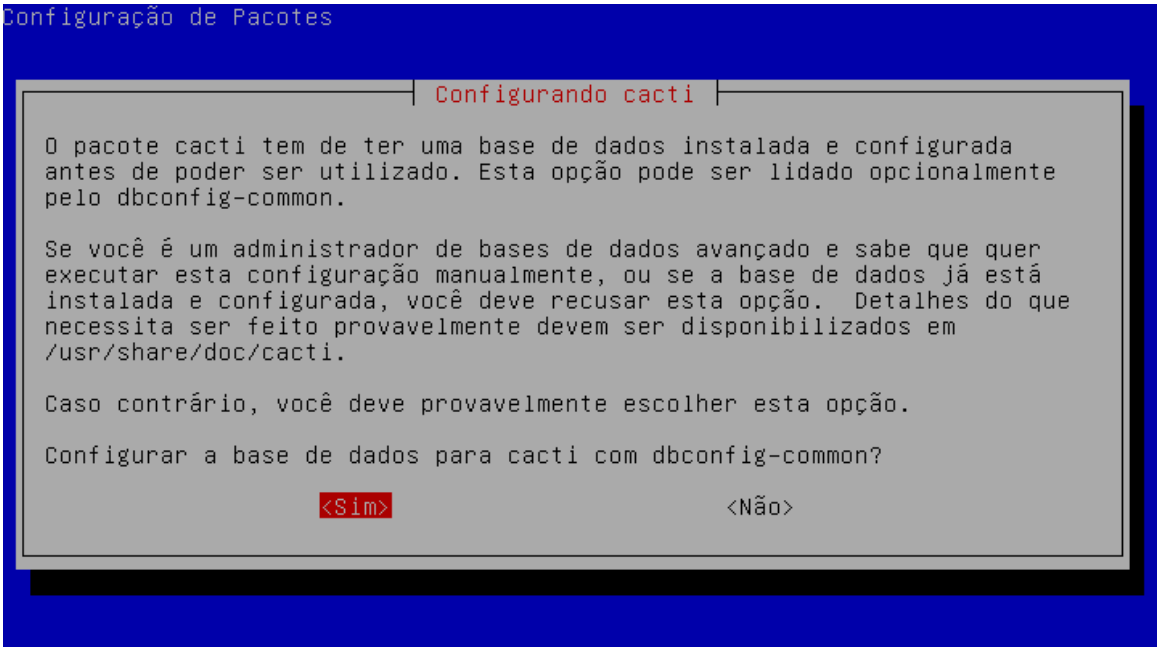
Figura 7 - Seleção do servidor WEB



Fonte: Autoria própria. Imagem retirada durante instalação da aplicação.

Por fim, deve-se definir o acesso à base de dados, conforme Figura 8. Neste caso será utilizado com o *dbconfig-commom*, por ser o padrão sugerido pelo programa.

Figura 8 - Seleção de configuração da base de dados



Fonte: Autoria própria. Imagem retirada durante instalação da aplicação.

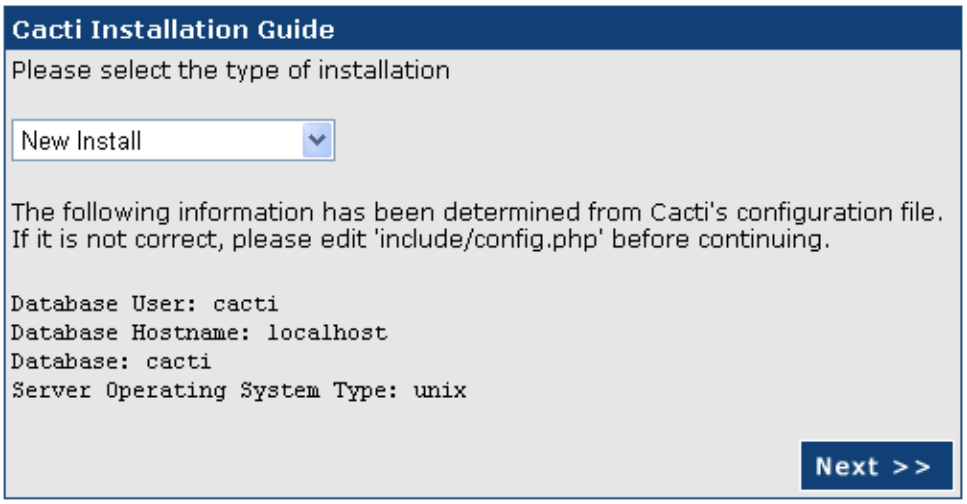
Dessa forma, é finalizada toda a configuração inicial do gerente Cacti. Somente com esses passos o gerente se encontrará pronto para utilização, e todas as configurações restantes poderão ser feitas, utilizando-se de algum terminal da rede.

4.3 Configuração inicial do Cacti

Para acessar o Cacti pela primeira vez, pode-se utilizar o *browser* de qualquer terminal que esteja com acesso ao IP do gerente. Para isto, basta digitar o endereço <*ip_do_gerente_Cacti*>/*cacti*> no navegador. A primeira tela a ser apresentada será a de boas-vindas. Logo a seguir, será solicitado o tipo de instalação.

No caso deste trabalho, tratava-se de uma nova instalação como apontada na Figura 9.

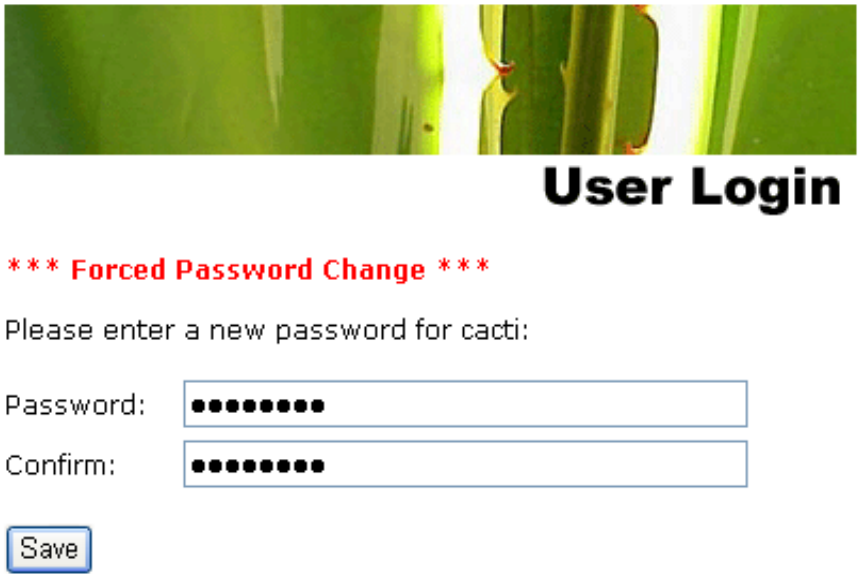
Figura 9 - Seleção do tipo de instalação



Fonte: Autoria própria. Imagem retirada durante instalação da aplicação.

Por padrão o Cacti vem com dois usuários criados: ***admin*** e ***guest***, sendo que o ***guest*** estará desativado, e o ***admin*** usa a senha *admin*. Por motivos óbvios de segurança, após o primeiro *logon*, será solicitada a troca da senha. Esse processo é revelado na Figura 10:

Figura 10 - Primeiro logon no Cacti



Fonte: Autoria própria. Imagem retirada durante instalação da aplicação.

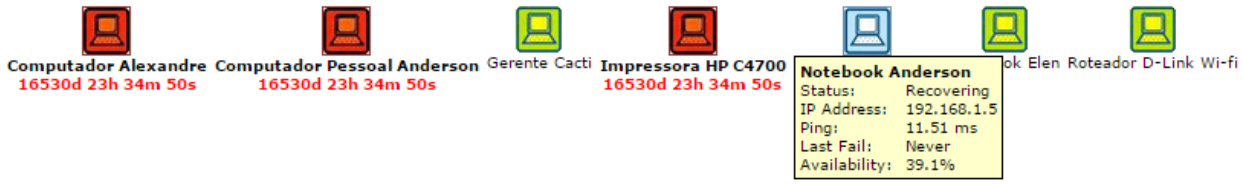
4.3 *Plug-ins*

Um dos principais atrativos do *software* Cacti está nos *plug-ins*[2], que são desenvolvidos e distribuídos gratuitamente por colaboradores e que adicionam novas funcionalidades ao sistema. Dentre os principais disponibilizados atualmente, alguns são citados a seguir com as suas definições retiradas do próprio *site* do Cacti, e que estão disponíveis em uma seção apropriada para *plug-ins*:

- **Settings** – Este *plug-in* é um pré-requisito para a instalação da maioria dos demais, pois adiciona novas opções de configuração ao Cacti em seu menu padrão, que não estão disponíveis em sua instalação inicial.
- **Thold** – Adiciona a opção de alertas por *e-mail*. Para cada item selecionado, podem ser definidas faixas de criticidade. No caso de espaço em disco, por exemplo, é possível definir como crítico quando 80% do disco estiver ocupado. Ao se atingir este valor, um *e-mail* será enviado, avisando sobre esta condição e em anexo pode ser enviado um gráfico mostrando o estado do dispositivo.
- **Syslog** – Permite visualizar as mensagens do sistema Linux e armazená-los no banco de dados usado pelo Cacti.
- **Weathermap** – Desenha mapas e diagramas da rede mostrando seu estado atual. É uma maneira fácil de mostrar a topologia da rede.
- **Monitor** – Permite visualizar todos os *hosts* da rede, bem como seu *status*, além de emitir alertas através de sons quando algum dispositivo estiver *off-line*. Permite também desabilitar o monitoramento de um *host*. Equipamentos verdes estão *on-line*. Equipamentos azuis significam que acabaram de ser ligados e estão iniciando a geração de gráficos. Equipamentos vermelhos estão *off-line* e um aviso sonoro é emitido quando estão neste *status*. Estes três tipos de *status* podem ser visualizados na Figura 11.

[2] Recursos adicionais instalados em programas de forma oculta

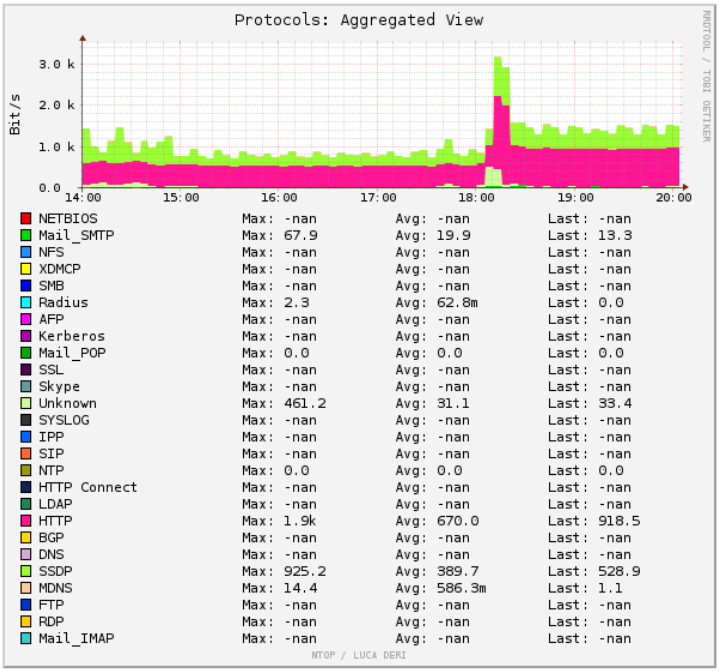
Figura 11 - Tela de monitoramento do *plug-in* "Monitor"



Fonte: Autoria própria. Imagem extraída durante monitoramento da rede.

- **NTop** – É uma ferramenta independente, mas que pode ser integrada facilmente ao Cacti. Através dela é possível identificar “gargalos” na rede e dimensionar a infraestrutura. Dentre várias características desta poderosa ferramenta, podem-se destacar: visualização das estatísticas de tráfego; relatórios de tráfego da rede; identificação das estações na rede e quem está consumindo mais banda. Ainda é possível identificar o tráfego por protocolos utilizados, como no exemplo da Figura 12, retirado do laboratório de testes. Nele é possível identificar os principais protocolos utilizados na rede, tais como: Skype, Netbios, Radius, entre outros.

Figura 12 - Gráfico do NTop



Fonte: Autoria própria. Imagem extraída durante durante monitoramento da rede.

4.4 *Templates*

Os *templates* são modelos existentes de configurações de equipamentos, que já vêm como opção ao se acrescentar um novo dispositivo. Se for instalado um equipamento de rede, como um *switch* ou um roteador, pode-se utilizar um *template* apropriado, que não fará monitoração de itens inexistentes nesse tipo de equipamento, como, por exemplo, espaço em disco rígido.

Como padrão o Cacti traz modelos para configuração dos principais sistemas operacionais, roteadores, *switches* e um padrão para equipamentos baseados no protocolo SNMP de forma geral.

A comunidade de desenvolvedores do Cacti, também fornece novos *templates* que são muito interessantes no monitoramento de redes. A seguir são mostrados alguns que estão disponíveis no *site* do Cacti, na seção *templates*:

- Monitoramento de impressoras – Adiciona para alguns modelos de impressora, tais como HP e Lexmark, a possibilidade de monitorar páginas impressas, nível de *toner* / tinta e tráfego de rede;
- Monitoramento de *no-breaks* – Em alguns modelos de UPS podemos monitorar nível de voltagem, nível da bateria, temperatura e tempo *on-line*.
- Monitoramento de programas e serviços – Há templates específicos para monitoramento de banco de dados, *proxy servers, firewalls, Citrix, Microsoft SQL, Groupwyse, VMWare*.
- Monitoramento de *hardware* completo – Alguns equipamentos têm modelos preparados para sua configuração. É o caso de alguns servidores da Dell, HP e IBM.

O conceito de *templates* desenvolvidas pela comunidade do *site*, aliado ao constante desenvolvimento de *plug-ins*, torna o Cacti em uma ferramenta que está em constante mudança e não a deixa estagnada, sem alterações por muito tempo.

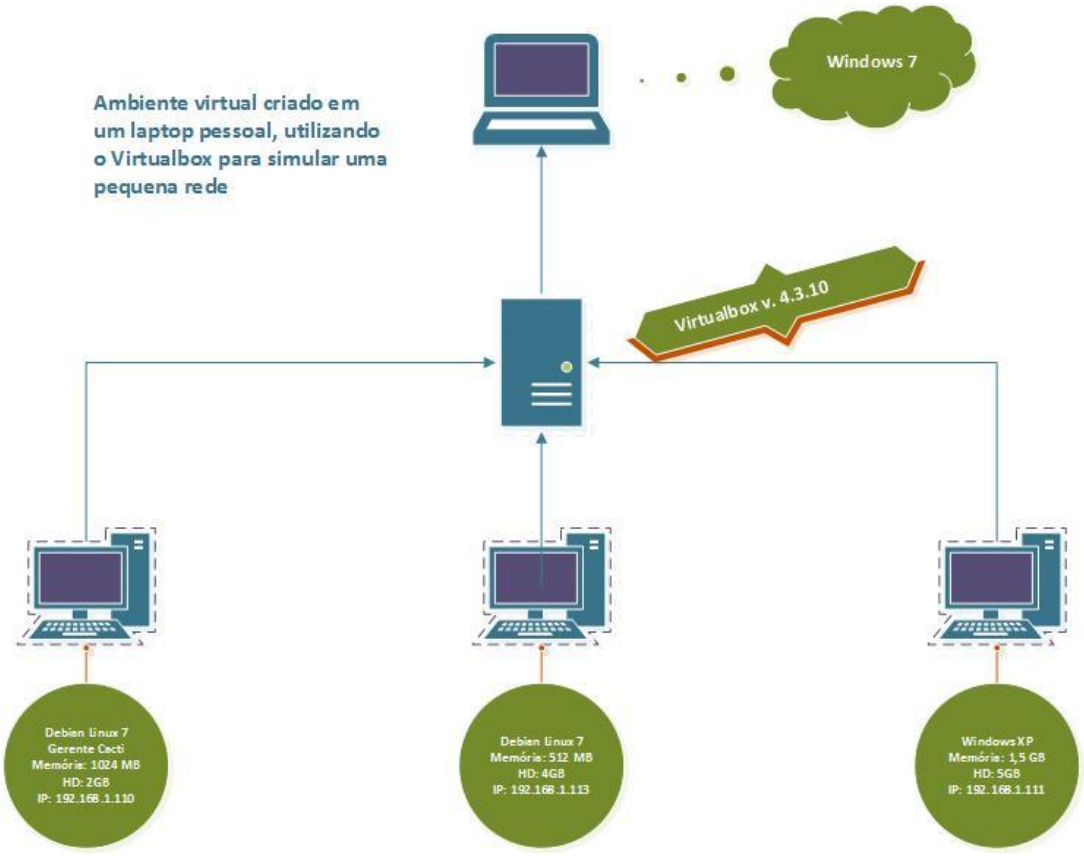
Apresentado o programa, em seguida será apresentado a análise do programa em execução.

5. ANÁLISE EXPERIMENTAL E COMPARATIVA

Para coleta dos dados, foram criados dois ambientes:

1) No primeiro ambiente utilizando o *software* Virtualbox, versão 4.2.24r92790, foram criados três equipamentos interligados em rede e sem acesso externo, conforme a topologia mostrada na Figura 13. Este laboratório foi desenvolvido para os testes mais simples e que não dependiam de nada além do sistema operacional em um *desktop*.

Figura 13 - Topologia virtual



Fonte: Autoria Própria. Topologia desenhada com o auxílio do *software* Visio 2013.

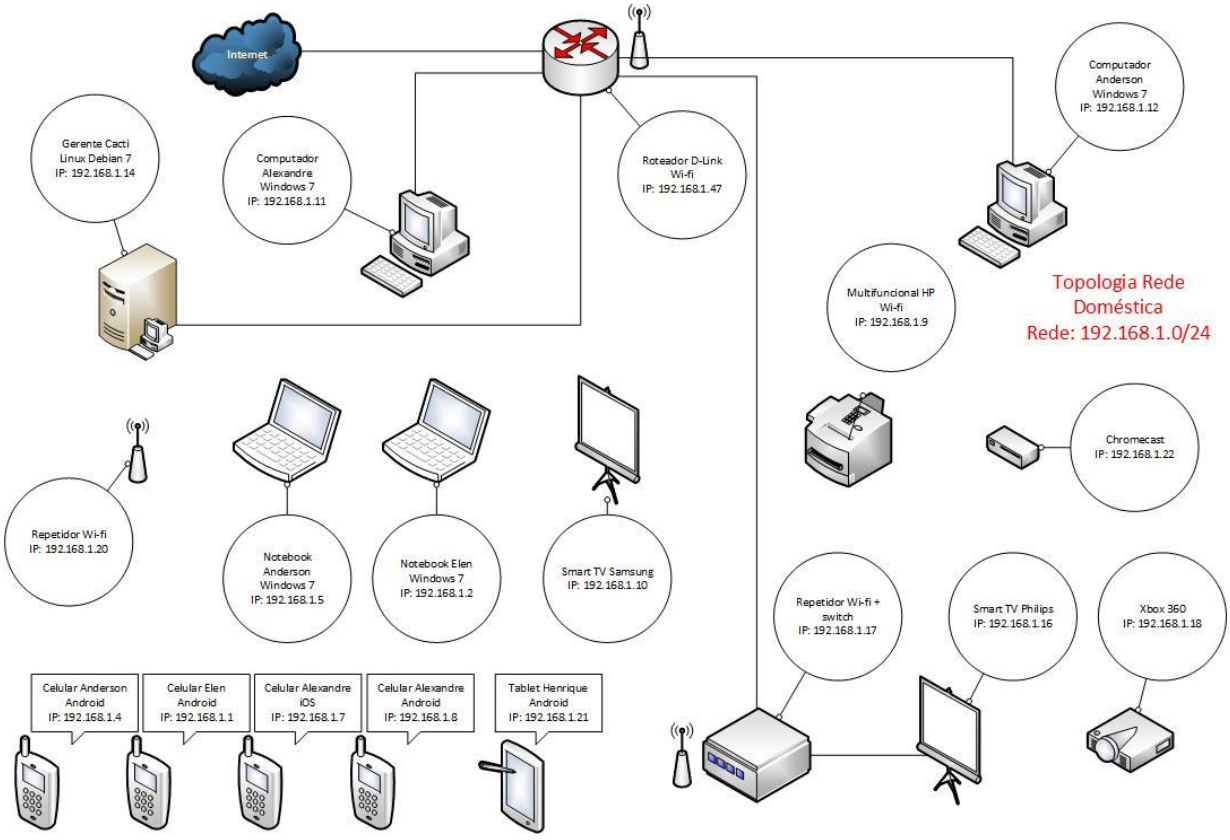
A máquina que emula o gerente, é uma máquina virtual com 1 GB de memória e disco de 2 GB, com o Debian 7 instalado em sua versão básica. Nas máquinas agentes, foram instalados os sistemas operacionais Linux Ubuntu e o Microsoft Windows XP.

Foi elaborada uma topologia de rede interna, sem acesso externo, entre essas máquinas, para o monitoramento de seu funcionamento, que serão descritos e mostrados os tipos de monitoramentos básicos.

Para simular situações de erros, alguns *softwares benchmark* [3] criarão as situações de alerta na rede.

2) Para criar o segundo laboratório, foi utilizada uma rede doméstica convencional, conforme a topologia mostrada na Figura 14.

Figura 14 - Topologia de rede doméstica



Fonte: Autoria Própria. Topologia desenhada com o auxílio do *software* Visio 2013.

[3] Programas que fazem testes e avaliam desempenho de partes do computador, tais como processador, memória, disco rígido.

Para formulação desta rede, foram usados os equipamentos utilizados na casa deste autor, bem como a configuração real das máquinas, a fim de se obter resultados em uma rede real.

Uma máquina foi especialmente configurada para ser o gerente da rede, com a seguinte configuração: Processador AMD Athlon XP 2200, 3GB de memória RAM, HD IDE de 80 GB.

A rede doméstica tem uma grande variedade de equipamentos, mas nem todos têm suporte ao protocolo SNMP, sendo, desta maneira, impossível o seu monitoramento via Cacti, uma vez que esse protocolo é indispensável para seu funcionamento.

Dentre os equipamentos operando na rede estão *Desktops*, *Laptops*, *Smart Phones*, *Tablets*, *Smart* TVs, Roteador Wi-Fi, Repetidores de Sinal Wi-Fi e uma Multifuncional de Rede.

Nesta topologia foram testadas as opções mais avançadas do Cacti, bem como a adição dos *plug-ins* utilizados neste projeto.

5.1 Monitoramento de utilização de CPU

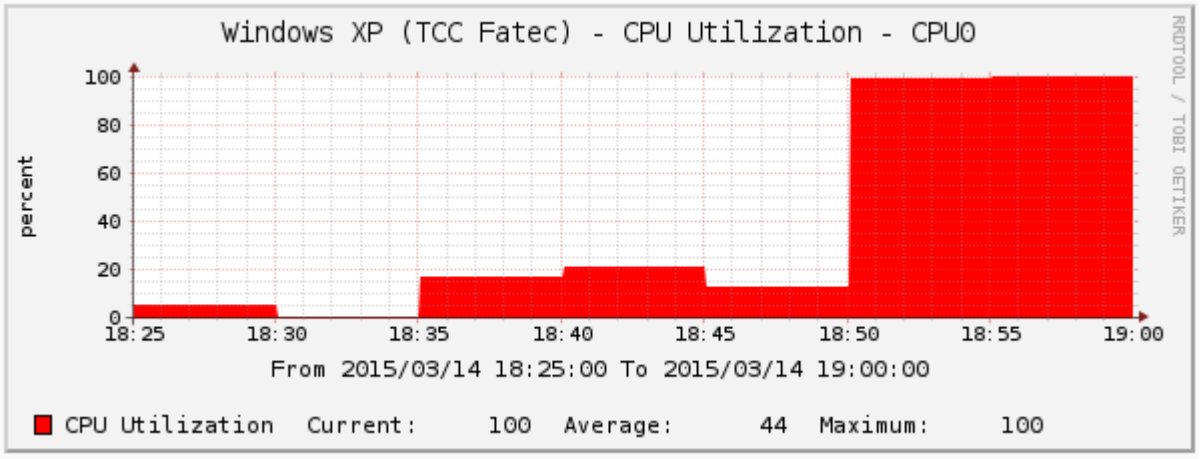
O monitoramento de utilização de CPU alerta o administrador de redes sobre a quantidade que o processador, em porcentagem, está sendo utilizado naquele momento, mostrando a origem de uma eventual lentidão excessiva e servindo de base para posterior *upgrade* do equipamento.

A seguir apresenta-se um gráfico como na Figura 15, na qual o CPU da máquina recebeu uma carga de processamento anormal, através do *software benchmark* Aida64, e alcançando desta forma 100% de utilização de seu poder de processamento. Esse tipo de situação, quando encontrado em um monitoramento do dia-a-dia, poderia indicar a presença de algum *malware*[4], por exemplo.

---

[4] Acrônimo de *Malicious Software*, são programas criados para infiltrar-se em sistemas, de forma ilícita, a fim de causar algum dano, furtar dados ou alterá-los de alguma forma

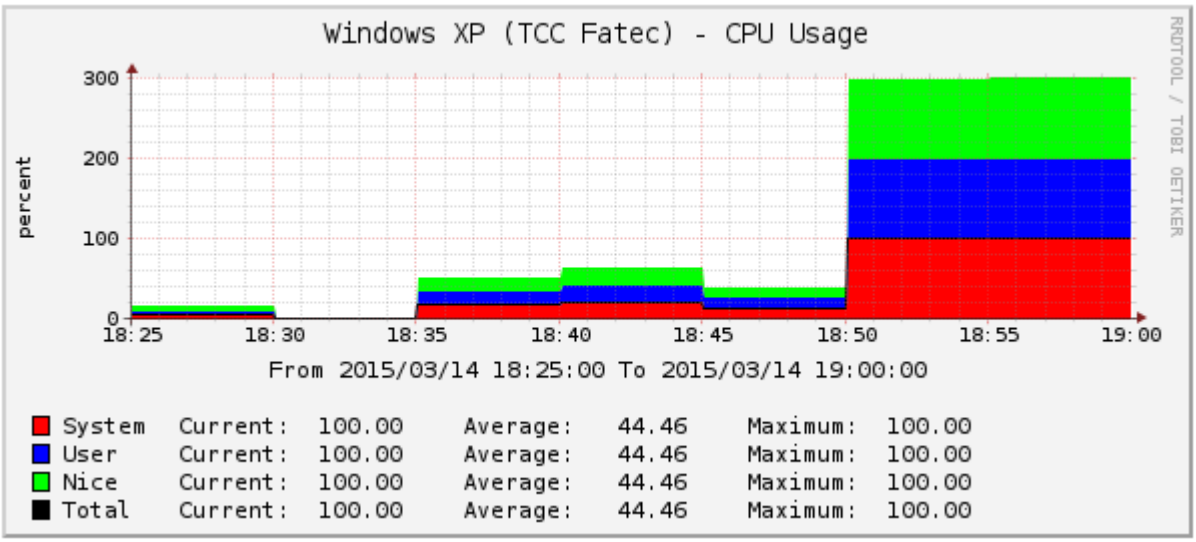
Figura 15 - Teste de *stress* da utilização de CPU



Fonte: Autoria própria. Imagem extraída durante durante monitoramento da rede.

Também é possível o monitoramento indicando quanto que o usuário e o sistema estão consumindo de processador. Esse modo é útil para identificação de *malwares* ou uma limitação do equipamento para o sistema operacional, e o seu gráfico pode ser conferido na Figura 16.

Figura 16 - Uso do CPU por usuário



Fonte: Autoria própria. Imagem extraída durante durante monitoramento da rede.

5.2 Monitoramento de tráfego de rede

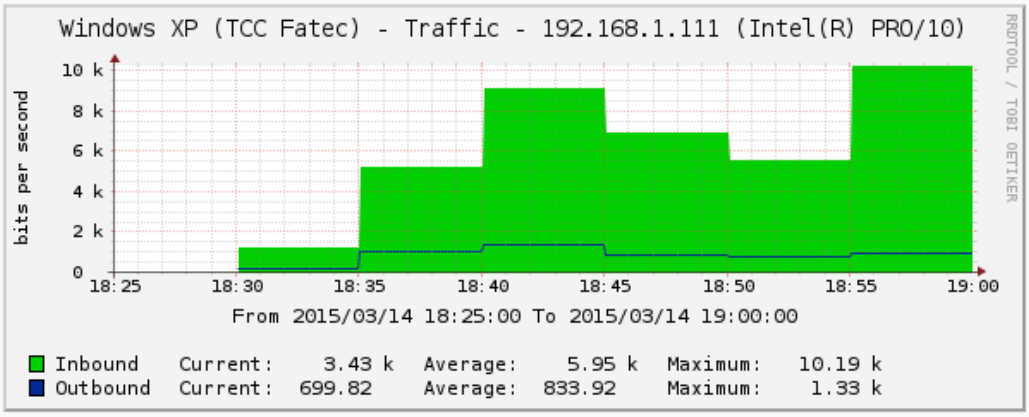
Da mesma maneira que feito nos testes anteriores, também foi monitorado uma placa de rede.

Neste modo, podem ser verificadas instabilidades no sistema, provindas do tráfego de rede. É possível verificar através do horário, os picos de uso da banda, quais os equipamentos que estão consumindo mais *link*, e até porções da rede que podem estar mais comprometidas.

Também seria possível o controle de atividades suspeitas, tais como acesso fora do horário de expediente, excesso de requisições a um determinado equipamento, que pode indicar uma tentativa de invasão, por exemplo.

A Figura 17 apresenta um gráfico na qual é mostrado o consumo de banda produzido por um equipamento, e que durante o pico de utilização, chega a consumir quase toda a capacidade da placa de rede.

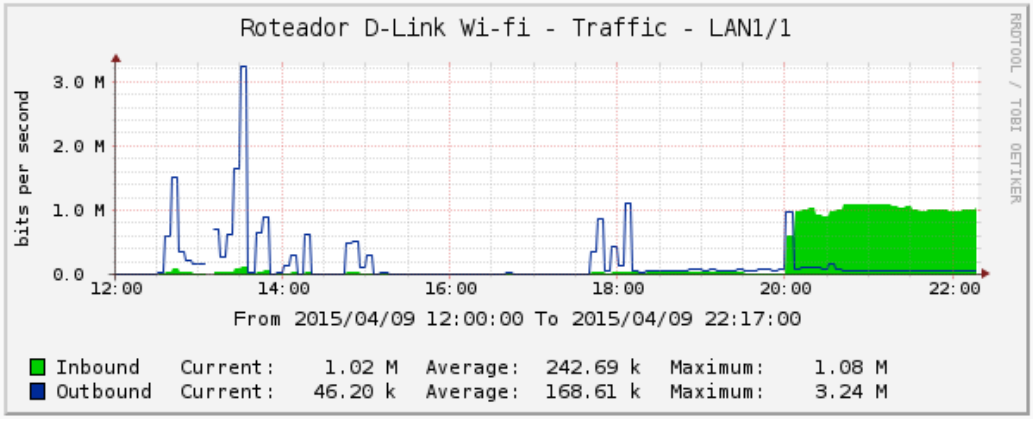
Figura 17 - Teste de *stress* da placa de rede



Fonte: Autoria própria. Imagem extraída durante durante monitoramento da rede.

No gráfico da Figura 18 é mostrada a taxa de download e upload numa das portas de um roteador wi-fi. É possível verificar na linha azul a quantidade de dados que saem do equipamento ligado à esta porta, e na linha verde, os dados que são enviados ao dispositivo.

Figura 18 - Monitoramento de porta do roteador



Fonte: Autoria própria. Imagem extraída durante durante monitoramento da rede.

5.3 Monitoramento de espaço utilizado em disco

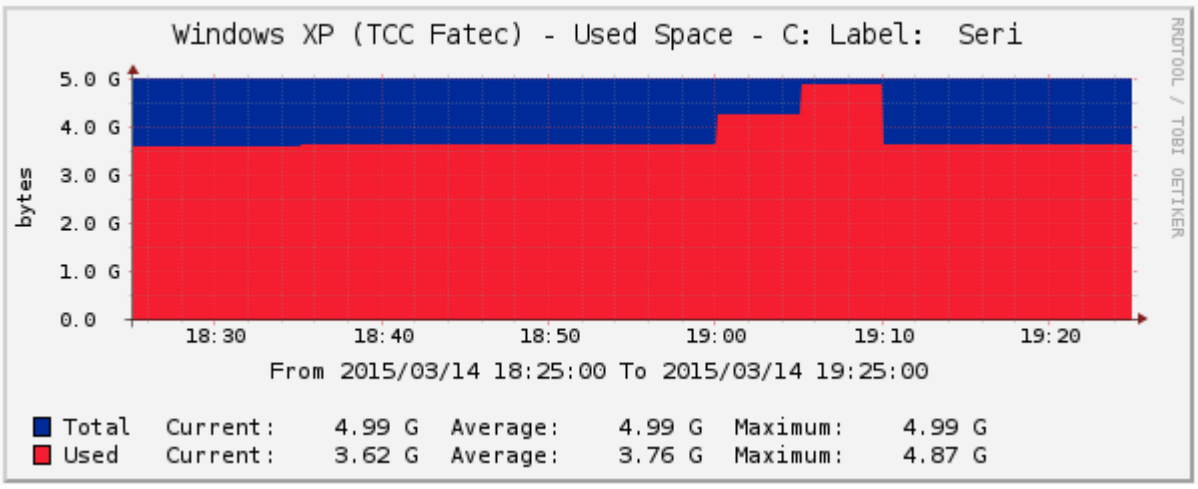
O monitoramento de espaço disponível em disco é útil para evitar que o sistema se torne lento e que arquivos não possam ser armazenados. É útil também para identificar problemas de má configuração do sistema, como limitação do espaço em disco para gravação de *logs*[5] do sistema. Em um servidor de arquivos, pode-se acompanhar o crescimento de dados mensalmente, por exemplo, e estipular um prazo para que o disco fique cheio. Dessa forma pode antecipar a um eventual problema de falta de espaço para armazenamento.

Para reproduzir o alerta, não foram utilizados programas *benchmark*. Apenas arquivos foram copiados para a unidade. Na Figura 19 foi utilizada uma das máquinas virtuais, configurada com 5 GB de espaço, e que já estava com mais de 3,5 GB ocupados pelo sistema operacional. É possível verificar o consumo do disco após a cópia do arquivo e a redução após o arquivo ser deletado da máquina.

O disco estava ocupado em um pouco mais de 3,5 GB de dados e com a cópia de um arquivo de 1,3 GB; o gráfico abaixo indica a quase totalidade do espaço em disco sendo ocupado.

[5] Registro de eventos relevantes em um sistema.

Figura 19 - Teste de *stress* do disco rígido



Fonte: Autoria própria. Imagem extraída durante durante monitoramento da rede.

5.4 Monitoramento de memória

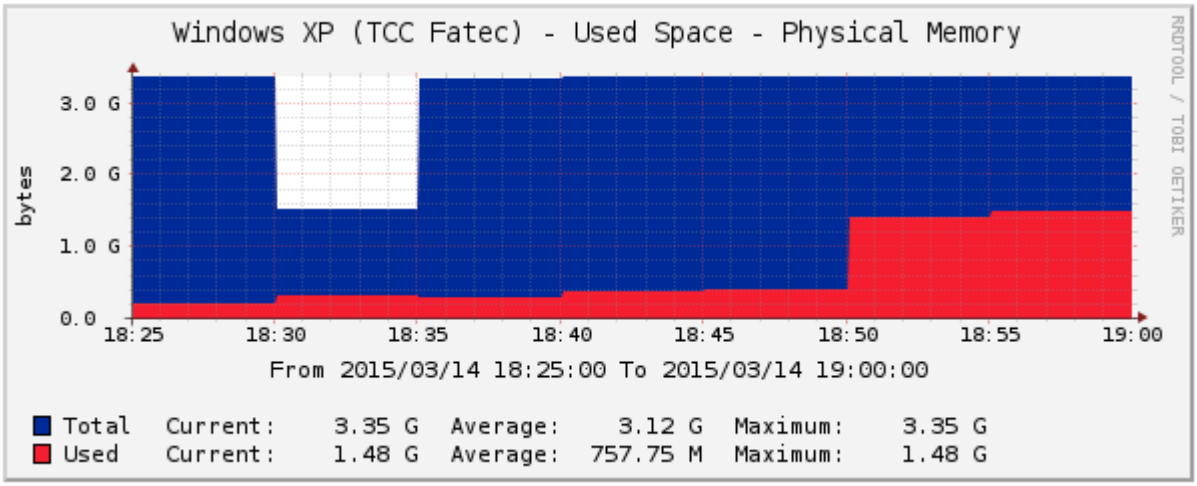
Esse tipo de teste monitora além da memória RAM do equipamento, também a memória virtual[6]. Útil para identificar a necessidade de *upgrade* de memória ou disco rígido. Na Figura 20 foi executado um teste de memória apenas abrindo alguns programas e documentos para mostrar a ocupação da memória RAM.

É possível verificar que o sistema tinha em torno de 3 GB de memória disponível, mas com os processos sendo executados não havia consumo superior a 1,5 GB.

Com esse tipo de informação, há dados para mostrar que esse equipamento tem memória de sobra para trabalhar, e o gasto com um *upgrade* de memória não é necessário.

[6] Armazenamento secundário de dados no disco rígido, o qual é utilizado quando a memória RAM está cheia.

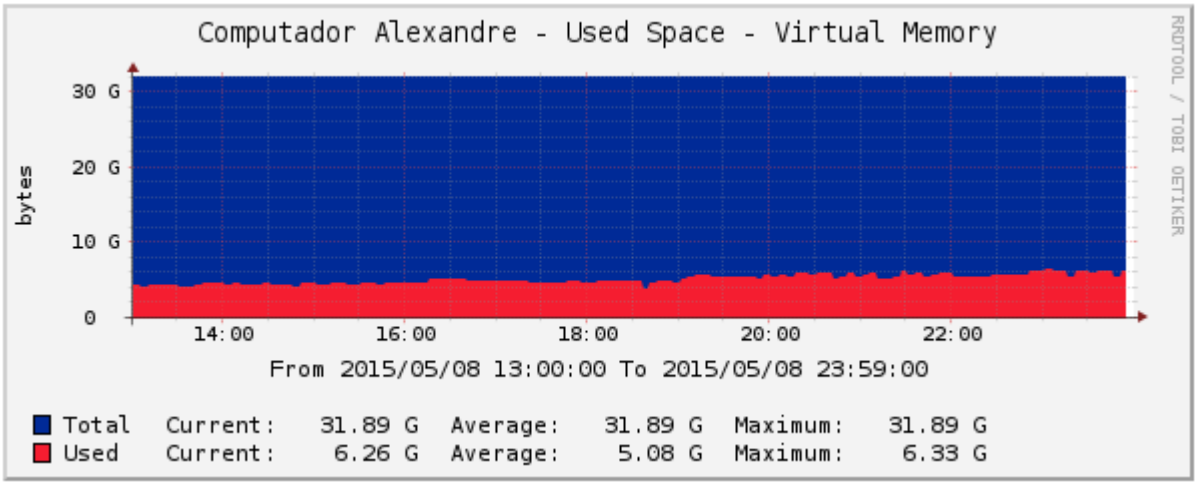
Figura 20 - Teste de consumo da memória RAM



Fonte: Autoria própria. Imagem extraída durante durante monitoramento da rede.

Na Figura 21 é indicado o consumo de memória virtual numa máquina que tinha reservado 30 GB de espaço em disco. Mesmo sendo utilizado durante uma seção de jogos *on-line*, não chega nem próximo de 25% do uso, pois o equipamento tem uma boa quantidade de memória RAM.

Figura 21 - Uso da memória virtual



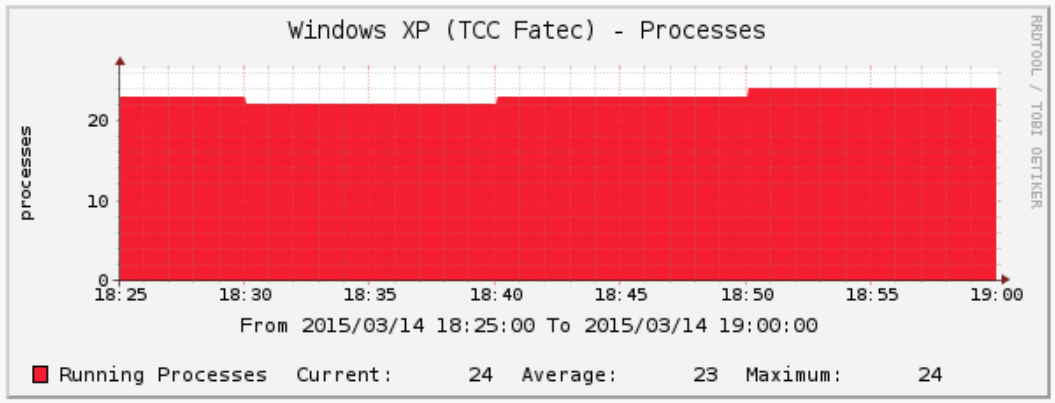
Fonte: Autoria própria. Imagem extraída durante durante monitoramento da rede.

5.5 Monitoramento de processos em execução no sistema operacional

Esse tipo de monitoramento é específico para controlar a quantidade de processos em execução num sistema operacional. Quando o sistema está em atividade, cada programa carregado em memória, seja ele parte do próprio sistema operacional ou um aplicativo qualquer, como um editor de textos, irá abrir um ou mais processo em execução no sistema. Com base em alterações na quantidade de processos diários executados no sistema, uma alteração drástica poderia indicar a presença de um *malware*, por exemplo.

Para um uso eficiente deste tipo de monitoramento, é necessário ter armazenado um período longo deste equipamento para que se possa comparar seu comportamento e definir se há alguma alteração brusca. Na Figura 22 revela-se a quantidade de processos sendo executado no Windows XP, ficando em torno de 25 processos.

Figura 22 - Monitoramento de processos no sistema



Fonte: Autoria própria. Imagem extraída durante durante monitoramento da rede.

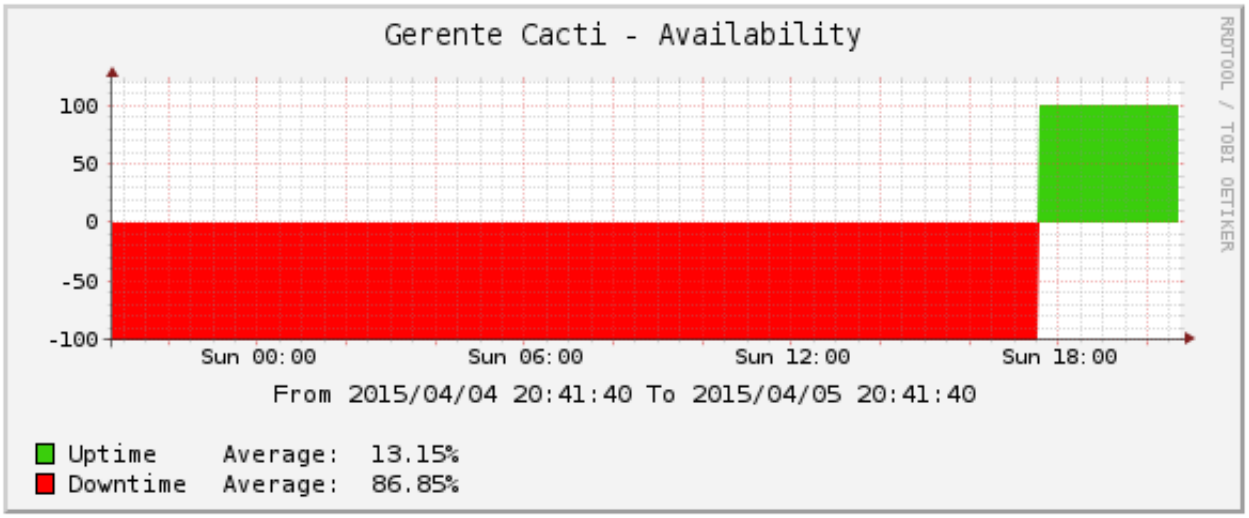
5.6 Monitoramento de disponibilidade do equipamento

Através deste de monitoramento é possível visualizar o tempo em que um equipamento esteve ligado ou desligado. Com base nesta informação pode-se definir se o equipamento está sendo utilizado durante o período em que ele deve estar operacional. Também pode-se verificar se um equipamento foi utilizado fora do horário de trabalho, por exemplo.

Também é útil em casos onde há acordos de prestação de serviço, pois se define a quantidade de tempo que um equipamento deve estar disponível.

Na Figura 23, visualizaremos que o equipamento esteve indisponível até aproximadamente às 17:30h do domingo, dia 05 de abril de 2015.

Figura 23 - Monitoramento de disponibilidade de equipamento



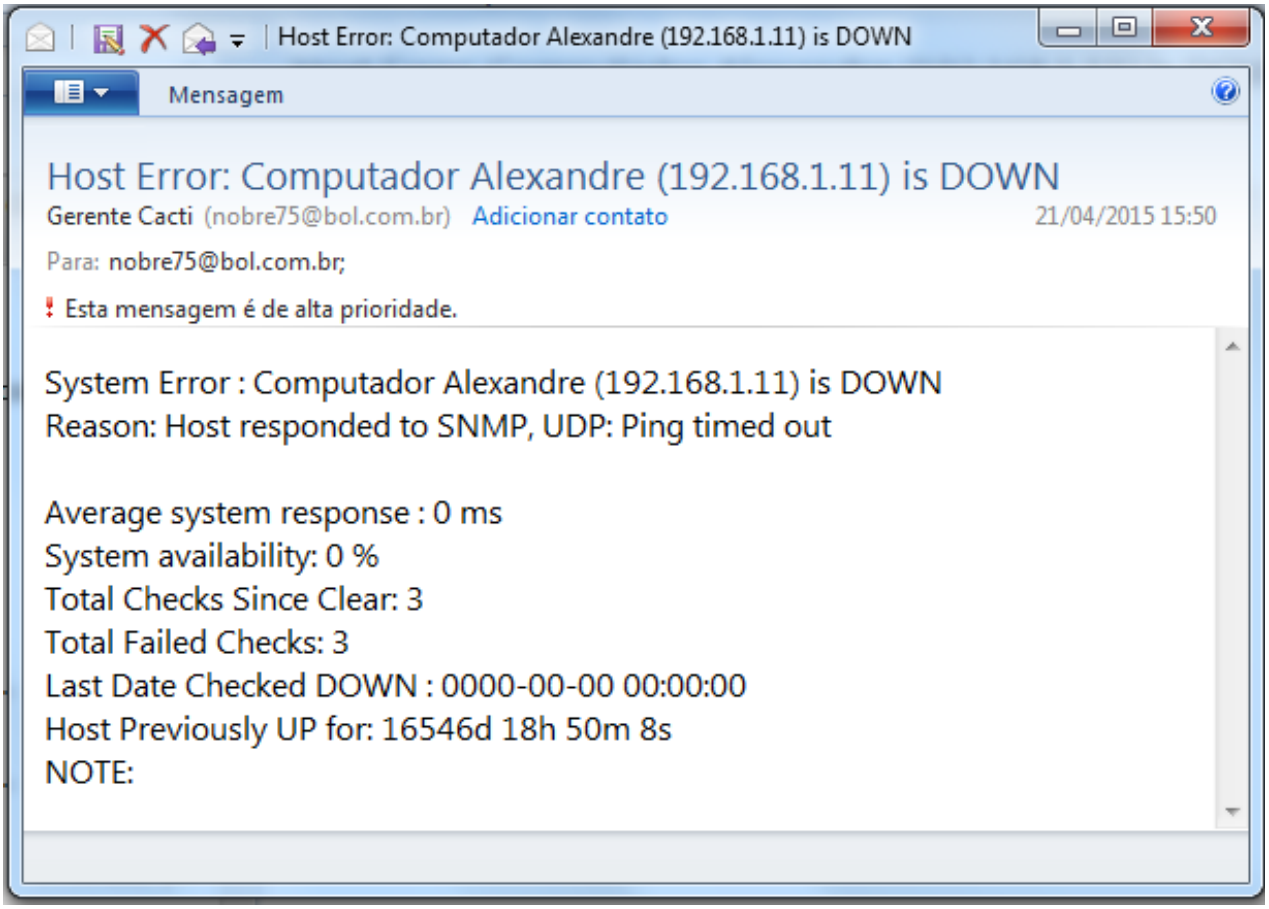
Autoria: Autoria própria. Imagem extraída durante durante monitoramento da rede.

Ainda no gráfico da Figura 23, é possível verificar qual a porcentagem de tempo que o equipamento está operacional (*Uptime*) e fora de operação (*Downtime*). Esta informação é útil para mensurar a confiabilidade de um equipamento na rede.

5.7 Recebimento de alertas por *e-mails*

Os alertas mais importantes podem ser recebidos por *e-mail*, por meio de um *plug-in* específico para essa função. No caso deste trabalho foi utilizado o Thold. No exemplo abaixo, foram configurados dois tipos de alertas. O primeiro, na Figura 24, avisou que um equipamento estava *off-line*. Desta forma, caso um equipamento seja indispensável para o negócio, um alerta será enviado logo que ele não consiga mais ser encontrado pelo gerente Cacti.

Figura 24 – Mensagem de aviso de *host off-line*

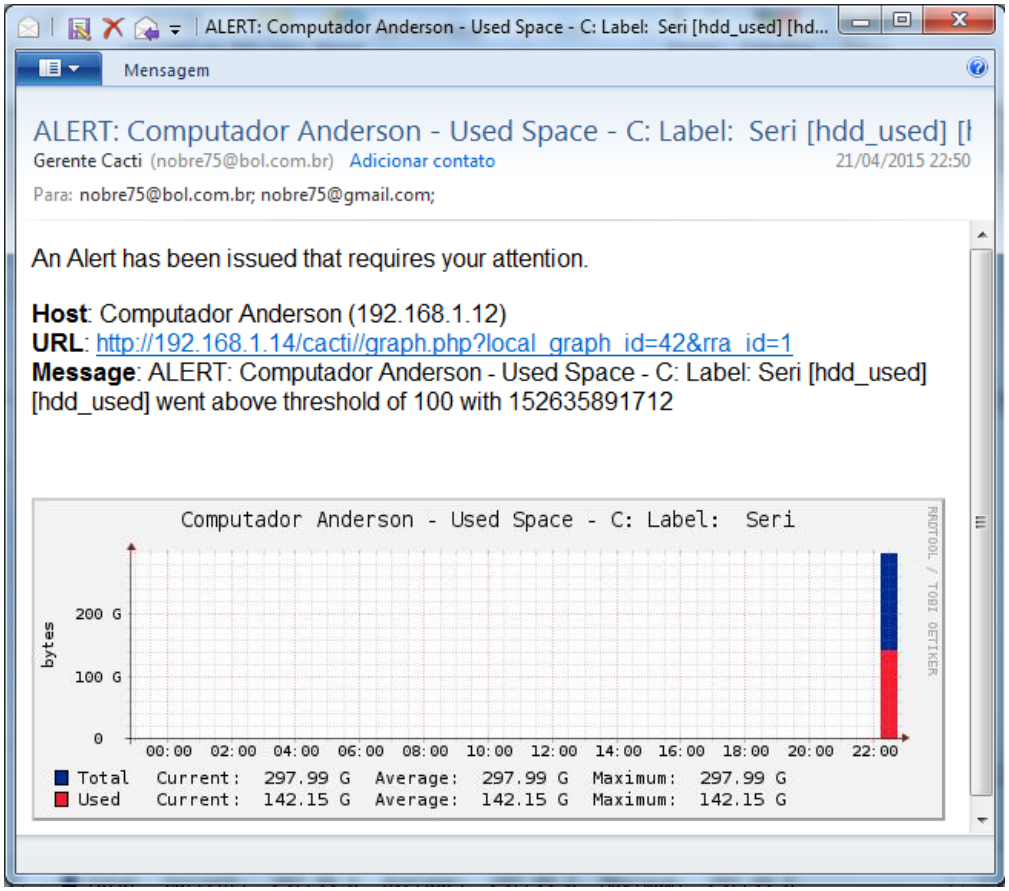


Autoria: Fonte própria. Mensagem recebida via *software* Windows Live Mail.

O segundo gráfico, mostrado na Figura 25, foi configurado para que um aviso seja enviado quando um disco rígido ultrapassar os 100 GB de espaço utilizado, com o uso do gráfico referente ao equipamento.

É possível configurar para que ocorra aviso sobre qualquer equipamento em qualquer um dos gráficos gerados pelo Cacti. Basta configurar um alerta para o gráfico do equipamento, indicando um valor mínimo e um valor máximo para o eixo *y*, para que um alerta seja enviado indicando que os valores foram ultrapassados.

Figura 25 – Mensagem de alerta de disco

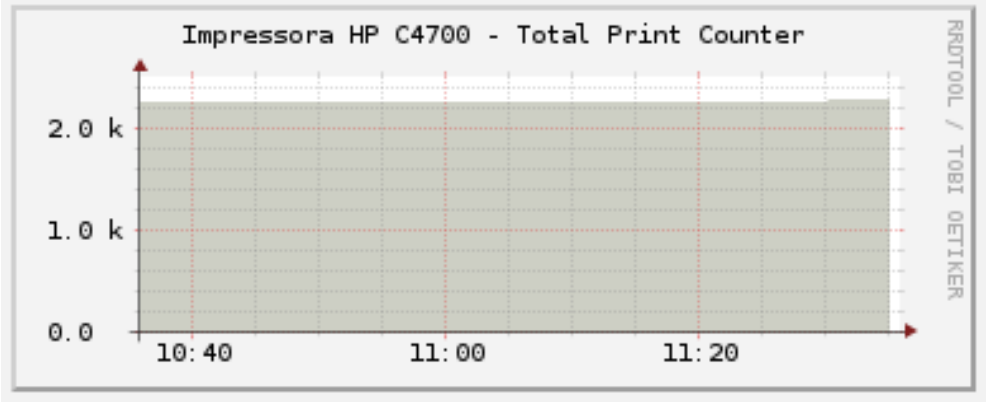


Autoria: Fonte própria. Mensagem recebida via *software* Windows Live Mail.

5.8 Monitoramento de impressoras

Através de um *template* específico foi possível monitorar o tráfego de rede de uma impressora, quantidade de páginas impressas no dia e um contador geral de impressões. Dependendo do modelo da impressora, também pode-se controlar o nível de tinta ou *toner* disponível no equipamento. Abaixo segue-se uma demonstração que revela como foi feito o monitoramento de uma multifuncional HP C4700. A Figura 26 apresenta o contador de páginas total do equipamento, que estava em 2.277 páginas já impressas. Este tipo de monitoramento é útil para programar manutenções preventivas, ou troca de suprimentos na impressora.

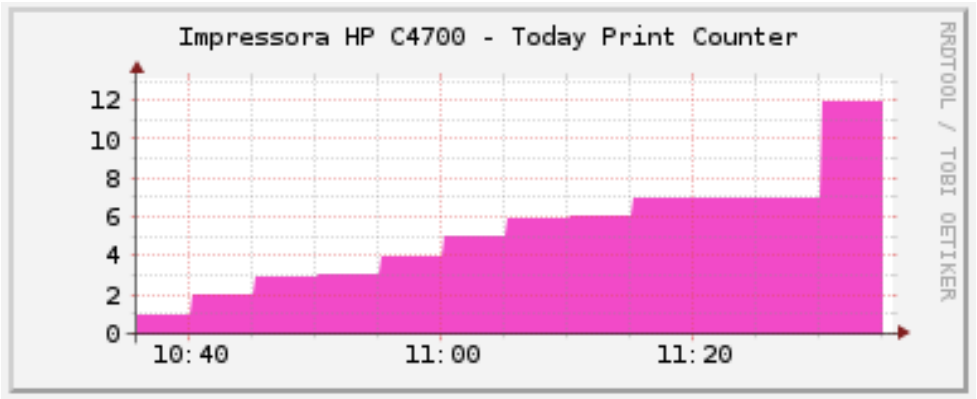
Figura 26 - Monitoramento de páginas impressas total



Autoria: Autoria própria. Imagem extraída durante durante monitoramento da rede.

Na Figura 27 apresenta um gráfico de impressões diárias, e foi enviado 12 impressões durante um certo intervalo de tempo para que o contador do gráfico fosse incrementado aos poucos.

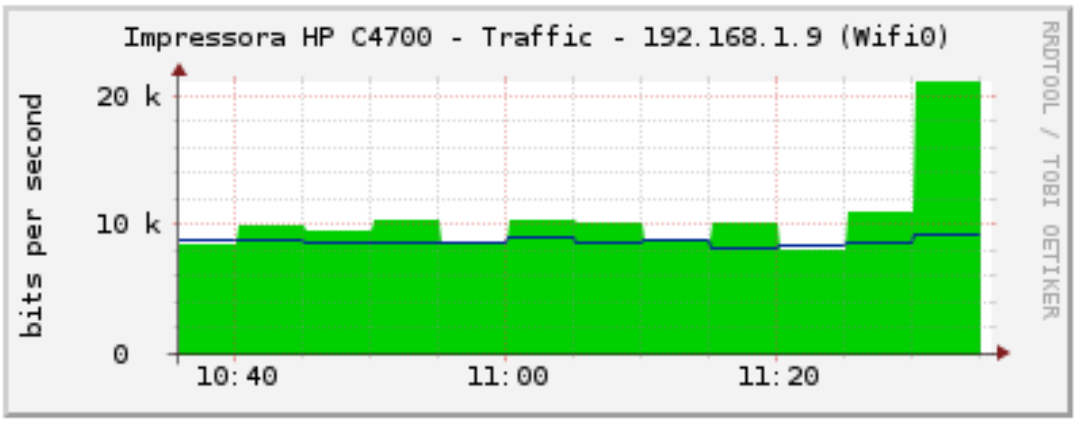
Figura 27 - Monitoramento de páginas impressas no dia



Autoria: Autoria própria. Imagem extraída durante durante monitoramento da rede.

Como se trata de uma impressora *wireless*, também foi possível monitorar o seu consumo de rede, conforme Figura 28, onde é apresentado o *download* de dados (verde) e o *upload* (azul).

Figura 28 - Monitoramento de consumo de banda pela impressora



Autoria: Autoria própria. Imagem extraída durante durante monitoramento da rede.

Este tipo de monitoramento é útil para identificar equipamentos que não estejam sendo suficientes para suprir a demanda de solicitações ou uso indevido do sistema de impressões baseado no uso diário.

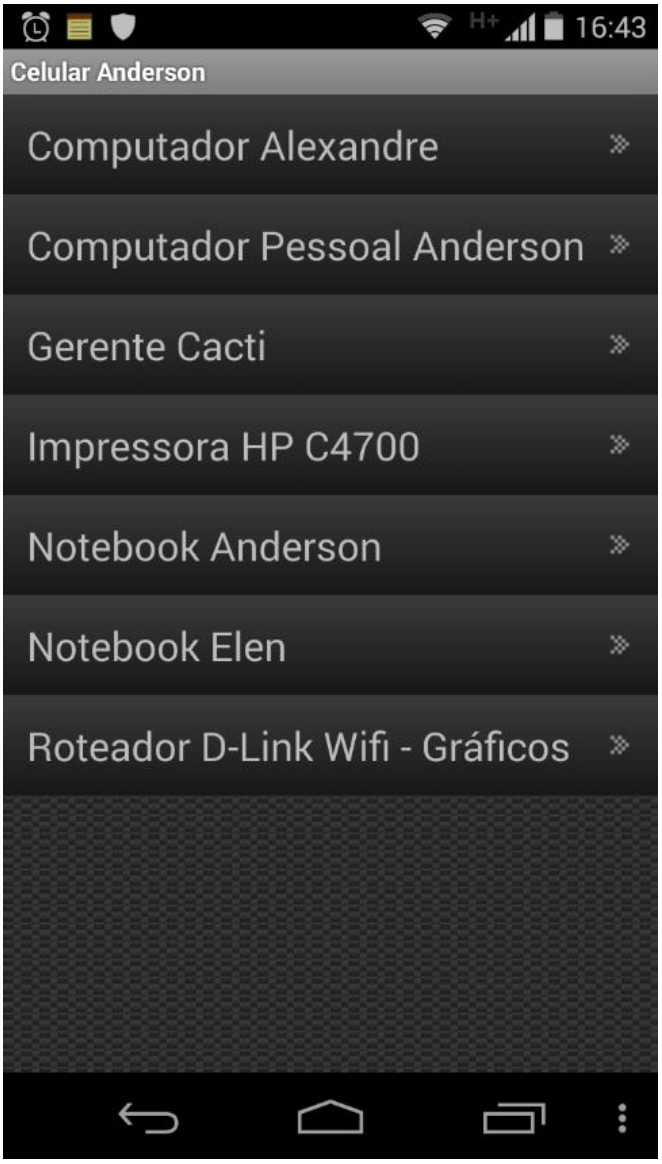
5.9 *Cacti Viewer*

Outra vantagem do monitoramento da rede pelo Cacti está no uso de um visualizador de gráficos, a partir de dispositivos móveis. O *software* gratuito Cacti Viewer proporciona a visualização de gráficos de forma simples e rápida através de qualquer dispositivo com o sistema operacional Android ou iOS, conforme a Figura 29 mostra logo a seguir. Na imagem é possível verificar todos os dispositivos que estão sendo monitorados pelo gerente Cacti.

Para instalação do sistema, basta fazer o *download* do programa no gerenciador de aplicativos do dispositivo móvel e na inicialização será solicitado para que seja informado o IP do gerente, juntamente com o usuário e a senha de acesso.

Para uma maior segurança, é possível criar um perfil no gerenciamento de usuários do Cacti, que permite, por exemplo, a visualização de gráficos.

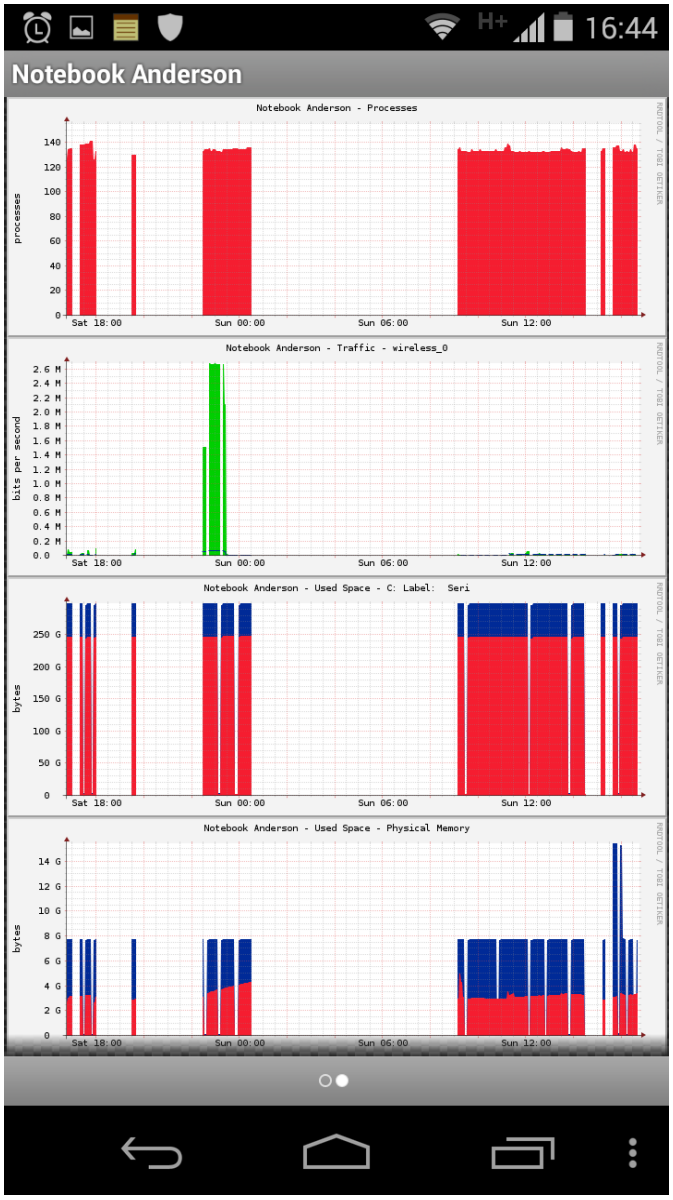
Figura 29 – Dispositivos que podem ser monitorados



Fonte: Autoria própria. Imagem extraída via *smartphone*.

O sistema permite visualização de todos os gráficos armazenados no gerente, porém não é permitido que seja feita nenhuma alteração nas configurações. A Figura 30 apresenta alguns gráficos de um dos dispositivos. É possível selecionar somente um dos gráficos e escolher qual o período, a partir de data e hora, que se quer visualizar os dados.

Figura 30 - Gráficos visualizados pelo Cacti Viewer



Fonte: Autoria própria. Imagem extraída via *smartphone*.

Como o próprio nome diz, o Cacti Viewer é um aplicativo desenvolvido somente para visualização dos gráficos, não sendo possível o acesso a nenhuma outra função do Cacti ou alteração de configurações. Sua grande vantagem está no acesso móvel, dispensando assim, o uso de um equipamento fixo para o monitoramento.

CONSIDERAÇÕES FINAIS

O uso da ferramenta Cacti traz diversos benefícios no monitoramento de uma rede, mas há algumas ressalvas a serem consideradas.

O *software* mostra de maneira prática e de fácil compreensão, situações que podem vir a se tornar um problema, mas não corrige nenhuma delas.

Existem falhas perceptíveis tais como não poder gerenciar versões desatualizadas de aplicativos e monitoração de processos específicos em sistemas operacionais. Também a limitação de receber alertas somente no sistema ou por *e-mail* e não haver a opção de recebimento por SMS[7], é algo que poderia ser um diferencial nos dias atuais.

Na área de gestão de TI, existe uma seção, que discute alguns modelos de gestão de equipamentos, como o Cobit e o Itil, denominada *Capacity Planning*. Essas seções elaboram formas de medir a capacidade dos equipamentos numa estrutura de rede, e nesse caso o Cacti se torna uma ferramenta muito mais útil.

A partir dos gráficos gerados, pode-se identificar diversos *hardwares* em uma rede que não estão conseguindo suportar a demanda de processos que lhe são dirigidas. Com facilidade pode-se identificar processadores, memórias, discos rígidos, equipamentos de rede, impressoras e *no-breaks* trabalhando no limite, e a partir desses dados, elaborar de forma concreta, um plano de atualização de equipamentos.

Mas o Cacti não se limita somente a esse tipo de planejamento. Com seus gráficos, é possível, por exemplo, verificar atividades na rede fora do horário de trabalho, identificar setores da rede onde há maior consumo de banda e até verificar quais tipos de protocolos estão consumindo mais a banda do ambiente. É possível diferenciar se a banda está sendo gasta com navegação via *browser*, FTP, *e-mail* ou *streaming* de vídeo, entre outros, e identificar de qual estação está partindo este consumo.

A adição de *plug-ins* e *templates*, criadas pela própria organização e por usuário do *site*, traz sempre diversas inovações ao sistema e o mantém atualizado com as

[7] Serviço de mensagens de texto curto, através de telefones celulares.

tendências do mercado. Equipamentos, tais como o *Blade Center* H, fabricado pela IBM, e que reúne diversos servidores em uma só máquina, tem *templates* projetados, que fazem o monitoramento de diversas funções, desde monitoramento de ventoinhas e temperatura, até disponibilidade dos servidores configurados.

De forma geral, é uma ferramenta muito válida, pois não necessita de *hardware* poderoso, podendo ser configurada em equipamentos de pouco poder de processamento e todos os *softwares* necessários para seu funcionamento são totalmente gratuitos. Desde o sistema operacional, banco de dados e *web server*, até as novas ferramentas e atualizações que são disponibilizadas para o produto.

Como trabalhos futuros, propõe-se a integração desta ferramenta com outras, tais como *softwares* que incorporem lista de patrimônio, atualizações de sistemas ou que possa fazer algum tipo de correção ou interação com as falhas encontradas, a fim de incrementar o poder de monitoramento e abranger uma quantidade maior de dispositivos. Sugere-se que um novo projeto de pesquisa seja feito com a utilização do Cacti, integrado à ferramenta Zabbix (PUSKA, 2011), Nagios (PONTUAL,2009) ou Pandora (BUENO, 2012), por exemplo.

REFERÊNCIAS

ABNT (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS). **NBR ISO/IEC 27002:2005;** Tecnologia da informação; Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

BERRY, Yan; *et al*. **The Cacti Manual**. Publicado em 2012. Disponível em: <www.cacti.net/downloads/docs/pdf/manual.pdf>. Acesso em: 01 out. 2014.

BUENO, Edimilson Moreira. **Monitoramento de Redes de Computadores com Uso de Ferramentas de *Software* Livre**. 2012. 73 f. Monografia (Especialista em *Software* Livre Aplicado à Telemática) Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná, Curitiba, 2012.

CACTI. **The Cacti Group**: The Complete RRDTool-Based Graphing Solution, 2001-2015. Disponível em: <http://www.cacti.net>. Acesso em: 17 maio 2015.

DANTAS, Marcus Leal. **Segurança da Informação;** Uma abordagem focada em Gestão de Riscos. Olinda, Pernambuco: Livro Rápido, 2011.

LOPES, Raquel Vigolvino; SAUVÉ, Jacques Philippe; NICOLETTI, Pedro Sérgio. **Melhores Práticas para Gerência de Redes de Computadores**. Rio de Janeiro: Campus, 2003.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet;** Uma Abordagem Top-Down. 5ª Ed. São Paulo: Pearson, 2010.

NIC.BR (NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR). **Introdução ao gerenciamento de redes;** Parte 4; SNMP. Publicado em 13 de abril de 2014. Disponível em: < https://www.youtube.com/watch?v=PqgDoG4gLK0>. Acesso em: 09 maio 2015.

PONTUAL, Rogério Pereira. **Projeto Baseado no Nagios para Monitoração de Autorizadores de TEF**. 2009. 64 f. Monografia (Bacharel em Engenharia da Computação), Escola Politécnica de Pernambuco, Recife. 2009. 64 f.

PUSKA, Alisson Andrey. **Solução de Gerenciamento de Redes Utilizando o Sistema de Código Aberto:** Zabbix. 2011. 62 f. Monografia (Especialização em Gerenciamento de Servidores e Equipamentos de Redes) – Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná, Curitiba.

RFC 1155. **Structure and Identification of Management Information for TCP/IP - based Internets**. USA: IETF, 1990. Disponível em: <https://www.ietf.org/rfc/rfc1155.txt>. Acesso em: 16 fev. 2015.

RFC 1157**. A Simple Network Management Protocol (SNMP)**. USA: IETF, 1990. Disponível em: <https://www.ietf.org/rfc/rfc1157.txt>. Acesso em: 16 fev. 2015.

RFC 3418. **Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)**. USA: IETF, 2002. Disponível em: <https://www.ietf.org/rfc/rfc3418.txt>. Acesso em: 16 fev. 2015.

RRDTOOL, Logging & Graphing. **About RRDTool**. Disponível em:<http://oss.oetiker.ch/rrdtool/index.en.html>. Acesso em: 09 maio 2015

WIKIPEDIA. **Round-Robin**. Disponível em: <https://pt.wikipedia.org/wiki/Round-robin>. Acesso em: 09 maio 2015