Centro Universitário de Brasília

Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

ANDERSON DA COSTA FERREIRA

MONITORAMENTO DE REDES COM CACTI

Brasília

2017

ANDERSON DA COSTA FERREIRA

MONITORAMENTO DE REDES COM CACTI

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu*,em Redes de Computadores com Ênfase em Segurança.

Orientador: Dr. José Eduardo Malta de Sá Brandão

Brasília

2017

ANDERSON DA COSTA FERREIRA

MONITORAMENTO DE REDES COM CACTI

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação Lato Sensu,em Redes de Computadores com Ênfase em Segurança.

Orientador: Dr. José Eduardo Malta de Sá Brandão.

Brasília, ___ de _____ de 2017.

Banca Examinadora

_____

Prof. Msc Francisco Javier de Olbadia Diaz

_____

Prof. Dr. Gilson Ciarallo

A Deus, que se mostrou criador, que foi criativo. Seu fôlego de vida em mim, me foi sustento e me deu coragem para questionar realidades e propor sempre um novo mundo de possibilidades.

AGRADECIMENTOS

Primeiramente, a Deus meu senhor e salvador, que me deu forças e iluminou o meu caminho durante esta caminhada.

Aos meus pais, irmãos, minha esposa Bárbara, e a toda minha família que, com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa de minha vida.

Ao professor orientador Brandão, por seus ensinamentos, paciência e confiança ao longo do trabalho.

RESUMO

O objetivo do presente trabalho consiste em apresentar o gerenciamento de redes através da ferramenta *Cacti*, que é um software para monitoramento da disponibilidade de máquinas e serviços de uma rede de computadores e também para inserção dos ativos de redes que se pretendam gerenciar por meio dessa ferramenta. Esta ferramenta permite transformar os dados coletados pelo *Cacti* em mapas, desta maneira, centralizando as informações da rede gerenciada, tendo como propósito facilitar a tarefa de gerenciamento de redes, monitorar de forma clara e precisa os ativos da rede de computadores, proporcionar a disponibilidade dos recursos e gerar relatórios sobre infraestruturas de rede. Desta forma, é possível dispor de uma ferramenta gratuita para monitoramento de redes de computadores, de fácil interação com o usuário, tanto na adição de novos dispositivos a serem monitorados como também na interpretação de seus gráficos, que é bastante intuitiva, dada a forma como são apresentados.

Palavras-chave: Cacti. Monitoramento de Redes. Gerenciamento de Redes.

ABSTRACT

The objective of this work is to present the management of networks through the Cacti tool, which is a software for monitoring the availability of machines and services of a computer network and also for insertion of network assets that are intended to be managed through this tool. This tool allows transform the data collected by Cacti into maps, in this way, centralizing the information of the managed network, aiming to facilitate the task of network management, to monitor clearly and precisely the assets of the computer network, to provide the availability of Resources and generate reports on network infrastructures. In this way, it is possible to have a free tool for monitoring computer networks, easy interaction with the user, both in adding new devices to be monitored as well as in the interpretation of their graphs, which is quite intuitive, given the way they are presented.

***Keywords**:* Cacti. Monitoring Networks. Network Management.

SUMÁRIO

INTRODUÇÃO

Não é possível prever quando uma fonte de alimentação vai se queimar, quando um servidor vai falhar, quando a largura de banda da rede cai, quando um roteador simplesmente para de funcionar, quando sua LAN é invadida e assim por diante. O gerenciamento de redes fornece instrumentos para que o administrador de redes consiga manter a rede funcionando o maior tempo possível, com o mínimo de interrupções, atendendo as expectativas dos usuários e satisfazendo as necessidades de uma empresa. Monitoramento de rede eficaz ajudará a lidar com tais situações e minimizar o tempo de inatividade.

O objetivo do presente trabalho é: apresentar uma solução de gerenciamento e monitoramento de redes, por meio de uma ferramenta que facilite o serviço dos administradores de redes. A ferramenta de monitoramento também ajudará a coletar informações periódicas sobre a rede, gerando arquivos de log e gráficos de desempenho das capacidades e respostas do sistema. Com esses dados, será possível otimizar uma infraestrutura de rede e desempenho. Para alcançar esses objetivos, alguns pontos foram observados, como: a rede deve, além de oferecer recursos e serviços, ser rápida e segura e, sobretudo estar sempre disponível.

O CACTI é uma ferramenta que recolhe e exibe informações sobre o estado de uma rede de computadores através de gráficos, e ela foi escolhida para ser observada neste estudo. Esta ferramenta foi desenvolvida para ser flexível, de modo a se adaptar facilmente a diversas necessidades, bem como ser robusto e fácil de usar, além de monitorar o estado de elementos de rede, de programas, a largura de banda utilizada e o uso de CPU.

Espera-se demonstrar com este estudo a importância da implementação de um software de monitoramento de rede, assim como a necessidade de monitorar e administrar uma rede de computadores.

O presente estudo foi estruturado em 3 capítulos, de modo a fornecer uma visão ampla e prática sobre os objetivos a serem alcançados.

O primeiro capítulo proporciona uma análise sobre o gerenciamento e o monitoramento de redes e a utilização de SNMP (*Simple Network Management*

Protocol), principal protocolo de gerenciamento de redes, tais como sua definição, seu modelo de funcionamento e sua estrutura.

No segundo capítulo, será apresentada a ferramenta de monitoramento de redes: o *Cacti*. Também será explanado sobre suas características de registros de dados e o funcionamento do RRDTool, sua capacidade de gerar gráficos, gerenciamento de contabilização, assim como os procedimentos de instalação da ferramenta.

Por fim, o último capítulo apresenta o ambiente de implementação e os testes que foram realizados durante a fase de implantação. Foi possível observar que através das ferramentas proporcionadas pelo *Cacti*, obtivemos resultados significantes e ficou clara a importância de uma ferramenta de gerência de redes.

1 GERENCIAMENTO DE REDES

A evolução dos ativos que interligam as redes e o aumento do número de usuários tem dificultado em muito a gerência, já que os profissionais necessitam se atualizar sobre os assuntos a cada versão lançada. Com a necessidade de melhorar o controle sobre os processos e recursos utilizados de seus clientes, é necessário saber a quantidade de memória utilizada pelos processos, se houveram falhas em equipamentos e entre outros tantos exemplos. Além disso, é importante para o administrador de rede verificar se ela está com um tráfego intenso de informações, ocasionando assim um congestionamento e uma demora nas respostas solicitadas pelos clientes.

O uso de ferramenta de gerenciamento de redes irá auxiliar aos administradores de rede a distribuir melhor o tráfego fazendo com que a rede tenha um melhor fluxo e, consequentemente, sua velocidade seja maior. De acordo com os gráficos que o software de gerenciamento fornece, é indicado ao administrador o tráfego de computadores na rede, isto facilita as identificações de falhas ocorridas nos clientes ou equipamentos.

1.1 Gerenciamento e Monitoramento de Redes

Em gerenciamento de redes está incluída a disponibilização, a integração e a coordenação de elementos de hardware, software e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar recursos da rede, e de elementos, para satisfazer às exigências operacionais, de desempenho e de qualidade de serviço em tempo real a um custo razoável (KUROSE; ROSS, 2006).

O gerenciamento está diretamente ligado ao controle das atividades e ao monitoramento dos recursos no ambiente a que se destina. Isso possibilita a otimização do uso dos recursos disponíveis e diminui o tempo de indisponibilidade do equipamento ou serviço de rede. A Gerência de redes é o controle de todos os equipamentos, seus respectivos recursos presentes em uma estrutura de rede, sendo eles passivos ou ativos (KUROSE; ROSS, 2006). Além do mais, é uma prática de extrema importância, pois através dela é possível identificar erros, falhas

e informações privilegiadas de uma rede. Um sistema de gerenciamento de redes é constituído por quatro segmentos básicos que são: o gerente, o agente, a base de informações gerenciadas e os protocolos.

Entretanto, monitoramento não é o único recurso existente quando se trata de gerenciamento, porém é o mais importante. A organização é outro importante fundamento que essa prática proporciona, já que o administrador em questão pode receber informações de forma instantânea em seu computador, além de poder prestar assistência técnica a qualquer usuário de maneira remota.

Existem quatro tipos de gerência de rede presentes no mercado, segundo Kurose & Ross (2006). A primeira é a centralizada, onde somente um gerente faz o monitoramento da rede, esse tipo de gerência é o que mais sobrecarrega o trabalho do gerente, já que todas as tarefas são gerenciadas por uma só pessoa. A segunda é a descentralizada, onde há uma divisão hierárquica que distribui o gerenciamento em setores ou nós, em que cada um é gerenciado por um gerente e na qual há um gerenciador principal ou administrador. A terceira é a reativa, processo na qual fundamenta em identificar a falha na rede, isolar, corrigir e documentar os erros ocorridos. E por último há a proativa, tipo de gerência na qual o administrador procura regularmente, informações que possam ser úteis para antecipar problemas nas redes. Também é necessário utilizar ferramentas para monitorar, gerenciar e relatar as atividades, procedimentos e outras informações essenciais para a regularidade dos serviços, pois os recursos a serem gerenciados alteram de acordo com a sua respectiva importância dentro da rede.

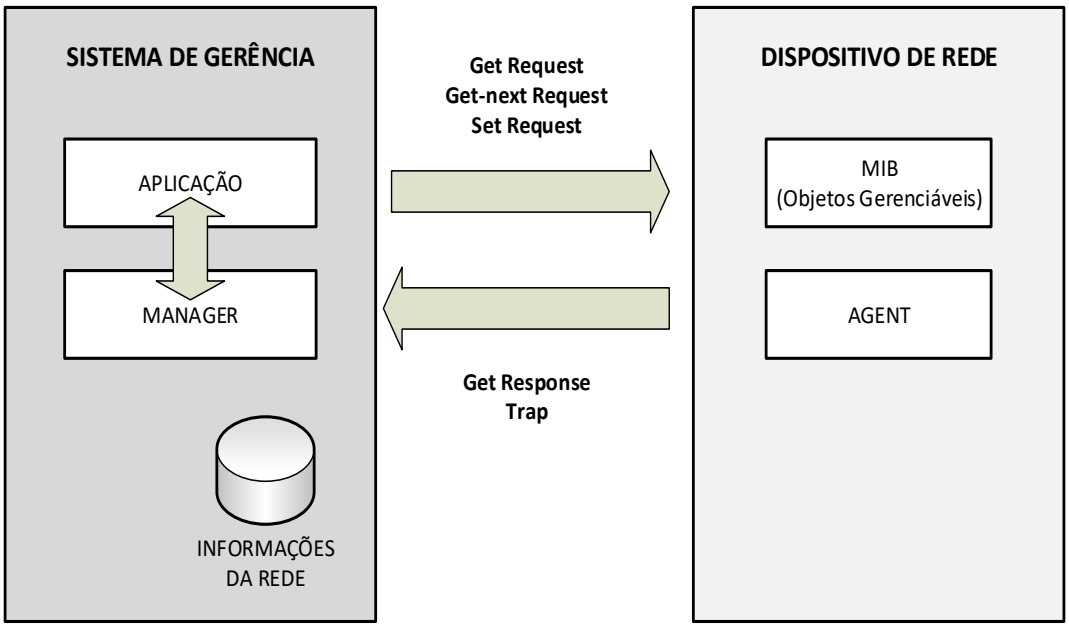
Segundo Kurose & Ross (2006), existem três etapas para se monitorar uma rede estruturada. A primeira etapa consiste em coletar dados, relatórios, gráficos, tabelas completas sobre cada usuário armazenado em arquivos *logs*. A segunda etapa fundamenta-se em diagnóstico, na qual é realizado o tratamento dos dados coletados e a identificação da causa dos problemas ou falhas detectadas. Já na terceira caracteriza-se a ação, no qual cabe uma ação ou controle sobre o recurso do problema já identificado.

1.2 SNMP

O Simple Network Management Protocol (STALLINGS, 1999) é um protocolo de gerência utilizado para obter informações de servidores SNMP – agentes espalhados em uma rede baseada na pilha de protocolos TCP/IP (KUROSE; ROSS, 2006). Os dados são obtidos através de requisições de um gerente a um ou mais agentes utilizando os serviços do protocolo de transporte UDP (KUROSE; ROSS, 2006) para enviar e receber suas mensagens através da rede.

O funcionamento do SNMP é baseado em dois elementos: o agente e o gerente. Conforme ilustrado na Figura 1, cada máquina gerenciada é vista como um conjunto de variáveis que representam informações referentes ao seu estado atual. Estas informações ficam disponíveis ao gerente através de consulta e algumas podem ser alteradas por ele, além disto, cada máquina gerenciada pelo SNMP deve possuir um agente e uma base de informações MIB. Management Information Base é um conjunto de informações organizadas hierarquicamente e que são acessadas através de protocolos de gerência de redes, onde o SNMP se encaixa. MIB's compreendem objetos gerenciados e são identificados por identificadores de objetos. Um objeto gerenciado é apenas um dos muitos dispositivos gerenciados.

Figura 1 – Funcionamento do protocolo SNMP.



Fonte – Elaborada pelo autor

Segundo Kurose & Ross (2006), MIB guarda objetos gerenciados, cujos valores, coletivamente, são gerenciados pela entidade gerenciadora através do envio de uma mensagem SNMP, sendo que o agente fica em um dispositivo que, por sinal, quem gerencia e a entidade gerenciadora. O objeto utiliza o OBJECT-TYPE do SMI que se agrupa em módulos MIB que utiliza MODULE-EDENTITY. Os objetos são nomeados hierarquicamente, através de um programa baseado na WEB, que percorre a rede identificando os objetos.

Basicamente, o SNMP pode apenas ler ou alterar o conteúdo de variáveis, que são instâncias de objetos gerenciados. Isso ocorre por meio de três operações genéricas:

- *Get* – Permite ao gerente consultar informações dos agentes. Essa conduta pode ser de dois tipos: *GetRequest*, no qual há a recuperação da primeira informação da lista de informações de um objeto; ou *GetNextRequest*, em que recupera a próxima informação disponível na lista a partir da última informação solicitada. Para cada *GetRequest* ou *GetNextRequest* enviado pelo gerente haverá uma resposta do agente, um *GetResponse*.
- *Set* – Operação de escrita. Permite ao gerente alterar valores dos objetos dos agentes; para cada *SetRequest* executado pelo gerente, o agente também responde com um *GetResponse*.
- *Trap* – Possibilita que um agente notifique um gerente sobre eventos significativos, sem que o gerente tenha solicitado previamente.

Durante vários anos o protocolo SNMP foi sendo modificado. No presente momento, têm-se três versões principais: a versão 1, a versão 2c e a versão 3, há uma quarta versão, mais popular e utilizada atualmente, que é a 2c. Esse protocolo consiste em três componentes principais: os dispositivos gerenciados, os agentes e os sistemas de gerenciamento de rede ou gerentes.

O SNMPv1 tem sua origem no protocolo Simple Gateway Monitoring Protocol que está definido na RFC 1028 (KUROSE; ROSS, 2006). O SGMP foi projetado para ser uma solução intermediária para o gerenciamento de redes, enquanto uma solução mais abrangente era explorada. No entanto muitos dos conceitos básicos do SNMP atual estão presentes no SGMP.

O SNMPv1 define cinco tipos de Protocol Data Unit, são eles: GetRequest, GetNextRequest, GetResponse, SetRequest e Trap.

- *GetRequest* – Permite ler o valor de uma ou mais instancias de variáveis.
- *GetNextRequest* – Permite ler o valor de uma ou mais instancias de variáveis sem conhecer o nome exato da mesma.
- *GetResponse* – Retorna o resultado de uma operação de leitura.
- *SetRequest* – Permite atribuir o valor de uma variável.
- *Trap* – Sinaliza a ocorrência de algum evento e possui um formato diferente.

Infelizmente, a segurança incorporada ao SNMPv1 é extremamente limitada e pode ser resumida em um conceito e uma tecnologia. É claro que a segurança simplória fornecida pelo SNMPv1 é suficiente, no entanto, para novos e grandes ambientes de rede, principalmente os que englobam redes públicas de operadoras, o SNMPv1 não fornece nível suficiente de segurança.

Após alguns anos de uso do SNMPv1, certas deficiências passaram a ser percebidas e as necessidades de melhoria foram identificadas. Isso levou ao desenvolvimento da versão original do SNMPv2, que tinha como objetivo aprimorar o SNMPv1 em várias áreas, incluindo as definições de objetos da MIB, operações do protocolo e segurança; esta última área, levou à proliferação de variantes do SNMPv2.

Visto que existem diferentes variações do SNMPv2, também existem variações nos formatos das mensagens utilizados para cada uma dessas variações. Isso é bastante confuso, mas seria muito pior caso as mensagens SNMP não possuíssem uma natureza modular. As operações do protocolo foram alteadas da versão SNMPv1 para o SNMPv2, e para isso foram necessárias alterações no formato do PDU, no entanto as operações do protocolo são as mesmas para todas as variações do SNMPv2.

As diferenças entre as variações do SNMPv2 estão nas áreas de implementação de segurança. Dessa forma, o resultado é que o formato do PDU é o

mesmo para todas as variantes do SNMPv2, mas o formato da mensagem difere de variação para variação.

Na versão 2 do SNMP foram introduzidas várias melhorias em relação à versão anterior. Entre elas, vale a pena destacar a possibilidade de comunicação entre entidades gerentes através das mensagens *InformRequest*, que tornou possível o gerenciamento distribuído. Outras mudanças são a inserção de uma PDU para otimizar e facilitar a recuperação de dados em tabelas, o *GetBulkRequest*, novos objetos MIBs para comunicação gerente-gerente e alterações nos nomes e formatos de operações existentes. São eles:

- *GetBulkRequest* – Permite a recuperação de grande quantidade de dados, normalmente o conteúdo de tabelas.
- InformRequest – Permite que um gerente envie informações para outro gerente.

Visto que a definição do SNMPv2c tem como objetivo manter as melhorias de funcionalidade do SNMPv2p, porém sem utilizar o mecanismo de segurança especificado para o mesmo, os mecanismos de segurança disponíveis para o SNMPv2c são exatamente os mesmos do SNMPv1.

O SNMPv3 foi criado para suprir uma necessidade padronização que se fez necessária com as várias variações do SNMPv2 que tentavam criar soluções de segurança para o protocolo. O SNMPv3 teve como base as definições das variações SNMPv2c e SNMPv2 (KUROSE; ROSS, 2006).

Além das definições das questões de segurança, o projeto do SNMPv3 também objetivou uma padronização de implementação das entidades (agente/gerente), modularizando suas funcionalidades, o que facilita a evolução de alguns mecanismos do protocolo sem exigir que novas versões sejam lançadas. Outros objetivos eram a manutenção de uma estrutura simples, facilitar a integração com outras versões e, sempre que possível, reaproveitar as especificações existentes.

O SNMPv3 incorporou o Structure of Management Information e o MIB do SNMPv2, assim como também utilizou as mesmas operações do SNMPv2, apenas com uma reescrita da norma para uma compatibilização da nomenclatura. A arquitetura proposta na RFC 2271 consiste em uma coleção distribuída de entidades

SNMP que interagem entre si. Cada entidade implementa uma porção das capacidades do SNMP e pode atuar como agente, gerente ou uma combinação dos dois. Cada entidade SNMP consiste em uma coleção de módulos que interagem entre si para prover serviços.

Com base nas informações apresentadas pode-se verificar que o SNMPv3 possui várias características que o torna muito mais seguro que suas versões anteriores, no entanto esse benefício de segurança vem acompanhado de uma maior complexidade para configurar todas as funcionalidades de segurança necessárias.

Dessa forma, para ambientes em que haja necessidade de uma implementação rápida e que segurança não seja uma questão crítica, é justificado o uso do SNMPv1, ou preferencialmente, do SNMPv2c.

No entanto, para ambientes em que a segurança é uma questão crucial, se faz necessário a utilização do SNMPv3, para que nem os dispositivos gerenciados nem as informações gerenciais sejam comprometidas.

1.2.1 O Agente

É um processo executado na máquina gerenciada, responsável pela manutenção das informações de gerência da máquina. As funções principais de um agente são:

- Atender as requisições enviadas pelo gerente;
- Enviar automaticamente informações de gerenciamento ao gerente, quando previamente programado;

Um agente SNMP tradicional pode conter três tipos de aplicação:

- Aplicação que Responde Comandos, que provê acesso aos dados gerenciados. Estas aplicações respondem às requisições que chegam recuperando ou alterando objetos gerenciados e então gerando um PDU Response.

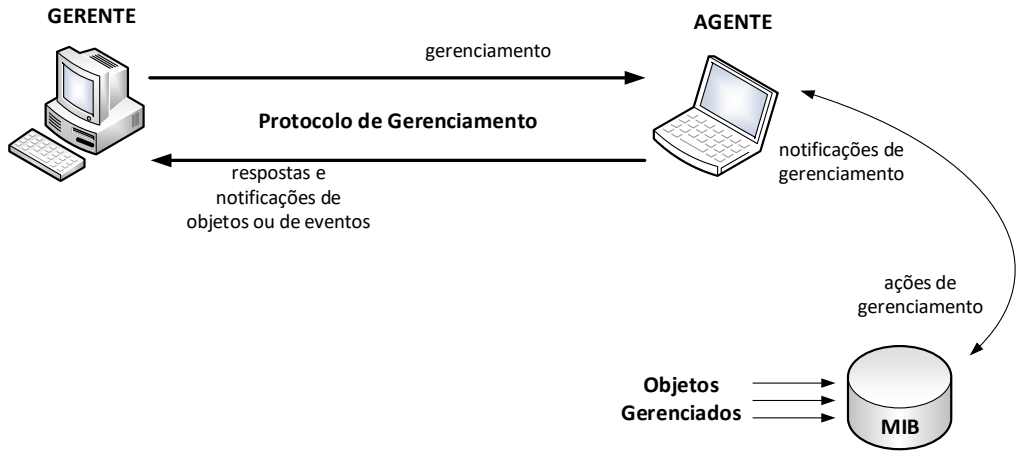
- Uma Aplicação Emissora de Notificações, que inicia mensagens assíncronas; no caso de um agente tradicional, o PDU Trapv2 ou Trap são usados por essa aplicação.
- Uma Aplicação Encaminhadora Proxy, que encaminha mensagens entre entidades.

O *engine* SNMP de um agente tradicional contém todos os componentes encontrados em um *engine* SNMP de um gerente tradicional, mais um Subsistema de Controle de Acesso. Esse subsistema provém serviços de autorização para controlar o acesso às MIBs quanto à leitura e gravação em objetos gerenciados. Esses serviços são executados com base no conteúdo dos PDUs. Uma implementação do Subsistema de Segurança pode suportar um ou mais modelos de controle de acesso distintos.

1.2.2 O Gerente

É um programa executado em uma estação servidora que permite a obtenção e o envio de informações de gerenciamento junto aos dispositivos gerenciados mediante a comunicação com um ou mais agentes.

Figura 2 – Relacionamento de um gerente com o objeto gerenciado.



Fonte – Elaborada pelo autor

O gerente fica responsável pelo monitoramento, relatórios e decisões na ocorrência de problemas enquanto que o agente fica responsável pelas funções de envio e alteração das informações e também pela notificação da ocorrência de eventos específicos ao gerente.

1.2.3 Operações e Mensagens do Protocolo SNMP

Existem duas operações básicas (*SET* e *GET*) e suas derivações (*GET-NEXT*, *TRAP*).

- A operação *SET* é utilizada para alterar o valor da variável; o gerente solicita que o agente faça uma alteração no valor da variável;
- A operação *GET* é utilizada para ler o valor da variável; o gerente solicita que o agente obtenha o valor da variável;
- A operação de *GET-NEXT* é utilizada para ler o valor da próxima variável; o gerente fornece o nome de uma variável e o cliente obtém o valor e o nome da próxima variável; também é utilizado para obter valores e nomes de variáveis de uma tabela de tamanho desconhecido;
- A operação *TRAP* é utilizada para comunicar um evento; o agente comunica ao gerente o acontecimento de um evento, previamente determinado. São sete tipos básicos de trap determinados:
  - ✓ *coldStart*: a entidade que a envia foi reinicializada, indicando que a configuração do agente ou a implementação pode ter sido alterada;
  - ✓ *warmStart*: a entidade que a envia foi reinicializada, porém a configuração do agente e a implementação não foram alteradas;
  - ✓ *linkDown*: o enlace de comunicação foi interrompido;
  - ✓ *linkUp*: o enlace de comunicação foi estabelecido;
  - ✓ *authenticationFailure*: o agente recebeu uma mensagem SNMP do gerente que não foi autenticada;
  - ✓ *egpNeighborLoss*: um par EGP parou;

- ✓ *enterpriseSpecific*: indica a ocorrência de uma operação TRAP não básica.

O formato geral das mensagens no SNMPv3 ainda segue a mesma ideia de uma mensagem “envelope” que contém um cabeçalho e um PDU encapsulado, no entanto, na versão 3 esse conceito está ainda mais refinado. Os campos do cabeçalho foram divididos em dois tipos: os que lidam e os que não lidam com questões de segurança. Os campos não voltados para segurança são comuns para todas as implementações do SNMPv3, enquanto o uso dos campos ligados a segurança podem ser guiados por cada modelo de segurança do SNMPv3, e processados pelos módulos correspondentes em uma entidade SNMP que lide com segurança. Esta solução provê uma considerável flexibilidade evitando os problemas que atormentaram o SNMPv2.

1.3 Ferramentas de Monitoramento

As ferramentas de gerenciamento são o braço direito do administrador de rede. Seja um simples comando ou um sistema especializado, elas auxiliam no diagnóstico de erros, resolução de problemas, detecção de gargalos, ou seja, permitem que o administrador visualize a rede e seus componentes, controlando-os ou interagindo com eles quando necessário.

Algumas ferramentas mais simples já vêm embutidas no sistema operacional e outras estão disponíveis na forma de aplicações que analisam protocolos, monitoram dispositivos, sistemas e serviços e oferecem recursos que facilitam procedimentos de configuração. Existem ainda plataformas de gerenciamento, que muitas vezes são sistemas distribuídos, compostos de hardware e software específico para realizar as atividades de gerenciamento. Esses sistemas manipulam e organizam dados e os apresentam na forma de gráficos, tabelas ou relatórios.

No caso do gerenciamento de contabilização, existem ferramentas que registram dados dos recursos monitorados e geram gráficos de apresentação, além de oferecerem outros recursos valiosos. Podemos citar o CACTI o que justifica a escolha da ferramenta para a proposta apresentada.

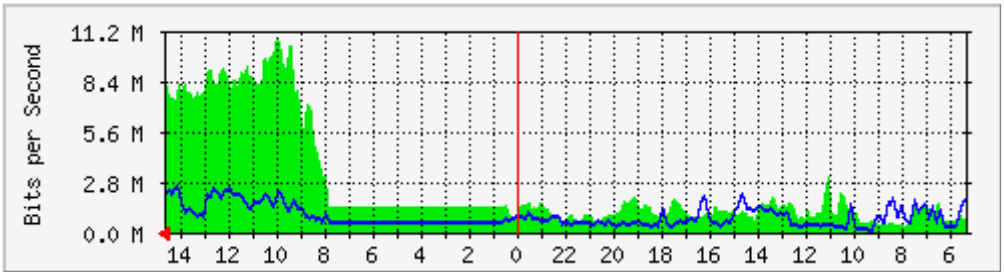
1.3.1 MRTG

O MRTG (OETIKER, 2011) é uma ferramenta de monitoração que gera páginas HTML com gráficos de dados coletados a partir de SNMP ou scripts externos. É conhecido principalmente pelo seu uso na monitoração de tráfego de rede, mas pode monitorar dispositivos conectados à rede desde que o host forneça os dados via SNMP ou script.

Criado nas linguagens de programações C (criado por Dennis Ritchie) e Perl (Criado por Larry Wall), utiliza o SNMP para acessar as variáveis de tráfego nos dispositivos gerenciados e com o objetivo de construir gráficos que representam as variáveis de tráfego do dispositivo gerenciado, podendo ser configurado em quatro tipos: diário, semanal, mensal e anual.

O gráfico diário é traçado a cada 5 minutos e possui abscissa com aproximadamente 33 horas. Pode-se observar no exemplo:

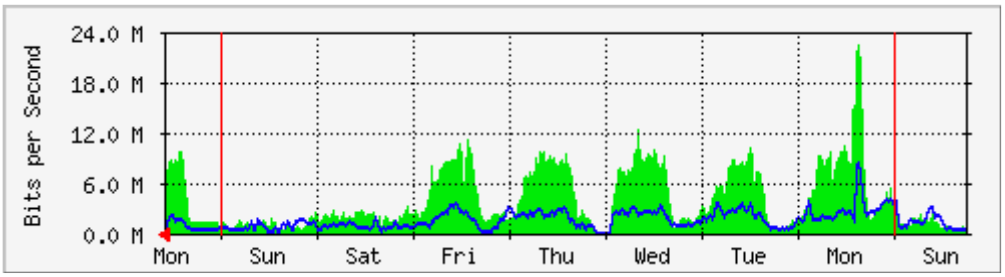
Figura 3 – Gráfico apresentando informações em horas.



Fonte – MRTG (OETIKER, 2011).

O gráfico semanal é traçado a cada 30 minutos e possui abscissa com aproximadamente oito dias. Exemplo:

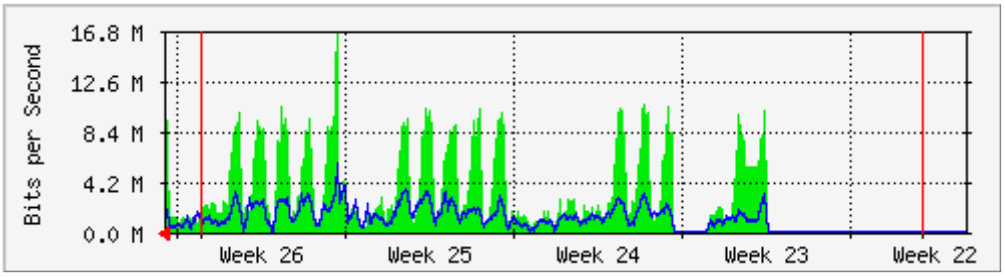
Figura 4 – Gráfico apresentando informações em dias.



Fonte – MRTG (OETIKER, 2011).

O gráfico mensal é traçado a cada 2 horas e possui abscissa com aproximadamente cinco semanas. Exemplo:

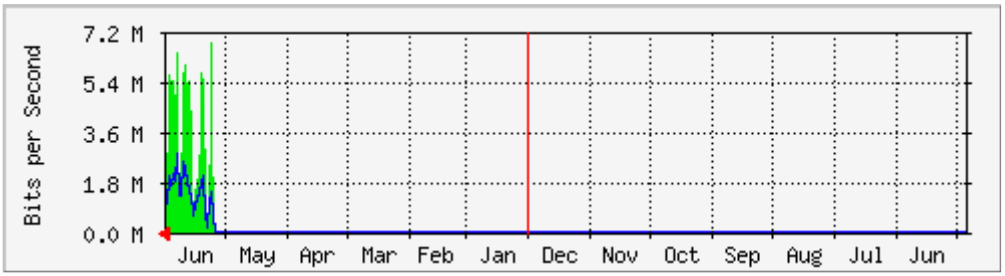
Figura 5 – Gráfico apresentando informações em semanas.



Fonte – MRTG (OETIKER, 2011).

O gráfico anual é traçado a cada um dia e possui abscissa com aproximadamente um ano. Exemplo:

Figura 6 – Gráfico apresentando informações em meses.



Fonte – MRTG (OETIKER, 2011).

1.4.2 Nagios

O *Nagios* é uma aplicação desenvolvida para monitoramento de rede. Ele pode monitorar *host* e serviços, enviando notificações de eventos. Ele foi originalmente desenvolvido para Linux, embora funcione também com Linux e com Windows.

Algumas de suas principais características são:

- Monitoramento de serviços de rede;
- Monitoramento de recursos de *hosts*: carga do processador, utilização de espaço em disco, utilização de CPU, entre outros;
- Notificações quando problemas com serviços ou *hosts ocorrem e são resolvidos;*
- Geração automática de arquivo de *log*;
- Interface gráfica para visualização do estado atual da rede, histórico de problemas e notificações.

É importante ressaltar que além da área de contabilização, o *Nagios* atua no gerenciamento de falhas, verificando periodicamente o estado dos recursos monitorados e enviando alertas caso ocorra alguma falha. O *Nagios* também é capaz de notificar o administrador caso os valores de utilização de um determinado dispositivo ultrapasse os limites máximos previamente definidos na sua configuração.

1.4.3 NTOP

O NTOP[1] (criado por University of Pisa) é um programa de código aberto desenvolvido para monitoramento de tráfego de rede em tempo real. Trabalha diretamente com a placa de rede analisando todos os pacotes transitados. Sua visualização é organizada em resultados formatados por uma página *HTML*. Este proverá o monitoramento ativo das conexões por interface do equipamento.

O NTOP possui métodos capazes de detectar pacotes que estão sendo transmitidos na rede e segmentá-los de acordo com características que possam ser analisadas visando a identificação de certos comportamentos que possam estar sobrecarregando a rede de um modo inverso às políticas de gerenciamento da mesma. Abaixo algumas características e funcionalidades:

- Analisa os pacotes que trafegam na rede;
- Lista e ordena o tráfego de rede de acordo com vários protocolos;
- Exibe estatísticas de tráfego;
- Identifica passivamente várias informações obre os hosts da rede, incluindo o sistema operacional executado e endereço de e-mail do usuário da estação;
- Exibe a distribuição do tráfego *IP* entre vários protocolos da camada de aplicação;
- Decodifica vários protocolos da camada de aplicação;
- Atua como coletor de fluxos gerados por roteadores e switches;
- Possui um *WebServer* integrado que permite consultas às informações através de um browser.

1.4.4 CACTI

O CACTI (CACTI, 2011) é uma ferramenta de monitoramento de rede, porém com enfoque principal em gerenciamento de contabilização. Escrito em *PHP*, o CACTI atua em conjunto com o RRDTool (OETIKER, 2011), um sistema capaz de reproduzir em gráficos as informações dos elementos monitorados. Exemplos de tipos de informações que podem ser monitoradas são: largura de banda, e-mails enviados e recebidos, requisições *HTTP*, média de processos, utilização de memória, entre muito outras.

Com o CACTI é possível gerar gráficos referentes ao uso de memória física, memória virtual, quantidade de processos, processamento, tráfego de rede, quantidade de espaço em disco, entre outros. Através do SNMP, é permitido ter acesso a gráficos, não só de sistemas operacionais Linux, mas também de Windows e de dispositivos de rede com switches e roteadores, bem como qualquer dispositivo que suporte o SNMP.

A escolha do CACTI para a realização do trabalho apresentado, é por ser uma solução completa de geração de gráficos sobre redes de computadores, desenhado

à máxima utilização dos dados armazenados via RRDTool, gerando gráficos funcionais. Além de prover um agente rápido, com modelos de gráficos avançados, múltiplos métodos de aquisição de dados e opções de gerenciamento. Tudo isso é provido em uma interface intuitiva, de fácil utilização e fácil adaptação, além do mais o CACTI permite que os gráficos gerados sejam organizados de diversos modos.

2 CARACTERÍSTICAS E INSTALAÇÃO DO CACTI

Este capítulo apresenta a ferramenta de monitoramento de redes, o Cacti. Para isso o *Cacti* (CACTI, 2011) atua em conjunto com o RRDTool (CACTI, 2011) um sistema capaz de produzir em gráficos as informações dos elementos monitorados.

O *Cacti* é um sistema completo web para monitoramento gráfico utilizando ferramentas RRD – *Round Robin Database* (OETIKER, 2011) para armazenamento e exibição de dados e coleta via SNMP (STALLINGS, 1999). Possui uma série de *plugins* que permitem agregação de serviços ao sistema principal. O desempenho de equipamentos e serviços de rede, bem como sua visualização do uso em tempo real. Também proverá um sistema de alerta para problemas e sobrecargas nos dispositivos monitorados.

Os gráficos são gerados em função de intervalos de tempo, produzindo assim um histórico de monitoramento. Vários modelos de hosts de gráficos e de tipos de dados estão disponíveis. As informações coletadas são armazenadas numa base de dados e podem ser consultadas através da interface Web do *Cacti*. Os gráficos criados podem ainda ser organizados em árvores, podendo ser separados por tipos.

Para que o *Cacti* possa operar, é necessário que o SNMP esteja instalado no servidor de monitoramento e também nos equipamentos que serão monitorados. E, uma vez que o *Cacti* trabalha diretamente com SNMP, qualquer informação que este possa recuperar pode também ser reproduzida na interface gráfica do *Cacti*. Além disso, é possível criar *scripts* e configurar o intervalo de tempo de obtenção dos dados, além dos tradicionais: dia, semana, mês e ano.

2.1 Características do Cacti

O *Cacti* é um front-end para a ferramenta RRDTool (*Round Robin Database Tool*) que coleta e organiza os dados (OETIKER, 2011). Ela permite a captura de dados de diversos dispositivos de rede, sem gerar um volume excessivo de dados armazenados, pois utiliza uma técnica que permite o armazenamento dos dados de

forma otimizada. Isso é possível porque a RRDTool adota métricas baseadas na média dos dados e não pelo seu total. Por exemplo, para os dados mais antigos ela somente armazena a média dos valores, assim consegue ter um histórico considerável de dados, sem que isso acarrete um número exagerado de informação, fato esse que pode vir a demandar muito espaço de armazenagem como também tornar lenta a ferramenta que irá utilizar estes dados (OETIKER, 2011). Este é o principal motivo que permite ao *Cacti* monitorar muitos dispositivos de rede, com pouco impacto em seu desempenho. Para armazenar estes dados o *Cacti* utiliza o banco de dados MySQL, uma ferramenta atual que já se mostrou confiável para cumprir as necessidades do sistema.

Quanto à interface WEB, utiliza-se o padrão PHP (criado por Rasmus Lerdorf em 1995), o que permite um grau elevado de compatibilidade com os principais navegadores do mercado, como também um desempenho adequado para os padrões do sistema.

O grande diferencial do *Cacti* é exatamente a possibilidade de gerar diversos tipos de gráficos com base nos dados coletados e, principalmente, de forma customizada. Como exemplo, é possível gerar gráficos de largura de banda, temperatura, capacidade de discos e uso de CPU, possibilitando ao usuário uma visão geral dos dispositivos e serviços gerenciados (CACTI, 2009).

De forma simplificada, o funcionamento do *Cacti* se realiza por meio da coleta de dados dos dispositivos cadastrados. Esta operação, denominada *polling*, se utiliza principalmente do protocolo SNMP, para receber dos equipamentos e serviços as principais informações que serão armazenadas no banco de dados MySQL. Este armazenamento ocorre com a ferramenta RRDTool. Com o uso desta técnica, há um aumento mínimo na base de dados, levando-se em consideração a grande ocorrência de *pollings*, que dependendo da quantidade de dispositivos monitorados, pode ocorrer com frequência inferior a um minuto, isto permite a coleta de dados de uma elevada quantidade de dispositivos de rede.

Em seguida, a interface WEB utiliza desta base de dados para gerar gráficos, que por sua vez são configurados de acordo com as necessidades de cada administrador ou operador, oferecendo possibilidades diversas no monitoramento das redes.

O *Cacti* possui uma arquitetura aberta, por isso permite a adição de *plugins* que possibilitam incrementar ainda mais seu uso e, consequentemente, seus resultados. Segue uma breve descrição dos principais plug-ins disponíveis atualmente (CONNER, 2011):

- *Discovery* – Com este plug-in é possível realizar um *scanner* na rede para encontrar hosts não monitorados pelo Cacti que estejam com o SNMP habilitado;
- *Hostinfo* – Mostra informações sobre o Cacti, *plugins*, RRDTool, SNMP e outras aplicações instaladas no máquina;
- *Monitor* – Mostra a situação dos hosts em tempo real, com alerta visual e sonoro caso algum host esteja fora do ar;
- *Ntop* – Realiza uma integração da ferramenta Ntop ao Cacti. Ntop é uma ferramenta que provê estatísticas sobre a rede usada;
- *Realtime* – Adiciona ao Cacti a possibilidade de visualizar os gráficos monitorados em tempo real;
- *Routerconfigs* – Este *plugin* utiliza o TFTP (KUROSE; ROSS, 2006) para realizar backup de configurações de switches e roteadores, e armazena de forma organizada o histórico das configurações alteradas;
- *Settings* – Adiciona a possibilidade de envio de e-mail à arquitetura de plugins;
- *Spine* – Aumenta a performance da coleta de dados SNMP;
- *Syslog* – Armazena informações do Syslog, e é possível criar alertas para determinadas situações;
- *Thold* – Com este *plugin* é possível criar qualquer tipo de alerta com base nos gráficos, e combinado com *settings* é possível enviar e-mails para o administrador;
- *Tools* – Adiciona uma interface para realizar testes de SNMP e checar alguns serviços no equipamento indicado;

- *Weathermap* – Com este plug-in é possível criar mapas da rede que facilitam a visualização e organização dos hosts, além de, possibilitar uma visão geral do estado atual da rede.

2.2 RRDTool

RRDTool (OETIKER, 2011) é um registro de dados de alta performance em um sistema gráfico, projetado para lidar com dados de séries temporais como largura de banda da rede, temperatura ambiente, carga da CPU, carga do servidor e monitorar dispositivos como roteadores, entre outros. Também é conhecido como algoritmo de agendamento de processos em ferramentas de banco de dados, um padrão da indústria, solução de código aberto. Ele permite que o administrador registre e analise dados coletados de todos os tipos de fontes de dados (DS), que são capazes de responder a consultas SNMP. A parte de análise de dados do RRDTool é baseada na capacidade de gerar representações gráficas dos valores de dados coletados durante um período de tempo definível.

RRDTool, também conhecido por sua famosa criação MRTG. RRDTool é escrito em linguagem de programação C e armazena seus dados em arquivos *.rdd*. O número de registros em um único arquivo *.rdd* nunca aumenta, o que significa que os registros antigos são frequentemente removidos e apresenta gráficos úteis processando os dados para impor uma determinada densidade de dados. RRDTool oferece várias opções de linha de comando para acessar e manipular arquivo *.rdd*:

- *Create* – Configurar um novo RRD.
- *Update* – Armazenar novos valores de dados em RRD.
- *Updatev* – Operacionalmente equivalente a atualizar, exceto para sáida.
- *Graph* – Crie gráficos a partir de dados armazenados em um ou vários RRDs. Além de gerar gráficos, os dados também podem ser extraídos.
- *Dump* – Em conexão com a restauração você pode usar isso para mover um RRD de uma arquitetura de computador para outro.
- *Restore* – Restaurar um RRD em formato XML para um RRD binário.

- *Fetch* - Obter dados para um determinado período de tempo de um RRD. A função de gráfico usa *fetch* para recuperar seus dados de um RRD.
- *Tune* - Alterar configuração e estrutura de um RRD.
- *Last* - Encontre a última atualização de um RRD.
- *Info* - Obter informações sobre um RRD.
- *Resize* - Alterar o tamanho dos RRAs individuais. Isso é perigoso!
- *Xport* - Exportar dados recuperados de um ou vários RRDs.

Há também um número de ligações de idioma para RRDTool, que permitem aos administradores ou programadores usá-lo diretamente a partir de linguagens de programação. Assim, ele pode ser usado para escrever arquivos de configurações de monitoramento personalizado ou criar aplicativos inteiros usando suas ligações de idioma.

2.2.1 Funcionamento do RRDTool

RRDTool segue um design lógico para adquirir e processar dados coletados de fontes de dados (DS). A seguir, uma breve discussão sobre as diferentes etapas do processo lógico:

- ***Data Acquisition***: Ao monitorar um dispositivo ou sistema, é necessário receber dados em um intervalo de tempo constante. Manualmente, não é possível manter essa atividade como um administrador do sistema. Em tais situações, o RRDTool é útil. Ele armazena os dados em um banco de dados *round-robin*, que é recebido em um intervalo de tempo constante definido pelo administrador do sistema, usando o aplicativo poller definido como agendador de tarefas no sistema operacional.
- ***Data Consolidation***: O administrador do sistema pode registrar os dados de intervalo de cinco minutos, mas ele poderia estar interessado em saber a atualização acumulada durante o último mês. Neste caso, simplesmente armazenar os dados em um intervalo de cinco minutos

para todo o mês irá resolver o problema. Mas isso exigirá enorme espaço em disco e uma quantidade considerável de tempo para analisar os dados, como em um ambiente de rede, os administradores não estão monitorando apenas um único dispositivo. RRDTool resolve esse problema com o recurso de consolidação de dados. Ao criar um banco de dados round-robin, o administrador pode definir em que intervalo a consolidação de dados deve ocorrer usando funções de consolidação (CF) como MÁXIMO, MÉDIA, MÍNIMO e outros.

- ***Round Robin Archives of Consolidated Data***: Os valores de dados da configuração de consolidação são armazenados em *round-robin archives* (RRA). Desta forma, o RRDTool armazena dados da forma mais eficiente durante um determinado período de tempo definido pelo administrador do sistema. Esse processo mantém o arquivo de banco de dados em um tamanho constante para processamento e análise mais rápido.
- ***Unknown Data***: RRDTool armazena dados em um intervalo constante em um banco de dados round-robin. Às vezes, esses dados podem não estar disponíveis para armazenar em RRD devido a falha do dispositivo ou outras causas. Nesse caso, o RRDTool armazena o arquivo RRD com valor de dados * UNKNOWN *. Este valor * UNKNOWN * é suportado por todas as funções RRDTool.
- ***Graphing***: O RRDtool permite que o administrador do sistema gere relatórios em formulários gráficos e numéricos com base nos dados armazenados no banco de dados *round-robin* (RDD) usando suas funções incorporadas de processamento de gráfico. A personalização desses gráficos é possível com base na cor, tamanho e conteúdo.

2.3 Instalando o Cacti

O *Cacti* tem alguns pré-requisitos. É necessário instalar esses pacotes antes de iniciar a instalação do *Cacti*:

- RRDTool1.0.49 ou superior;

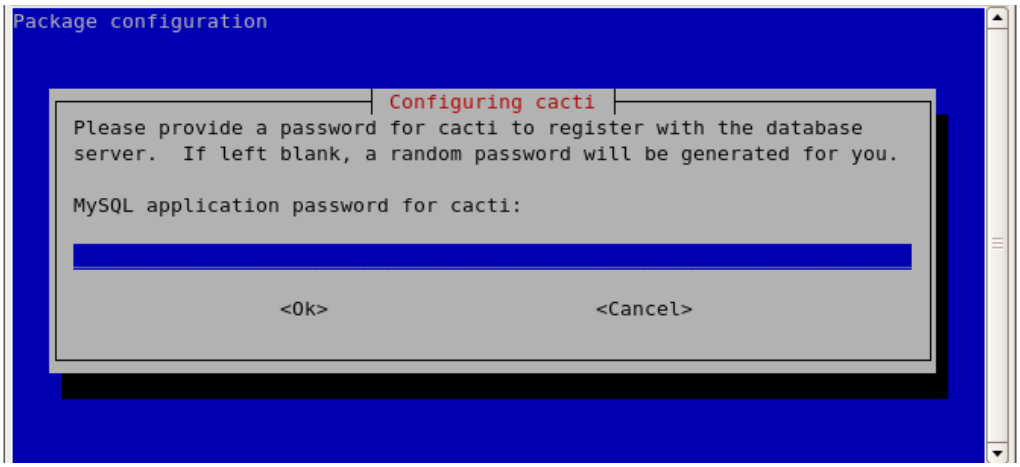
- NET-SNMP;
- MySQL4.1.x ou superior;
- PHP 4.3.6 ou superior;
- Apache / IIS ou qualquer outro servidor web.

Para a instalação do *Cacti* em uma máquina Linux, basta aplicar o comando abaixo:

- *$ apt-get install cacti*

Este comando iniciará a instalação do *Cacti*. Um assistente será iniciado, e pedir-lhe algumas informações importantes. Aqui, você deve digitar a senha-mysqlserver do MySQL, ou qualquer que você tenha definido antes - para que ele possa criar um usuário *Cacti* e o banco de dados no servidor MySQL. Ele não pedirá novamente para a confirmação de senha, então você precisa de pouco cuidado aqui:

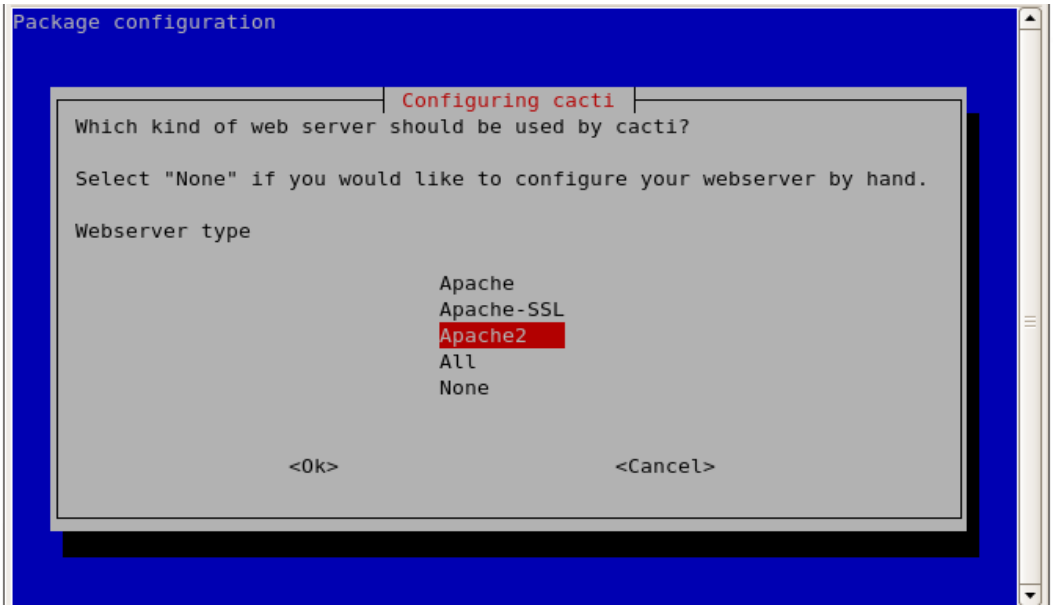
Figura 8 – Configurando senha no MySQL



Fonte – CACTI (KUNDU; LAVLU, 2009)

Como utiliza-se o Apache 2 como nosso servidor web, você terá que escolher Apache2 neste menu:

Figura 9 – Selecionando o servidor Apache2.

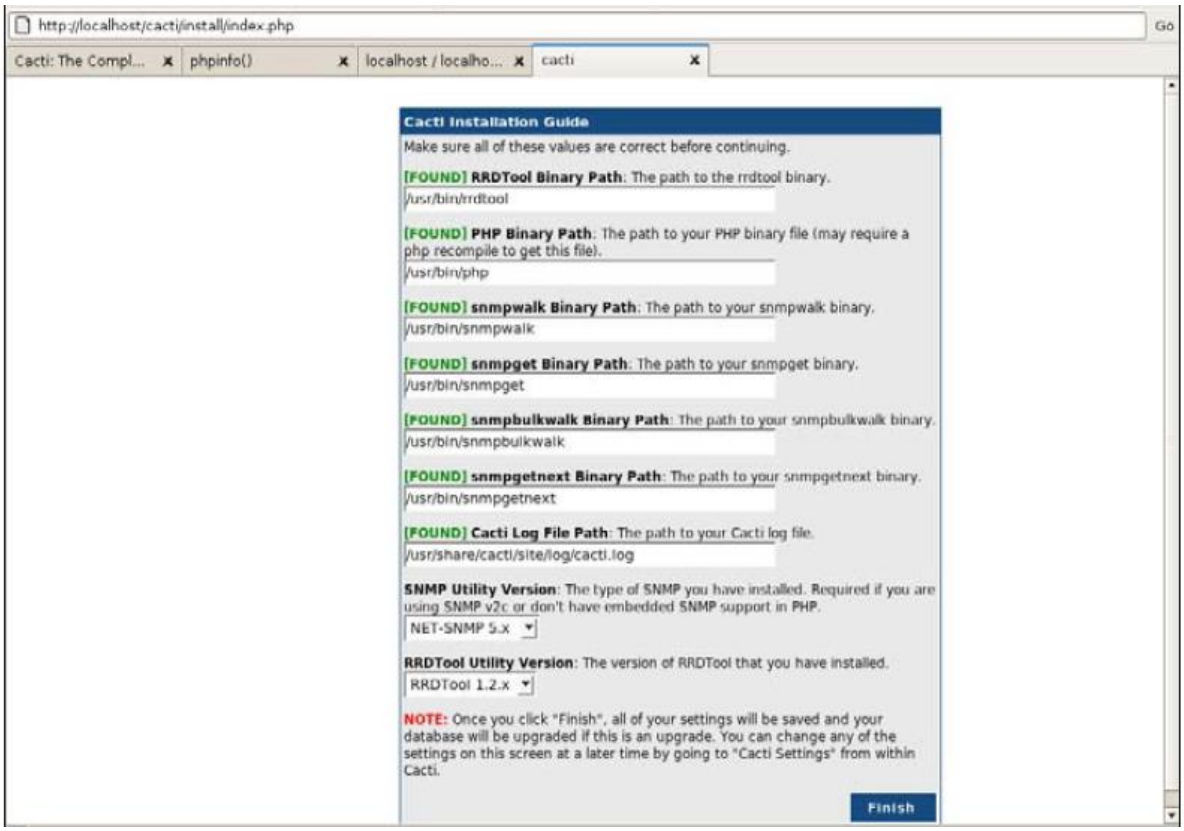


Fonte – CACTI (KUNDU; LAVLU, 2009)

Depois disso, o ambiente estará pronto para configurar o *Cacti*, pois todos os arquivos necessários para o *Cacti* agora estão instalados em seu sistema.

Para concluir o processo de configuração, abra http://localhost/cactus no seu navegador favorito. A página de configurações de caminho determina automaticamente os caminhos instalados para RRDTool, PHP, SNMP eCacti.log, bem como as versões para Net-SNMP e RRDTool. Se algum destes estiver em falta, ou pretender utilizar uma versão diferente, ajuste-os nesta página e, em seguida, clique em Finish, como mostra a figura a seguir:

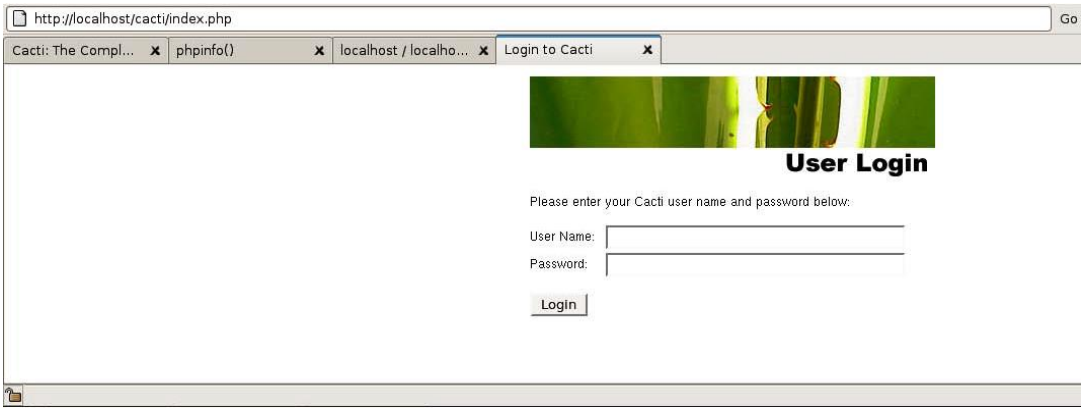
Figura 10 – Instalando via Browser.



Fonte – CACTI (KUNDU; LAVLU, 2009)

Esta é a tela de login do *Cacti*. O nome de usuário é “admin” e a senha padrão é “admin”:

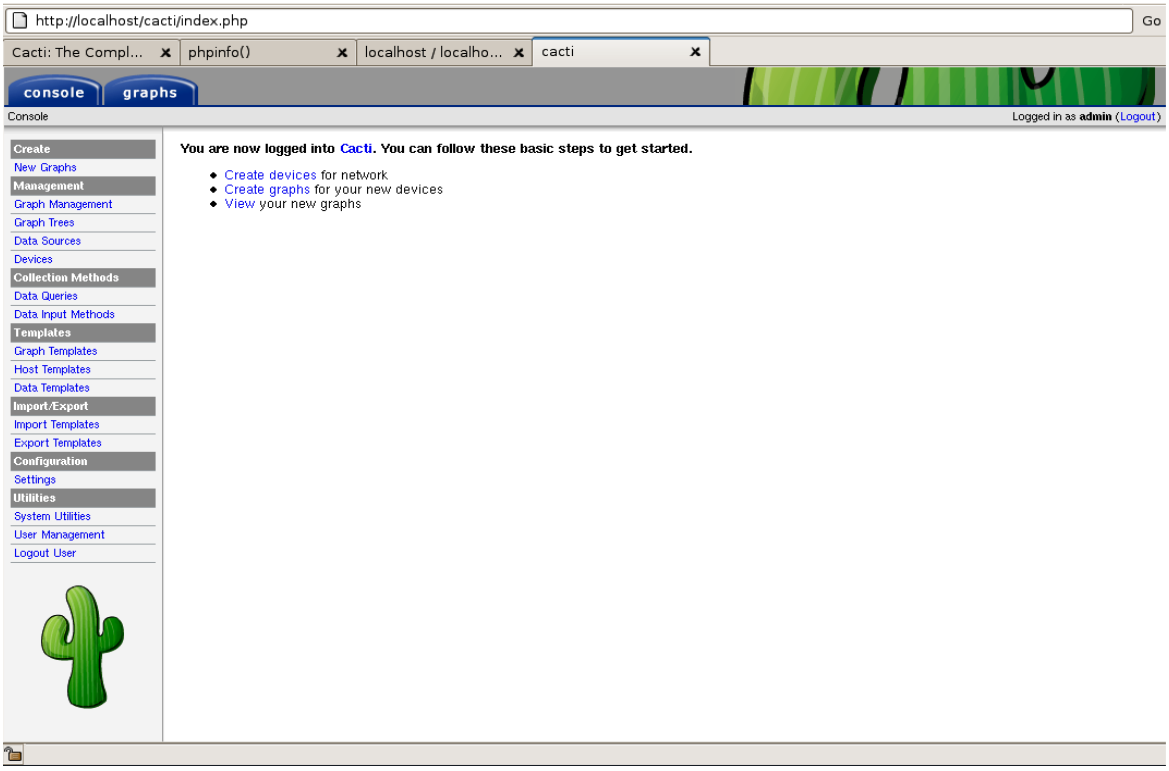
Figura 11 – Página de Login.



Fonte – CACTI (KUNDU; LAVLU, 2009)

Após um login bem-sucedido pela primeira vez, o sistema solicitará que você defina uma nova senha. Digite uma nova senha e certifique-se de que irá lembrá-la. Sem esta senha, você não pode administrar o sistema.

Figura 12 – Página do Cacti.



Fonte – CACTI (KUNDU; LAVLU, 2009)

2.4 Gerenciamento de Redes e Dispositivos com Gráficos

Agora percebe-se um ambiente *Cacti* em funcionamento, será visto adicionar dispositivos conectados à rede no sistema *Cacti* e produzir gráficos para monitorar redes pequenas e instalações de diversos tamanhos em redes complexas com centenas de dispositivos. É bastante fácil de gerenciar dispositivos através da página web do *Cacti*. Ela fornece um poller rápido, um modelo de gráfico avançado e vários métodos de aquisição de dados fora da caixa, envolvidos em uma interface fácil de usar que faz sentido para o administrador de rede.

Caso esteja familiarizado com RRDTool, então saberá, *Cacti* é projetado para aproveitar o poder de armazenamento de dados RRDTool e funcionalidade de gráficos. Se não estiver, não há preocupação - o *Cacti* criará gráficos sem a entrada de configuração extensiva dos usuários. Modelos de gráfico incorporados facilitarão a sua vida, por isso não é necessário compreender a funcionalidade de cada campo para criar gráficos para dispositivos conectados à rede. Cada gráfico armazena diferentes conjuntos de parâmetros que controlam diferentes aspectos de cada gráfico.

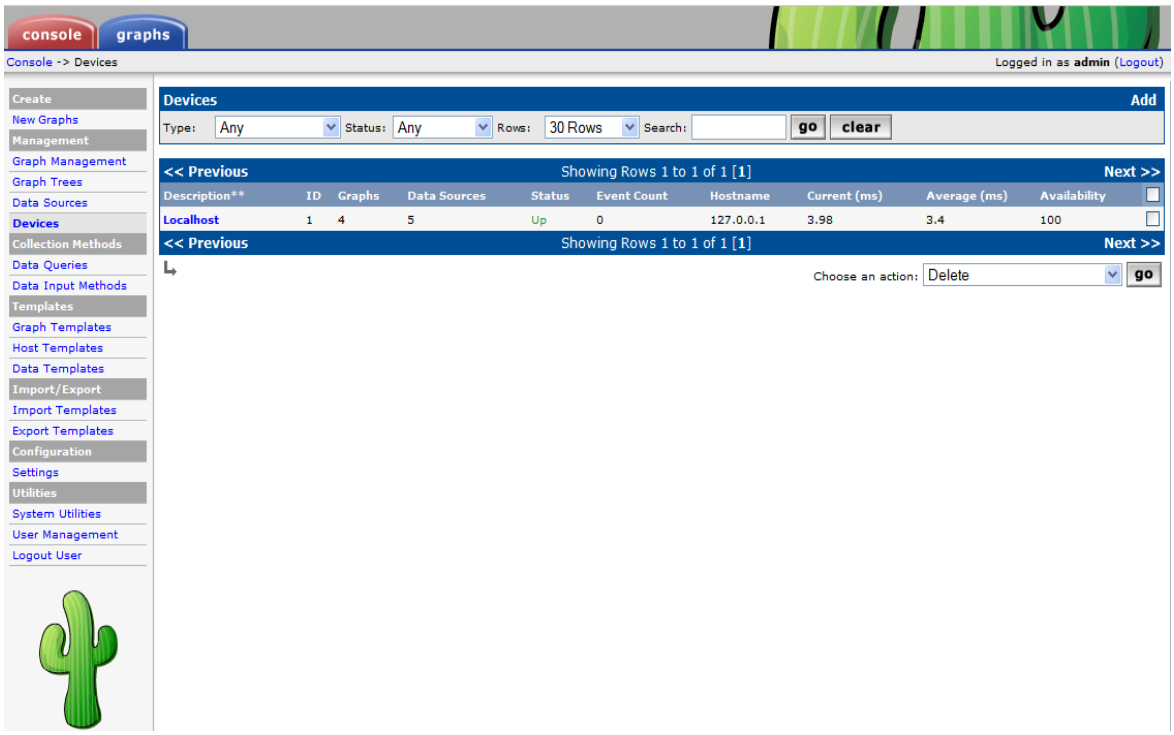
2.4.1 Criando Gráficos

No momento da criação de gráficos, haverá de enfrentar um pouco de uma curva de aprendizado rígida. Mantenha-se no curso, em breve será possível criar gráficos para diferentes dispositivos muito rapidamente. Como abordado nos capítulos anteriores, *Cacti* pode criar gráficos para qualquer SNMP-enabled, network-attached dispositivos. Isso pode ser um switch, roteador, servidor, computador de mesa, impressora, IPS, UPS e assim por diante. Inicialmente, não será apresentado sobre o modelo personalizado e o desenvolvimento do script de consulta de dados para nenhum dispositivo habilitado para SNMP. Em vez disso, serão utilizadas as opções padrão em *Cacti*. Para construir um modelo personalizado, precisamos entender o protocolo SNMP e as ferramentas de linha de comando do conjunto de aplicativos Net-SNMP. No Capítulo 6, será discutido o protocolo SNMP e o conjunto de aplicativos Net-SNMP em detalhes. Primeiramente serão criados gráficos com base nos modelos e dispositivos disponíveis.

2.4.2 Adicionando Dispositivos

Antes de adicionar um gráfico, precisa-se adicionar um dispositivo para o qual você deseja criar o gráfico. Para isso, clique em Dispositivos sob Gestão. *Cacti* abrirá o painel de exibição "*Dispositivos"*. Isso aparecerá assim:

Figura 13 – Adicionar Dispositivos.



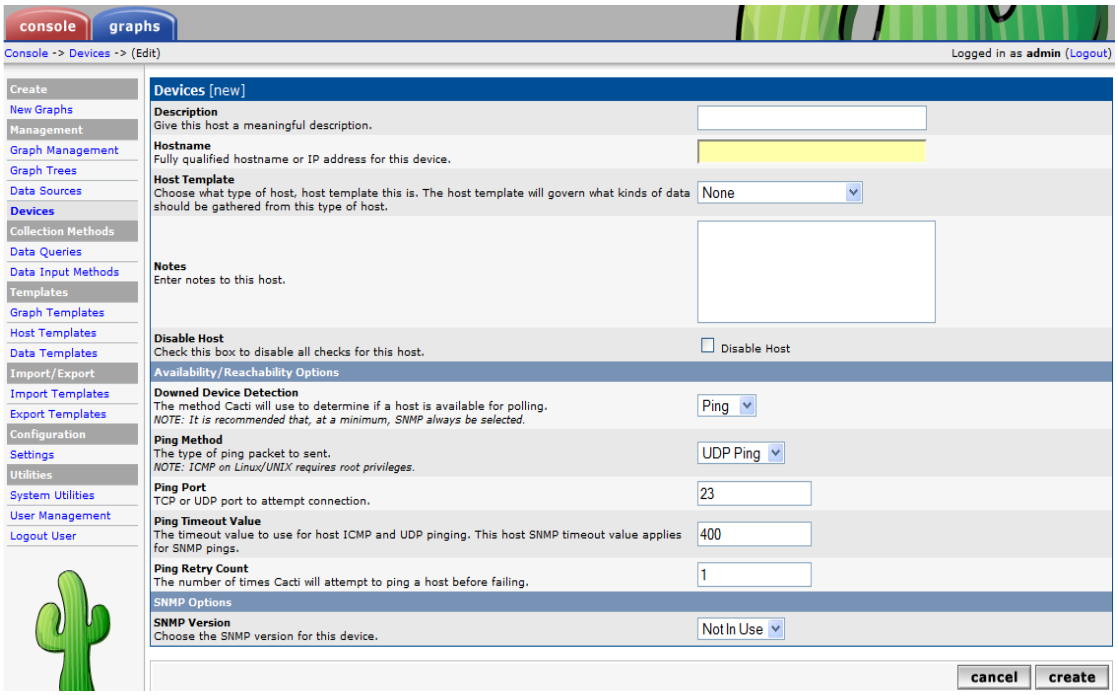
Fonte – CACTI (KUNDU; LAVLU, 2009)

Se você clicar em *Adicionar* no canto superior direito, ele abrirá um novo formulário para adicionar um novo dispositivo. Os dois primeiros campos, "*Descrição"* e *"Nome de host"*, são ambos necessários para a configuração padrão. Os outros campos na seção "*Dispositivo"* (*Notas e Desativar Dispositivo*) podem ser

deixados como estão. Se o modelo de host existir no menu suspenso, certifique-se de selecionar o modelo. Começa-se com um dispositivo habilitado para SNMP, se você não tiver certeza de qual modelo selecionar, você pode selecionar o modelo de host Genérico habilitado para SNMP.

É importante saber que adicionar um modelo a um dispositivo não bloqueará o dispositivo para nenhuma configuração específica, pois modelos de gráfico e consultas podem ser adicionados e removidos de um dispositivo a qualquer momento. A seguinte captura de tela mostra como o formulário *Adicionar um dispositivo* é exibido:

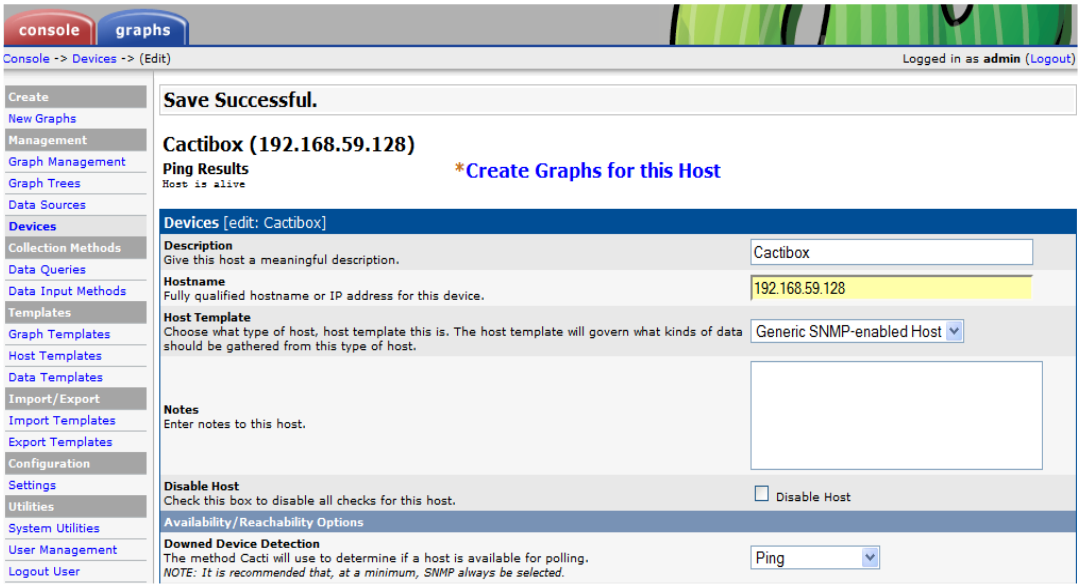
Figura 14 – Criando novo dispositivo.



Fonte – CACTI (KUNDU; LAVLU, 2009)

Depois de criar o dispositivo, *Cacti* redireciona você para o mesmo formulário com informações adicionais. Se for bem-sucedido, será exibida uma tela de informações apresentada na figura 15:

Figura 15 – Formulário de informações.

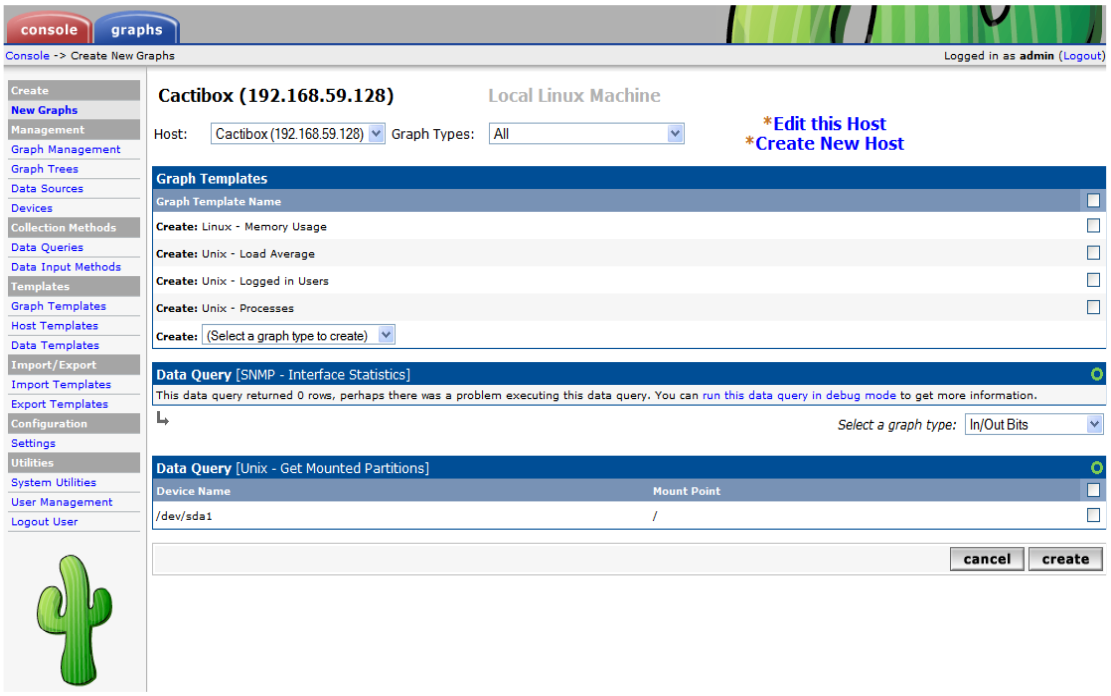


Fonte – CACTI (KUNDU; LAVLU, 2009)

2.4.3 Criando um Gráfico no Dispositivo

Agora que foi criado um dispositivo no sistema, é hora de criar alguns gráficos para este dispositivo. Você pode pular para criar um gráfico a partir de dois locais diferentes: selecione Novos Gráficos em Criar ou se ainda estiver no modo de edição do dispositivo, clique em Criar Gráfico para este Host. Depois de clicar na opção, você pode ver um formulário como o seguinte. Você pode ter opções diferentes com base no dispositivo / host que você escolher na caixa drop-down:

Figura 16 – Criando gráfico no dispositivo.



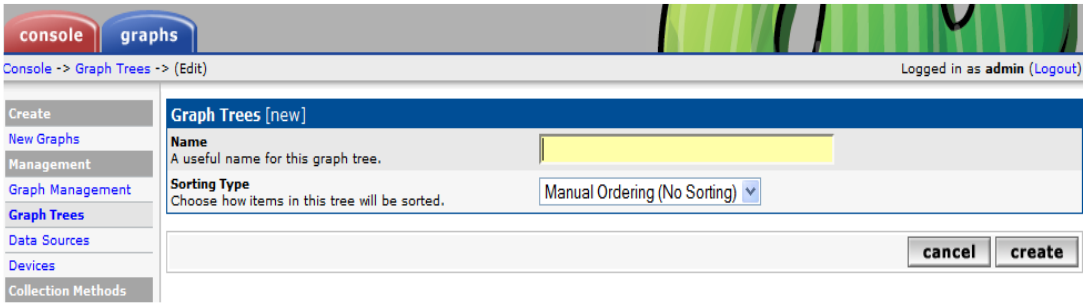
Fonte – CACTI (KUNDU; LAVLU, 2009)

Neste exemplo, cria-se um gráfico para o próprio CactiBox. Assim, você não está vendo algumas opções na seção *Data Query*. Será visto essa seção quando for criado um gráfico para uma interface de rede. É praticamente direto criar um gráfico para um dispositivo. Você só precisa verificar a opção ao lado de linhas diferentes que são mostradas nas seções modelos de gráfico e consulta de dados. Depois de verificar as opções, clique no botão *Criar*. Você verá outro formulário onde pode escolher cores ou legenda e algumas opções adicionais, se os modelos exigirem entrada adicional. Depois de introduzir os valores necessários nesta página, aperte novamente o botão *Criar* para criar os gráficos. *Cacti* então agendará a criação de gráficos para o dispositivo.

2.4.4 Organizando Gráficos

No *Cacti*, os gráficos podem ser organizados em uma estrutura de árvore hierárquica. Cada árvore de gráfico contém zero ou mais ramos contendo hosts ou gráficos individuais. Mesmo cada nó da árvore poderia ter vários ramos. Desta forma, podemos organizar gráficos funcionalmente. Você pode acessar gerenciamento de gráficos em árvores. Na página de *Gráficos Árvores*, clique no botão *Adicionar* para uma nova árvore de gráfico:

Figura 17 – Adicionando gráficos em árvores.



Fonte – CACTI (KUNDU; LAVLU, 2009)

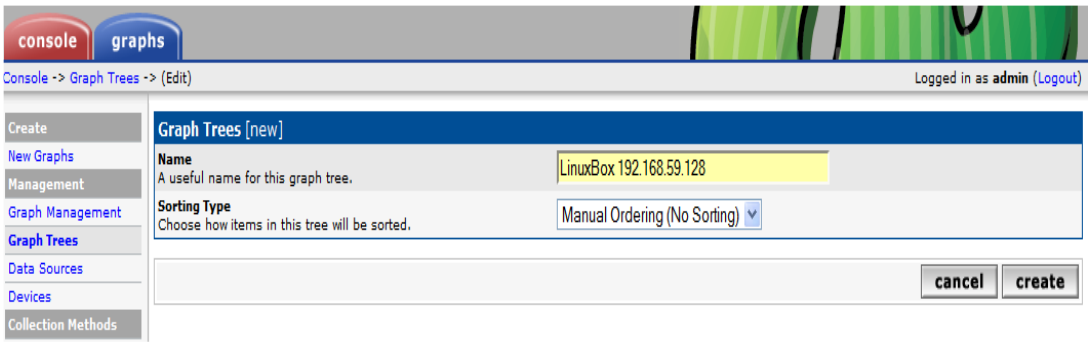
Escolha um nome e selecione um tipo de classificação na caixa suspensa. Há quatro tipos de classificação na caixa suspensa:

- Ordem manual: Cada gráfico/dispositivo adicionado pode ser reordenado dentro da árvore/ramo;
- Ordem Alfabética: Cada gráfico/dispositivo é ordenado alfabeticamente;
- Ordenação Numérica: Cada gráfico/dispositivo é ordenado numericamente;
- Ordenação Natural: Ordenação alfanumérica tendo em conta o aumento numérico.

Você pode escolher a classificação que irá atender às suas necessidades.

Neste exemplo, usa-se um nome de árvore LinuxBox 192.168.59.128 e tipo de classificação ordem manual:

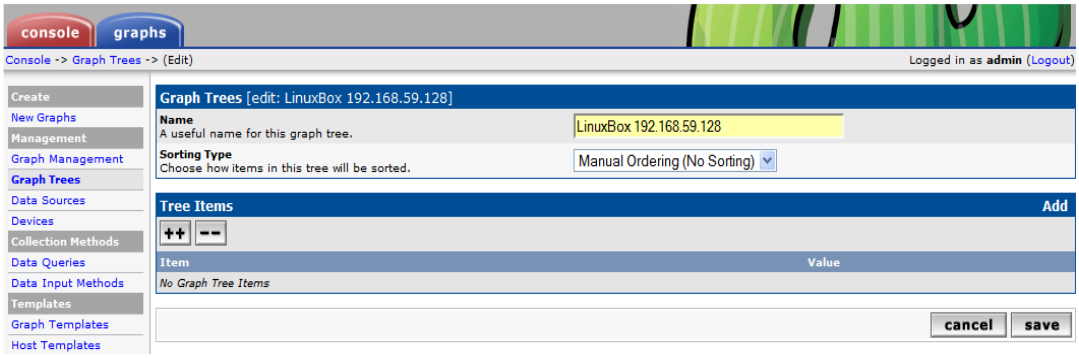
Figura 18 – Ordem Manual.



Fonte – CACTI (KUNDU; LAVLU, 2009)

Selecionando a aba ou icone em gerenciamento de gráficos em árvores, podemos ver o LinuxBox 192.168.59.128. Clique em Linux 192.168.59.128 para adicionar gráficos à árvore:

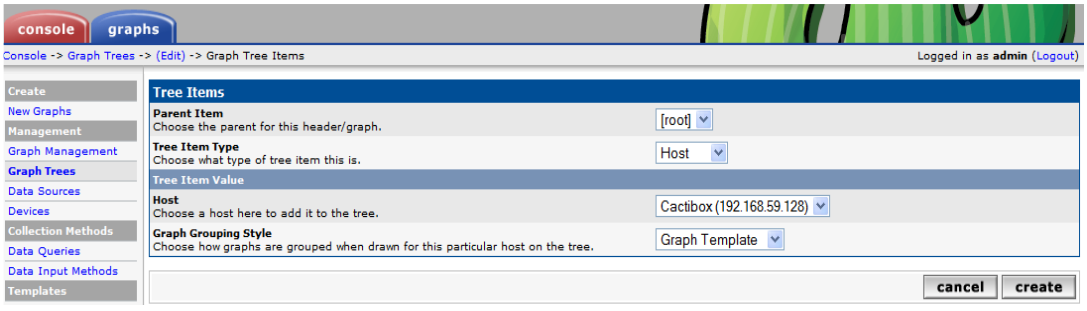
Figura 19 – Gráfico em árvores.



Fonte – CACTI (KUNDU; LAVLU, 2009)

Agora, pressione *Adicionar* na próxima página para adicionar host, cabeçalho e gráficos ao nó. Há uma opção chamada *Tipo de Item de Árvore* onde você pode escolher o tipo de item de árvore - host, cabeçalho ou gráfico. Neste exemplo, adiciona-se o primeiro host, que é Cactibox:

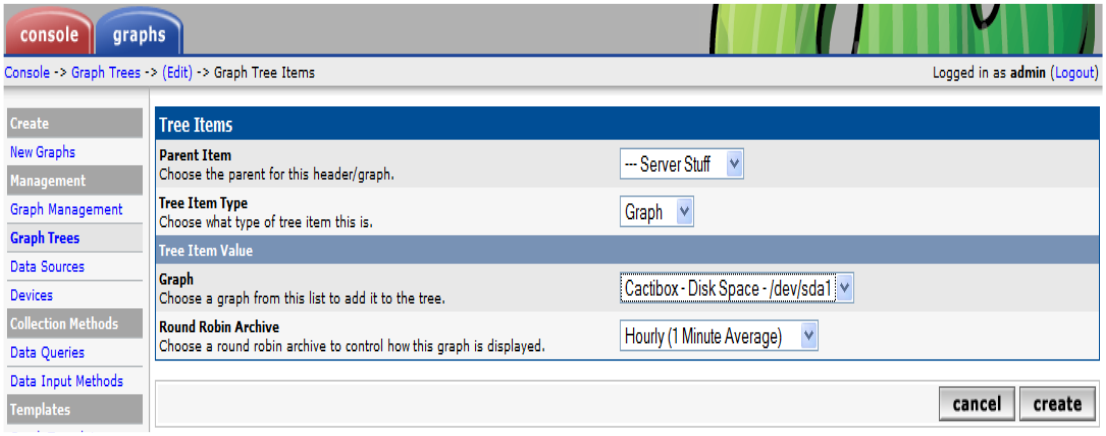
Figura 20 – Adicionar host, cabeçalho ou gráfico.



Fonte – CACTI (KUNDU; LAVLU, 2009)

Agora, pode-se adicionar dois cabeçalhos chamados *Server Stuff* e *Server Traffic*. Quando estiver pronto, adicionaremos gráficos a ambos os cabeçalhos. Para fazer isso, clique em Adicionar e a tela de figura 21, será exibida:

Figura 21 – Gráficos em Stuff e Traffic.



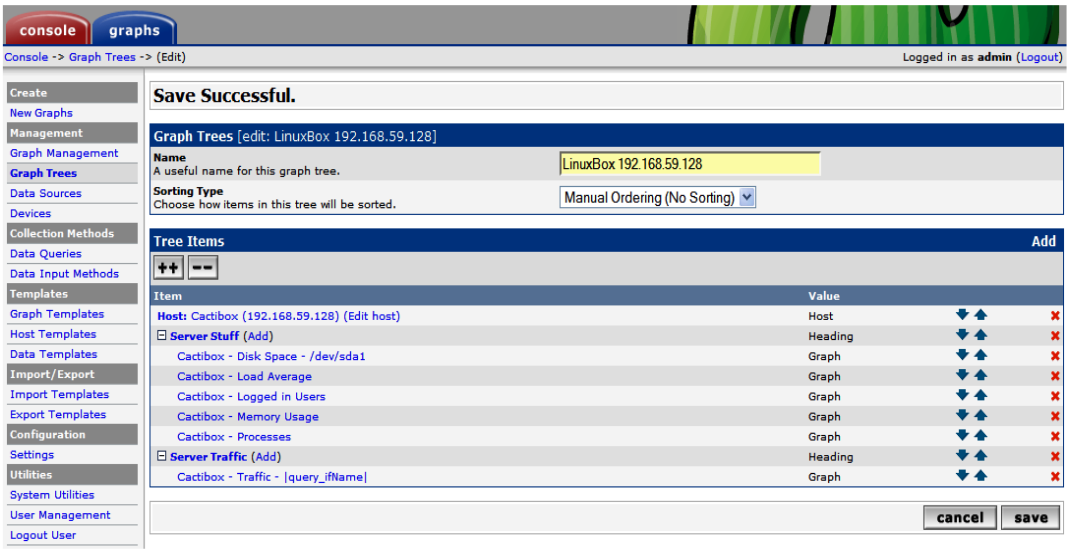
Fonte – CACTI (KUNDU; LAVLU, 2009)

Na caixa suspensa *Item Pai*, selecione *Material do Servidor*, gráfico no *Tipo de Item da Árvore*, Cactibox - espaço em disco - / dev / sda1 no gráfico e hora (média de 1 minuto) no arquivo *Round Robin*. Da mesma forma, adicione os seguintes gráficos em *Server Stuff*:

- Load Average
- Logged in Users
- Memory Usage
- Processes

No final, adicione *Tráfego* em *Tráfego do Servidor*. Quando terminar, a árvore de gráficos LinuxBox 192.168.59.128 será semelhante à imagem a seguir:

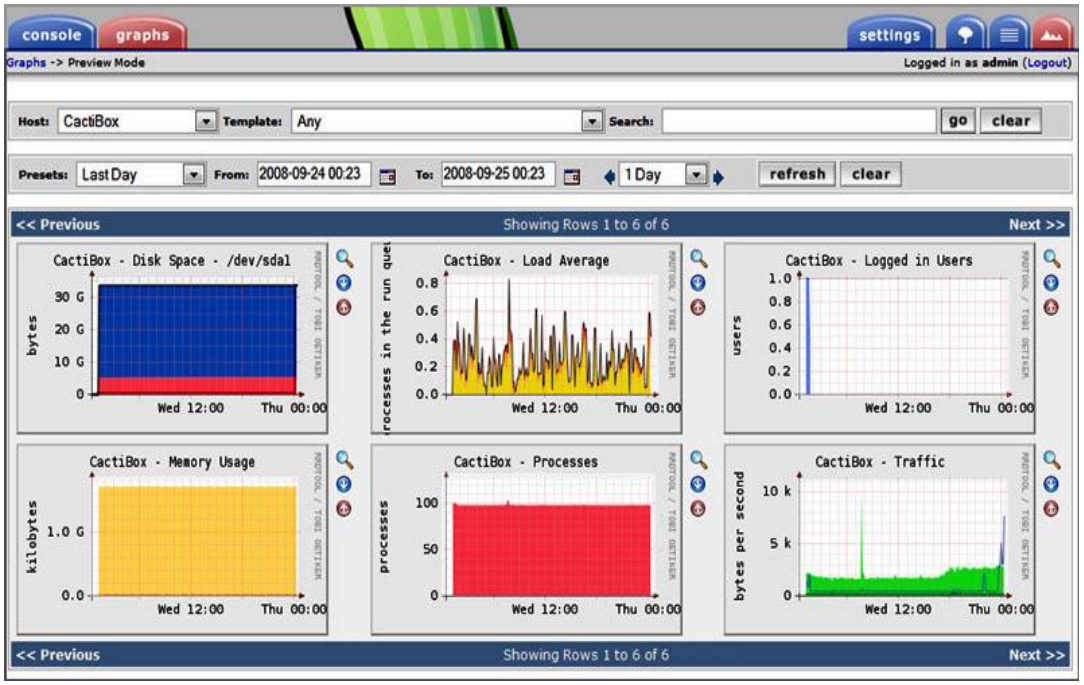
Figura 22 – Server Traffic.



Fonte – CACTI (KUNDU; LAVLU, 2009)

Agora, é possível ver os gráficos como o seguinte, clicando na guia *Gráficos* na parte superior. Para mostrar os gráficos em três colunas, foram alteradas algumas configurações:

Figura 23 – Gráficos em colunas.

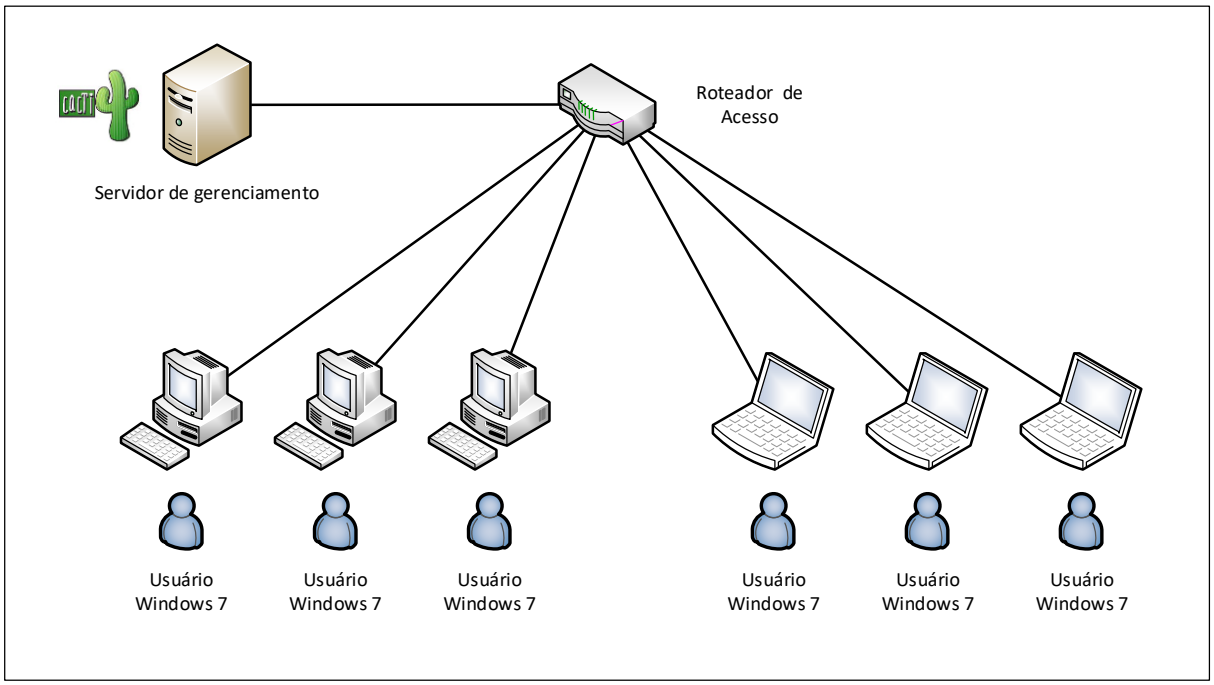


Fonte – CACTI (KUNDU; LAVLU, 2009)

3 IMPLANTAÇÃO E TESTES

O cenário de implantação e testes é composto por uma rede pequena com algumas máquinas físicas. Existe um servidor de gerenciamento, um roteador de pacotes e algumas máquinas conectadas à rede, essas máquinas utilizam o sistema operacional Windows 7, o cenário descrito pode ser visualizado na figura 24.

Figura 24 – Ambiente de implementação.



Fonte – Elaborado pelo autor

O CACTI foi instalado, no sentido de gerenciamento, através do código fonte em um servidor virtual, estrategicamente localizado no servidor de gerenciamento, possibilitando assim a comunicação entre todos os *hosts* da rede.

3.3 Ambiente de Implantação

Em tal ambiente, grande parte dos esforços associados ao seu gerenciamento estão voltados a sua máxima disponibilidade, escalabilidade e no aproveitamento de

seus recursos computacionais da melhor forma possível, objetivando menores quantidades de intervenções corretivas e minimizando ou evitando a ocorrência de situações de degradações e interrupções de modo geral. Desta forma é indispensável utilizar ferramentas que contribuam para que tais objetivos sejam alcançados e mantidos, os quais podem ser simplificados e realizados, por exemplo, por meio da solução de gerenciamento CACTI.

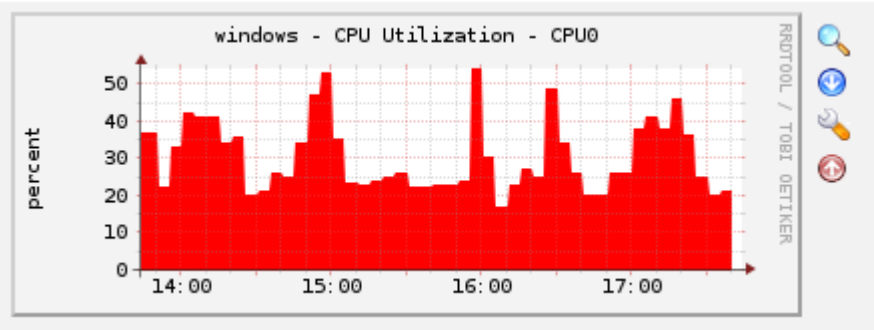
Por meio da solução CACTI é possível visualizar, em frações de segundos e de modo simples e objetivo, gráficos associados à utilização dos vários recursos dos servidores e equipamentos virtualizados no ambiente.

3.4 Testes Realizados

Para o procedimento de testes o servidor do CACTI permaneceu ligado por duas semanas para monitorar os equipamentos da rede e identificar seu comportamento diante dos eventos de falhas e uso dos equipamentos monitorados. Foi verificado que os gráficos gerados pela ferramenta apresentam informações muito úteis para a tomada de decisões em uma rede, como no caso de uma falha de uma das máquinas.

Na opção de *Graphic Preview Mode* é possível verificar os gráficos de monitoramento dos computadores no período de 4 horas. O período da tarde é aonde encontra-se a maior utilização de recursos na rede. Conforme a figura 25 é possível observar o gráfico associado à utilização de recursos de processamento do computador que está sendo monitorado.

Figura 25 – Utilização de CPU

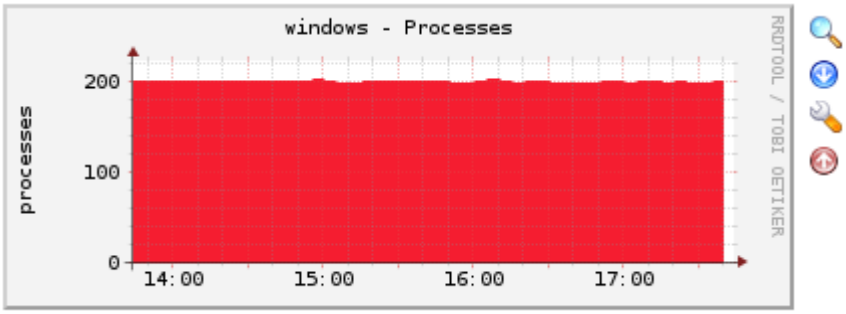


Fonte – Elaborado pelo autor

Observe que, por meio desse gráfico, é possível visualizar de forma simples e objetiva a carga de processamento desse equipamento em momentos específicos de sua utilização.

Já na figura 26 é possível monitorar os processos que estão rodando no equipamento monitorado. Este gráfico coleta informações em um período de 4 horas.

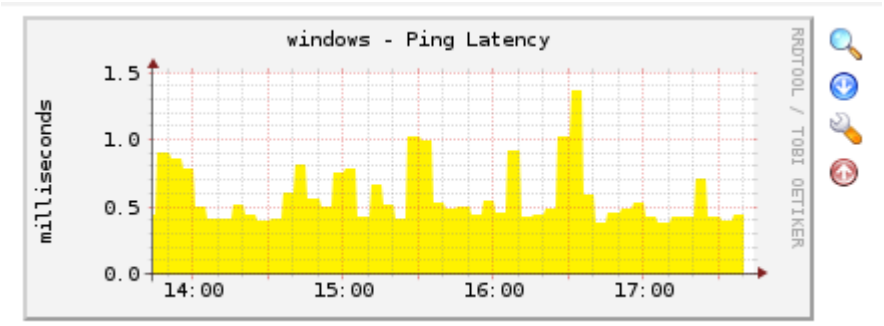
Figura 26 – Processos



Fonte – Elaborado pelo autor

Na figura 27 é possível observar a latência de *ping* de uma máquina que está sendo monitorada. Neste gráfico foi coletado informações num período de 4 horas. Percebe-se uma maior utilização de banda no período entre 15:30 horas e 16:30 horas, devido ao grande consumo de banda larga.

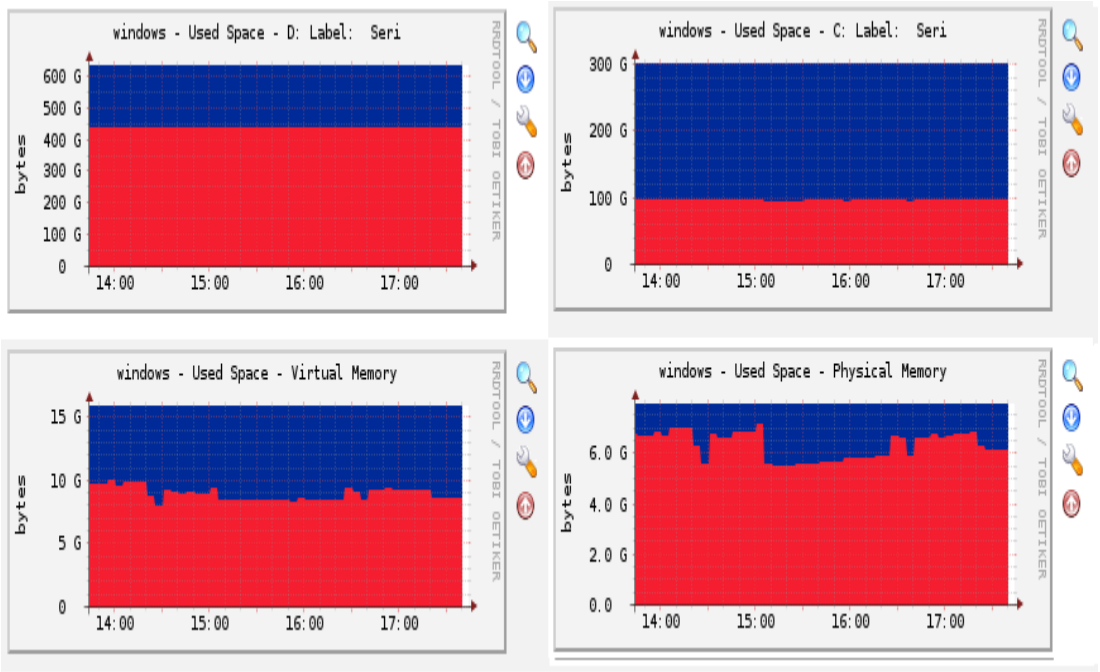
Figura 27 – Latência de *ping*



Fonte – Elaborado pelo autor

De forma similar e complementar às informações sobre recursos como utilização de memória física e virtual, assim como armazenamento em discos também podem ser monitoradas, conforme imagem 28.

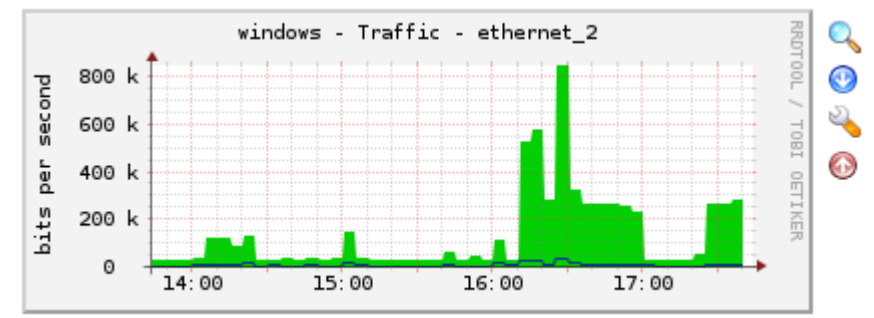
Figura 28 – Armazenamento



Fonte – Elaborado pelo autor

É possível obter informações de qualquer dispositivo conectado à rede e executando o protocolo SNMPv3, capturando informações do tráfego na rede, conforme ilustra a imagem 29.

Figura 29 – Tráfego de redes



Fonte – Elaborado pelo autor

3.5 Resultados

No período de duas semanas foi observado diariamente o comportamento dos equipamentos para identificar eventos de falhas e uso. Pela análise dos gráficos foi possível observar que o *Cacti* é uma ferramenta importante, pois apresenta informações úteis para a tomada de decisões em uma rede.

O *Cacti* apresenta gráficos que geram um histórico preciso do consumo de recursos tais como memória, tráfego de interfaces de rede, erros nas interfaces de rede e outros. O interessante é que a ferramenta está configurada para registrar eventos a cada 5 minutos, resultando em gráficos diários com histórico da média de utilização calculada de 5 em 5 minutos; gráficos semanais, com histórico da média de utilização calculada de 30 em 30 minutos; gráficos mensais, com histórico da média de utilização calculada de 2 em 2 horas e gráficos anuais com histórico da média de utilização calculada a cada 24 horas. Isso possibilita que os administradores de rede percebam os momentos de maior utilização de um determinado recurso, identificando assim possíveis gargalos e planejando com maior segurança a expansão da rede.

CONCLUSÃO

As possibilidades do software *Cacti* são muitas. Quando utilizado em suas funções básicas é possível visualizar gráficos diários, semanais, mensais e anuais sobre utilização de interfaces de rede, CPU, memória, espaço em disco, entre outros. Mas quando são adicionadas as funcionalidades desenvolvidas pela comunidade do *Cacti*, como *plugins* e *templates* diversos este software se torna excelente para qualquer área funcional do gerenciamento de redes, além de ficar muito mais robusto e funcional.

São evidentes as vantagens da implantação do software *Cacti* em qualquer ambiente de rede, devido a sua robustez, facilidade de implantação e excelente desempenho. É uma economia para qualquer empresa com suporte de TI, pois economiza com a aquisição do software, por ser gratuito, tem aperfeiçoamento constante, com foco na qualidade e diversificação de ferramentas pela comunidade de software livre, além de ser possível fazer uma adaptação do software aos objetivos específicos de cada pessoa ou empresa.

Tudo isso é possível graças ao SNMP, sem o qual provavelmente o mundo do monitoramento das redes de computadores não seria o mesmo. Uma solução de gerenciamento baseada em SNMP, ainda que não contemple todas as áreas nas quais o protocolo se desdobra, se implantada numa rede antes desprovida de um sistema de gerenciamento, eleva significativamente o padrão de qualidade do trabalho do administrador de rede. Faz isso por diminuir o tempo de detecção de falhas, auxiliar ativamente na detecção de gargalos e na expansão da rede, manter histórico de contabilização de recursos, de disponibilidade e de tendências, e por permitir ao administrador ter uma visão acurada e centralizada de todos os elementos importantes da rede.

Naturalmente, uma solução de gerenciamento de rede não substitui o administrador de rede, apenas o instrumentaliza para suas atividades, facilitando sua vida. Por outro lado, o fato de ferramentas de software poderem fazer a leitura do estado do próprio software e também do hardware, é fascinante. Talvez num futuro seja possível desenvolver ferramentas mais inteligentes, capazes de reparar falhas de software ou até mesmo de hardware, o que certamente tornará ainda mais interessante a fantástica área de monitoramento de redes de computadores.

Por fim, de modo complementar a tais benefícios e características, a solução CACTI, que é *software* livre, pode ser customizada e adequada aos mais variados e complexos ambientes computacionais, fornecendo recursos em nível de codificação ou de integrações por meio de arquivos de configurações a uma grande quantidade de outras ferramentas e soluções, contribuindo para o gerenciamento proativo dos mais variados e complexos ambientes de rede.

REFERÊNCIAS

CACTI, The Complete RRDtool-based Graphing Solution. **Cacti Manual 0.8.7**. Atualizada em Janeiro de 2011. Disponível em: http://docs.cacti.net/manual:087.

CONNER, Jimmy. **CactiUser** – Plugins. Atualizada em Janeiro de 2011. Disponível em: http://cactiusers.org/downloads/.

KUNDU, Dinangkur e S.M. Ibrahim LAVLU. Monitor your network with ease. **Cacti 0.8 Network Monitoring** Packt Publishing (31 de julho de 2009)

KUROSE, James F. e ROSS, Keith W. **Redes de Computadores e a Internet** – Uma abordagem Top Down. 3ª edição. São Paulo: Pearson Addison Wesley, 2006.

OETIKER, Tobias. **RRDtool** – Logging & Graphing, Documentation. Atualizada em Junho de 2011. Disponível em: http://oss.oetiker.ch/rrdtool/doc/rrdtool.en.html.

STALLINGS, William. **SNMP, SNMPv2, SNMPv3, RMON 1 and RMON 2**. 3. ed. Massachusetts: Pearson Addison Wesley, 1999.

TANENBAUM, Andrew S. **Redes de Computadores**. 4. ed. Rio de Janeiro: Campus, 2003.