UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

LEANDRO KOEHLER CARDOSO

IMPLANTAÇÃO DA FERRAMENTA NAGIOS PARA MONITORAÇÃO DE REDE E ANÁLISE E TRATAMENTO DOS EVENTOS POR MEIO DE SOFTWARES DE APOIO

CRICIÚMA, DEZEMBRO DE 2011

LEANDRO KOEHLER CARDOSO

IMPLANTAÇÃO DA FERRAMENTA NAGIOS PARA MONITORAÇÃO DE REDE E ANÁLISE E TRATAMENTO DOS EVENTOS POR MEIO DE SOFTWARES DE APOIO

Trabalho de Conclusão de Curso apresentado para Obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. MSc. Rogério Antônio Casagrande.

CRICIÚMA, DEZEMBRO DE 2011

LEANDRO KOEHLER CARDOSO

IMPLANTAÇÃO DA FERRAMENTA NAGIOS PARA MONITORAÇÃO DE REDE E ANÁLISE E TRATAMENTO DOS EVENTOS POR MEIO DE SOFTWARES DE APOIO

Submetido ao corpo docente do Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense como um dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Profa. MSc. Ana Claudia Garcia Barbosa
Coordenadora do Curso de Ciência da Computação

Banca Examinadora:

Prof. MSc. Rogério Antônio Casagrande (UNESC)
Orientador

Prof. MSc. Gustavo Bisognin (UNESC)

Prof. Esp. Sérgio Coral (UNESC)

Dedico este trabalho ao meu pai Valdemar Pedro Cardoso por tudo que fez por mim, e com todo seu empenho junto com minha mãe Juraci K. Cardoso que me orientaram na vida e como pessoa.

AGRADECIMENTOS

Agradeço a Deus, aos meus pais por todo incentivo e força para que eu pudesse ter um ensino superior, a minha esposa Mariane por me incentivar nos momentos difíceis.

Não posso deixar de agradecer ao meu orientador Professor Rogério Antônio Casagrande por toda ajuda e paciência comigo neste trabalho de conclusão de curso e aos meus professores, colegas de curso e amigos que me auxiliaram nas dificuldades do projeto.

“Só existem dois dias no ano que nada pode ser feito. Um se chama ontem e o outro se chama amanhã, portanto hoje é o dia certo para amar, acreditar, fazer e principalmente viver.”

Dalai Lama

RESUMO

Este trabalho tem como objetivo avaliar o comportamento do Nagios no levantamento de dados dos problemas detectados na rede. O estudo foi realizado em um ambiente controlado, próprio para testes simulando diversos eventos e erros, assim podendo verificar o desempenho da rede e dos equipamentos monitorados dos erros levantados pelo Nagios e o software de apoio Cacti. Foram avaliadas as ferramentas com o intuito de comprovar o funcionamento e a eficácia no auxílio dos profissionais que desejam implantar esta tecnologia, como solução de software livre para monitorar rede e equipamentos. Foi realizado um estudo do funcionamento da rede, sua estrutura e protocolos, como também métodos de monitoramento e gerenciamento de rede a fim de ter um embasamento amplo para implementar as ferramentas de gerenciamento de rede e poder realizar os testes com segurança e levantar os dados que indicarão se a utilização do Nagios em conjunto com Cacti realmente podem auxiliar na administração de um ambiente de rede complexo.

Palavras-Chave: Cacti, Gerenciamento de rede, Monitoramento, Nagios, Software livre.

ABSTRACT

This study aims to evaluate the behavior of Nagios in the data collection of problems detected on the network. The study was conducted in a controlled environment, suitable for tests simulating various events and errors, making it possible to check the performance of the network and equipment's monitored by Nagios and Cacti support software. Tools were evaluated in order to demonstrate the operation and effectiveness in helping practitioners who want to deploy this technology as a free software solution to monitor network and equipment. A study of the functioning of the network structure and protocols was conducted, as well as methods for monitoring and network management in order to have a broad foundation to implement network management tools and can safely perform the tests and to be able to collect data that indicate whether the use of Nagios in conjunction with Cacti can actually assist in managing a complex network environment.

Keywords*: Cacti, Network Management, Monitoring, Nagios, Free Software.*

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

CGI	Common Gateway Interface
CMIP	Common Management Information Protocol
CPU	Central Processing Unit
CRC	Cyclic redundancy check
DARPA	Defense Advanced Research Agency
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
MRTG	Multi Router Traffic Grapher
NetBEUI	NetBIOS Extended User Interface
NNTP	Network News Transfer Protocol
NRPE	Nagios Remote Plugin Executor
NSCA	Nagios Service Check Acceptor
OSI	Open Systems Interconnection
PHP	Personal Home Page
POP3	Post Office Protocol Versão 3
RRDTool	Round Robin Database Tool
SMTP	Simple Mail Transfer Protocol
SNMP	Simpe Network Management Protocol
SPX	Sequenced Packet Exchange

SSH	Secure Shell
TCP	Transmission Control Protocol

SUMÁRIO

1 INTRODUÇÃO

Com elevado número de máquinas interligadas e distribuídas numa grande estrutura, fica quase impossível gerenciar e monitorar todos os eventos ocorridos em uma rede de computadores, onde se tem de ficar conectado 24 horas por dia e 7 (sete) dias por semana. Por isso, utilizar uma ferramenta de monitoração seria de fundamental importância para poder sanar o mais rápido possível, eventuais problemas que possam ocorrer nesta estrutura.

Existem diversas ferramentas para monitoramento de serviços e hardware. Diante deste cenário, é de extrema importância definir exatamente quais são as necessidades antes de fazer a escolha da ferramenta mais adequada. É importante separar em grupos as ferramentas de acordo com aquilo que elas monitoram com mais eficiência. Têm-se como grupos principais os que monitoram em nível de sistema operacional, monitoramento de rede, monitoramento por meio de robôs e acompanhamento por alarmes. A Ferramenta Nagios pode monitorar elementos de rede ou mesmo hardwares proprietários por consultas SNMP.

A utilização da ferramenta Nagios, trata-se de uma solução gratuita e extremamente eficiente e flexível, tendo algumas das características como: o monitoramento de serviços de rede, monitoramento de recursos de servidores como CPU, memória, disco e processos. Tem a capacidade de definir hierarquia da rede, enviar notificações imediatamente sobre problemas na rede via e-mail e Pager.

O Nagios pode tomar contramedidas de acordo com o problema na rede, gerar relatórios, gráficos e históricos dos acontecimentos. É versátil, flexível e verifica constantemente a disponibilidade dos serviços e hosts.

Com isso, é possível demonstrar diversas maneiras de interagir com os problemas utilizando a ferramenta Nagios e alguns softwares de apoio, no monitoramento de serviços, hardware e softwares analisando e tratando os eventos apresentados. A principal utilização

desta ferramenta está em evitar problemas de rede por meio de monitoramento evitando que algum equipamento ou toda estrutura fique parada por minutos, horas ou até mesmo dias, já que todo equipamento não dá 100% de garantia de sua utilização.

1.1 OBJETIVO GERAL

Implantar e avaliar o comportamento da ferramenta de monitoramento Nagios no levantamento de soluções dos problemas detectados em uma rede em conjunto com o software de apoio o Cacti.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos são listados abaixo:

a) estudar software livre Nagios;
b) estudar *Plugins* e software Cacti aplicados à ferramenta Nagios;
c) simular eventos de erros relacionados ao funcionamento da rede;
d) documentar resultados alcançados com a implantação do software Nagios;
e) validar resultados e avaliação geral da ferramenta.

1.3 JUSTIFICATIVA

Quando algo estranho está ocorrendo na rede à equipe de gerência deve ser notificada. São muitas as situações que podem gerar um evento: dispositivos ou interfaces não operacionais, padrões de tráfego estranhos, serviços não respondendo a uma requisição ou respondendo de forma lenta, entre outros (LOPES et al, 2003).

A detecção de um evento pode ser do tipo preventiva ou reativa. As detecções preventivas são aquelas que têm por objetivo evitar que o problema aconteça avisando o responsável pela rede quando algo esta para acontecer. Já as detecções reativas têm por objetivo informar que o problema está acontecendo. Indisponibilidade de comunicação e serviços são exemplos que caracterizam esta situação. Quando apresentar uma ocorrência desse tipo o responsável pela rede tem de buscar a solução no menor tempo possível, pois em geral essa situação implica em prejuízo para a empresa.

O Software de monitoração Nagios, dentre suas características tem o monitoramento de serviços de rede como SMTP, POP3, HTTP, NNTP, entre outros. O monitoramento de rede e sistemas proporcionado por esta aplicação permite a verificação de equipamentos e serviços desejados e gerar alarmes quando necessário, possibilitando definir tratadores de eventos durante o gerenciamento, o que possibilita um gerenciamento preventivo ou reativo (reativo e pró-ativo).

Deste modo os responsáveis pela rede terão possibilidade de atuar instantaneamente na solução dos problemas ocorridos na infraestrutura, bem como, a disponibilidade de informações relativamente importantes que podem contribuir para evitar a interrupção de seus serviços de rede.

Devido ao grande fluxo de informações e o expressivo aumento do número de usuários e equipamentos nos mais diversos setores, observou-se a necessidade da implantação de um sistema como o Nagios, que monitorasse a rede e os serviços, evitando que setores importantes ou mesmo todo o ambiente computacional da empresa possam parar, já que praticamente todos os setores hoje são informatizados e dependentes da informática. A falha em alguma unidade de rede (como switch) pode paralisar setores chaves gerando grandes transtornos.

Com um número reduzido de funcionários e sempre com contenção de despesas, a implantação de uma ferramenta como o Nagios poderá ajudar a ter um ambiente computacional com poucas possibilidades de falhas. Tornando-se importante para futuras aplicações e correções, visando estabilidade e segurança de todo o ambiente computacional.

1.4 ESTRUTURA DO TRABALHO

Neste trabalho de conclusão de curso encontra-se um breve relato sobre redes de computadores, seus protocolos e arquiteturas, passando para o conceito de gerência de redes e alguns métodos como, gerência de falhas e desempenho com a utilização do SNMP e suas aplicações.

A seção seguinte descreve sobre as ferramentas de monitoração de rede e suas características. Dentre essas ferramentas o Nagios e o Cacti foram escolhidos para serem utilizadas neste trabalho e estão descritas em detalhes, seus recursos e maneiras que podem ser empregadas na gerência de rede.

Também são apresentados os trabalhos correlatos que auxiliaram na realização deste trabalho seguindo com o trabalho realizado, descrevendo como foi montado o ambiente a ser gerenciado com a proposta de solução de gerenciamento. Simulações e testes foram empregados em busca de resultados, para avaliar as ferramentas de monitoramento, verificando se realmente atende as necessidades e se é viável sua implantação, concluindo o trabalho.

2 REDES DE COMPUTADORES

Atualmente, com a importância cada vez maior de se dispor de acesso a informações e facilidades de comunicação, as redes de computadores estão projetadas para crescer indefinidamente (CANTÚ, 2003).

Redes de computadores são estruturas físicas (equipamentos) e lógicas (programas, protocolos) que permitem que dois ou mais computadores possam compartilhar suas informações entre si (CARVALHO, 2009).

Na Figura 1 apresenta uma das estruturas de redes mais utilizadas, estrutura de rede do tipo estrela.

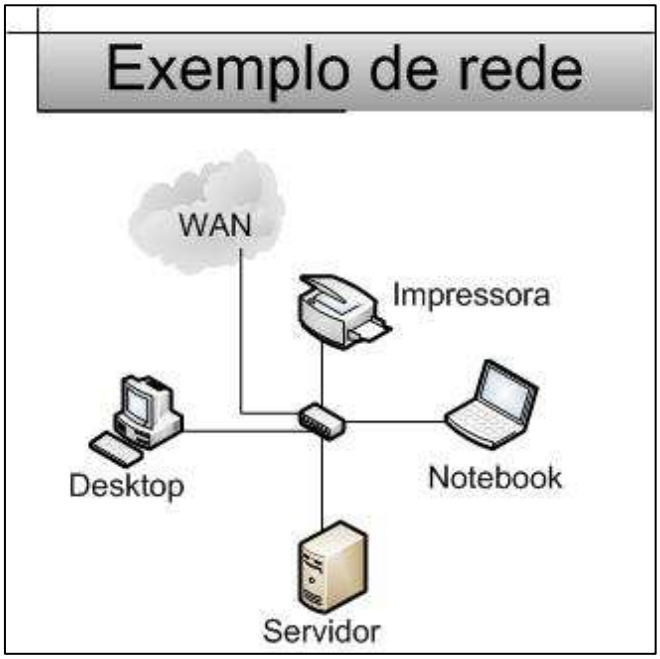


Figura 1. Exemplo de rede de computadores

O uso das redes vem, a cada dia, tornando-se um recurso indispensável em todos os locais onde existe um conjunto de computadores. Com o crescimento da Internet, abrangendo todos os ramos de atividades, aumentou ainda mais a necessidade de ligação dos computadores em redes, entretanto, é importante saber que há vantagens e desvantagens do

uso das redes e também os cuidados que deve-se tomar para evitar os problemas (MENDES, 2007).

Problemas que ocorrem nos aparelhos que centralizam as informações, tais como o HUB, switch, servidores de rede podem gerar muitos problemas como lentidão da rede, lentidão de uma parte da rede ou até a sua parada definitiva independente da topologia utilizada (MENDES, 2007).

2.1 AMBIENTE DE REDE

As redes de computadores foram projetadas, inicialmente, como um mecanismo para permitir o compartilhamento de recursos caros, tais como, impressoras, modem de alta velocidade, etc, existindo apenas em ambientes acadêmicos, governamentais (principalmente em organizações militares) e em empresas de grande porte. Entretanto, a evolução das tecnologias de redes aliada à grande redução de custos dos recursos computacionais, motivou a proliferação das redes de computadores por todos os segmentos da sociedade (MENEZES, 1998).

À medida que essas redes foram crescendo e tornando-se integradas às organizações, o compartilhamento dos dispositivos adquiriu aspecto secundário em comparação às outras vantagens oferecidas. As redes passaram então a fazer parte do cotidiano das pessoas como uma ferramenta que oferece recursos e serviços que permitem uma maior interação entre os usuários e um consequente aumento de produtividade (PINHEIROS, 2006).

Pinheiros (2006), acrescenta ainda que também ocorreu uma grande mudança nos serviços oferecidos. Além do compartilhamento de recursos, novos serviços, tais como, correio eletrônico, transferência de arquivos, Internet, aplicações multimídia dentre outras,

foram acrescentadas, aumentando ainda mais a complexidade das redes. Não bastassem esses fatos, o mundo da interconexão de sistemas ainda passou a conviver com a grande heterogeneidade de padrões, sistemas operacionais, equipamentos etc.

2.2 PROTOCOLOS DE COMUNICAÇÃO

Toda rede de computadores tem sua comunicação dependente de um protocolo ou de vários. Protocolo é o nome dado a um conjunto de regras que os computadores devem seguir para que a comunicação entre eles permaneça estável e funcional (CARVALHO, 2009).

Os programas aplicativos que usam uma rede não interagem diretamente com o hardware de rede. Em vez disso, um aplicativo interage com o software de protocolo que segue as regras de um determinado protocolo quando da comunicação (COMER, 2007).

Os protocolos definem o formato e a ordem das mensagens enviadas e recebidas pelas entidades da rede bem como as ações que são tomadas quando da transmissão ou recepção da mensagem (CANTÚ, 2003).

2.3 MODELO OSI

O principal objetivo para a criação de um modelo de protocolos de interconexão para comunicação de dados entre dispositivos foi à padronização.

Para facilitar a interconexão de sistemas de computadores, a Organização Internacional para Padronização do inglês International Standards Organization (ISO) desenvolveu um modelo de referência chamado Interconexão de Sistemas Abertos do inglês Open Systems Interconnection (OSI).

OSI foi desenvolvido com o objetivo de facilitar a elaboração de aplicações distribuídas que pudessem ser executadas em equipamentos de diferentes fornecedores, permitindo a intercomunicação de maneira transparente (TEIXEIRA JÚNIOR et al, 1999).

O principal enfoque desse modelo é o conceito de camada, em que cada camada executa uma função específica, fornecendo um serviço de qualidade para as camadas superiores, pela adição de funcionalidades das camadas inferiores (TEIXEIRA JÚNIOR et al, 1999).

O modelo OSI é dividido em sete camadas. É interessante notar que o TCP/IP (provavelmente o protocolo de rede mais usado atualmente) e outros protocolos "famosos" como o IPX/SPX (usado pelo Novell Netware) e o NetBEUI (usado pelos produtos da Microsoft) não seguem esse modelo ao pé da letra, correspondendo apenas a partes do modelo OSI (TORRES, 2007).

Pode-se observar na Figura 2 as camadas na sua organização.

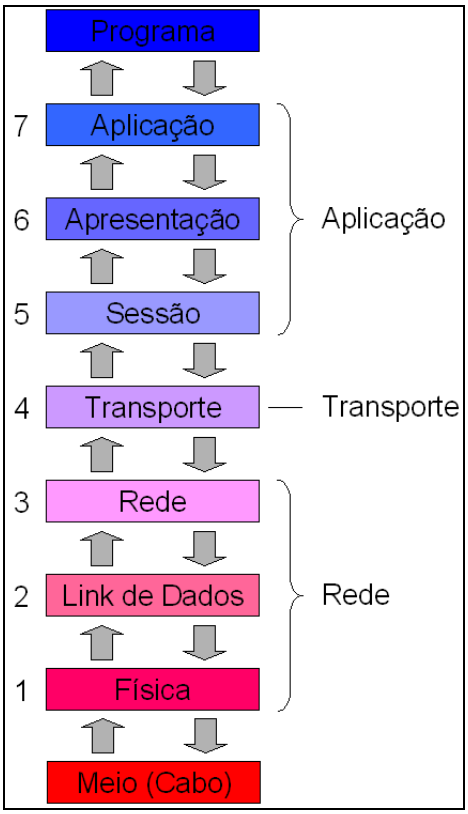


Figura 2. As sete camadas do modelo OSI
Fonte: TORRES, G. (2007)

No modelo OSI os programas comunicam-se apenas com a camada 7, a camada de Aplicação, enquanto que a camada “abaixo” da camada 1 é o meio de transmissão da rede (por exemplo, cabo ou ar, no caso de redes sem fio). O cabeamento de rede é às vezes referido como “camada 0”.

As sete camadas podem ser agrupadas em três grupos: Aplicação, Transporte e Rede.

As camadas do grupo Rede são camadas de baixo nível que lidam com a transmissão e recepção dos dados da rede, transporte é a camada responsável por pegar os dados recebidos da rede e transformá-los em um formato compreensível pelo programa. Quando seu computador está transmitindo dados, esta camada pega os dados e os divide em vários pacotes para serem transmitidos pela rede. Quando seu computador está recebendo dados, esta camada pega os pacotes recebidos e os coloca em ordem; e na camada de Aplicação, camada de mais alto nível, que colocam os dados no formato usado pelo programa.

2.3.1 Camadas OSI

Cada camada no modelo OSI, contém uma ou mais entidades conceituais para definir suas funções. Essas entidades comunicam-se com suas entidades parceiras (ou entidades pares) por meio dos protocolos de comunicação, os quais envolvem comandos formalizados e regras relacionadas utilizadas para garantir o trabalho cooperativo em cada lado, de modo que se consiga efetivar as funções comuns de cada camada (TEIXEIRA JÚNIOR et al, 1999).

Camada 7 – Aplicação: a camada de aplicação faz a interface entre o programa que está enviando ou recebendo dados e a pilha de protocolos.

Camada 6 – Apresentação: também chamada camada de Tradução, esta camada

converte o formato do dado recebido pela camada de Aplicação em um formato comum a ser usado pela pilha de protocolos.

Camada 5 – Sessão: esta camada permite que dois programas em computadores diferentes estabeleçam uma sessão de comunicação. Nesta sessão, esses dois programas definem como será feita a transmissão dos dados e coloca marcações nos dados que estão sendo transmitidos. Se porventura a rede falhar, os dois computadores reiniciam a transmissão dos dados a partir da última marcação recebida em vez de retransmitir todos os dados novamente.

Camada 4 – Transporte: nas redes de computadores os dados são divididos em vários pacotes. Quando você está transferindo um arquivo grande, este arquivo é dividido em vários pequenos pacotes. No computador receptor, esses pacotes são organizados para formar o arquivo originalmente transmitido. A camada de Transporte é responsável por pegar os dados enviados pela camada de Sessão e dividi-los em pacotes que serão transmitidos pela rede. No computador receptor, a camada de Transporte é responsável por pegar os pacotes recebidos da camada de Rede e remontar o dado original para enviá-lo à camada de Sessão.

Camada 3 – Rede: esta camada é responsável pelo endereçamento dos pacotes, convertendo endereços lógicos em endereços físicos, de forma que os pacotes consigam chegar corretamente ao destino. Essa camada também determina a rota que os pacotes irão seguir para atingir o destino, levando em consideração fatores como condições de tráfego da rede e prioridades.

Camada 2 – Link de Dados: essa camada (também chamada camada de Enlace) pega os pacotes de dados recebidos da camada de rede e os transforma em quadros que serão trafegados pela rede, adicionando informações como o endereço da placa de rede de origem, o endereço da placa de rede de destino, dados de controle, os dados em si e uma soma de verificação, também conhecida como CRC. O quadro criado por esta camada é enviado para a

camada Física.

Camada 1 – Física: esta camada pega os quadros enviados pela camada de Link de Dados e os transforma em sinais compatíveis com o meio onde os dados deverão ser transmitidos.

2.4 ARQUITETURA TCP/IP

A agência Defense Advanced Research Agency (DARPA), juntamente com outras organizações, desenvolveu um conjunto padrão de protocolos não proprietários para fornecer comunicação facilitada entre os computadores conectados a uma rede multinós. Esses protocolos foram implementados com 10 anos de antecedência com relação aos protocolos OSI/ISO (TEIXEIRA JÚNIOR et al, 1999).

O conjunto de Protocolos da internet TCP/IP é o padrão mundial para interconexão de sistemas abertos. Nenhum outro conjunto de protocolos proporciona tanta interoperabilidade ou abrange sistemas de tantos fornecedores (COMER, 1999).

O nome TCP/IP, usado para definir a pilha de protocolos, advém do nome de seus dois principais protocolos: Protocolo de Controle de Transmissão do inglês Transmission Control Protocol (TCP) na camada de transporte e Protocolo de Interconexão do inglês Internet Protocol (IP) na camada de rede (TEIXEIRA JÚNIOR et al, 1999).

A arquitetura TCP/IP esta organizado em quatro camadas conceituais: Camada de Aplicação onde contém os dados do usuário (mensagens ou *streams*), Camada de Transporte contém os pacotes de protocolos de transporte, Camada da Internet contém Datagramas IP, Interface de rede que envia e recebe os quadros de redes específicas e a Camada de Hardware (COMER, 1999).

O TCP/IP foi desenhado segundo uma arquitetura de pilha, onde diversas camadas

de software interagem somente com as camadas acima e abaixo. Há diversas semelhanças com o modelo conceitual OSI da ISO, mas o TCP/IP é anterior à formalização deste modelo e, portanto possui algumas diferenças (LOZANO, 1998).

Segundo Lozano (1998), o nome TCP/IP vem dos nomes dos protocolos mais utilizados desta pilha, o IP e o TCP. Mas a pilha TCP/IP possui ainda muitos outros protocolos, vários deles necessários para que o TCP e o IP desempenhem corretamente as suas funções.

Na Figura seguinte pode-se comparar as camadas dos protocolos OSI com as camadas dos protocolos TCP/IP.

Figura 3. Modelo OSI comparado com Modelo TCP/IP
Fonte: OLONCA, R. (2007)

Primeira camada a Física cuida da comunicação com o meio físico da rede, como placas e cabos.

Na segunda camada Rede, nessa cuida da identificação da máquina na Internet, ou numa rede.

Terceira camada de Serviços é responsável de identificar a aplicação dentro da máquina. Na transmissão de dados, a camada de transporte é responsável por pegar os dados

passados pela camada de aplicação e transformá-los em pacotes.

Quarta camada de Aplicação rodam os aplicativos. Esta camada faz a comunicação entre os programas e os protocolos de transporte. Existem vários protocolos que operam na camada de aplicação.

Desde a década de 1980, vários grupos têm trabalhado para definir arquiteturas padronizadas (e abertas) para o gerenciamento de redes heterogêneas, ou seja, redes compostas por equipamentos de diferentes fabricantes (PINHEIROS, 2002).

As principais arquiteturas abertas de gerenciamento de redes são relacionadas às tecnologias TCP/IP e OSI da ISO e estas são conhecidas mais facilmente pelos nomes dos protocolos de gerenciamento utilizados: Protocolo Simples de Gerência de Rede do inglês Simple Network Management Protocol (SNMP), do TCP/IP e o Protocolo de Gerência de Informações Comuns do inglês Common Management Information Protocol (CMIP), do modelo OSI. Muitos produtos de gerenciamento já foram desenvolvidos obedecendo estes padrões. Por razões históricas, os primeiros produtos seguiram o padrão SNMP e até hoje este é o protocolo que possui o maior número de implementações (SILVA, 2010).

3 GERÊNCIA DE REDE

A área de gerência de redes foi inicialmente impulsionada pela necessidade de monitoração e controle do universo de dispositivos que compõem as redes de comunicação. Atualmente as redes de computadores e os seus recursos associados têm assumido papel de grande importância para empresas, onde os níveis de falhas e de degradação de desempenho considerados aceitáveis estão diminuindo cada vez mais, dependendo do tipo de aplicação (STALLINGS, 1999).

Gerenciar o ambiente de rede é uma das preocupações mais constantes entre empresas e organizações. Dispor de ferramentas que façam esse controle é fundamental para facilitar o trabalho e identificar imediatamente algum tipo de erro providenciando assim uma ação efetiva (SILVA, 2007).

A gerência de uma rede pode não ser simples, dada sua heterogeneidade em termos de hardware, software e de componentes da rede, por vezes incompatíveis. As falhas intermitentes, se não forem detectadas, podem afetar o desempenho da rede. Um software de gerência de redes permite ao gestor monitorar e controlar os componentes da sua rede (COSTA, 2008).

Representada na Figura 4 uma arquitetura de rede básica com sistema de gerenciamento de rede aplicado. Cada nó da rede contém softwares dedicados à função de gerência de rede.

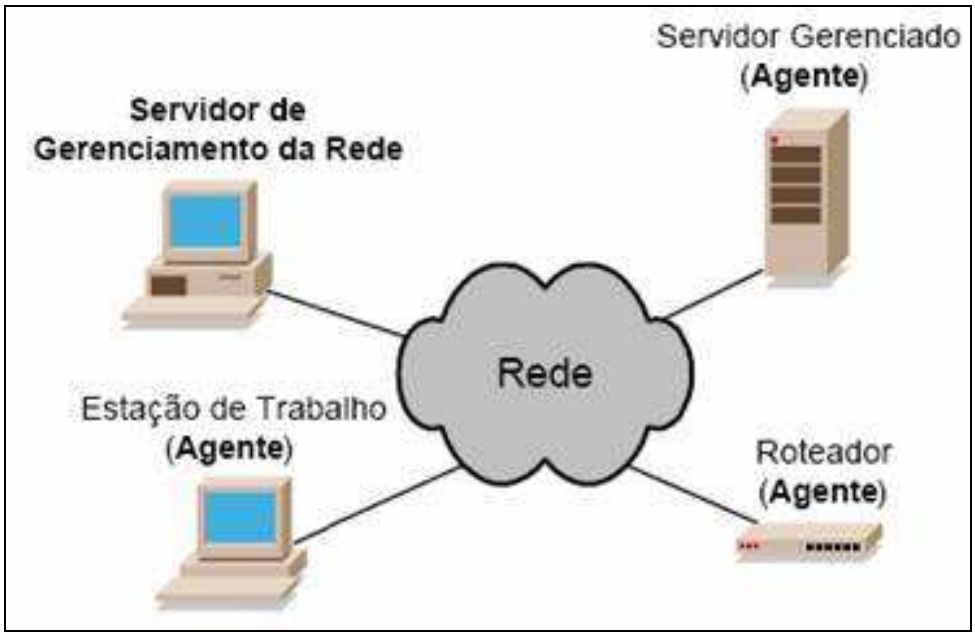


Figura 4. Modelo Sistema de Gerenciamento
Fonte: PINHEIROS, J. (2006)

Um dos aspectos destacados nesse tipo de solução é opção por controle por meio de gráficos e relatórios, além de alertas pelos quais o administrador pode ter a opção de ser avisado se acontecer qualquer instabilidade na rede. Proporcionando um acompanhamento em tempo real dos acontecimentos (SILVA, 2007).

O gerenciamento de rede pode ser definido como a coordenação (controle de atividades e monitoração de uso) de recursos materiais (modems, roteadores, etc.) e ou lógicos (protocolos), fisicamente distribuídos na rede, assegurando, na medida do possível, confiabilidade, tempos de resposta aceitáveis e segurança das informações (PINHEIROS, 2006).

Na Figura 5 pode ser observada uma estrutura de rede mais complexa do que vista na figura anterior.

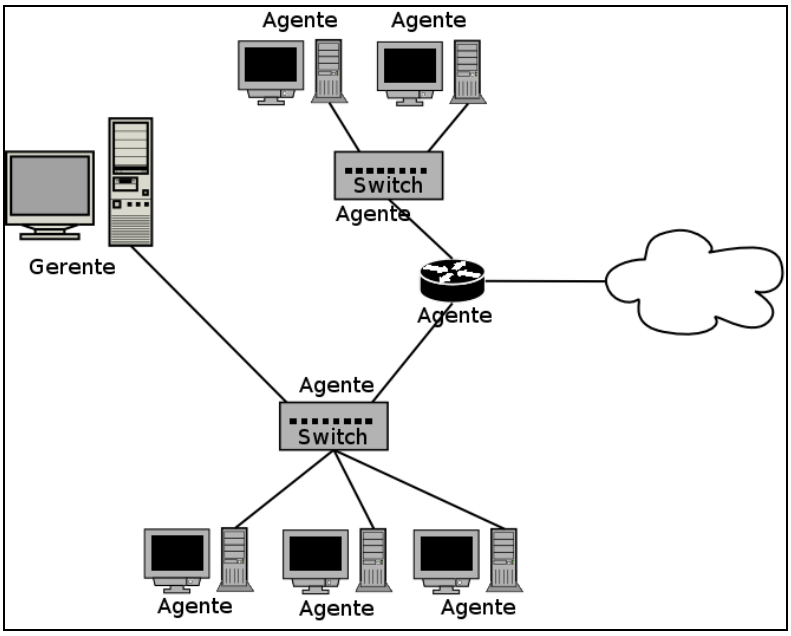


Figura 5. Exemplo de cenário de gerenciamento de rede
Fonte: MATOS, L. (2009)

O modelo clássico de gerenciamento pode ser sumarizado em três etapas:

Coleta de dados: um processo, em geral automático, que consiste de monitoração sobre os recursos gerenciados (PINHEIROS, 2006);

Diagnóstico: consiste no tratamento e análise realizados a partir dos dados coletados. O computador de gerenciamento executa uma série de procedimentos (por intermédio de um operador ou não) com o intuito de determinar a causa do problema representado no recurso gerenciado (PINHEIROS, 2006);

Ação ou controle: Uma vez diagnosticado o problema, cabe uma ação, ou controle, sobre o recurso, caso o evento não tenha sido passageiro (incidente operacional) (PINHEIROS, 2006).

O programa gerente de rede é a entidade responsável pelo monitoramento e controle dos sistemas de hardware e software que compõem a rede, e o seu trabalho consiste em detectar e corrigir problemas que causem ineficiência (ou impossibilidade) na comunicação e eliminar as condições que poderão levar a que o problema volte a surgir (COSTA, 2008).

3.1 GERÊNCIA DE FALHAS

Falhas não são o mesmo que erros. Uma falha é uma condição anormal cuja recuperação exige ação de gerenciamento. Uma falha normalmente é causada por operações incorretas ou um número excessivo de erros (SPECIALSKI, 2007).

Gerência de falhas tem como principais ações a identificação da falha, Isolar e corrigi-la. É uma das tarefas mais importantes para deixar uma rede com um bom nível de confiabilidade (SILVA, 2007).

É uma tarefa complexa, que necessita de ferramentas bastante escaláveis e de preferência que automatizem ao máximo o processo, desde a identificação até a correção de uma falha (SILVA, 2007).

3.2 GERÊNCIA DE DESEMPENHO

O gerenciamento do desempenho de uma rede consiste na monitoração das atividades da rede e no controle dos recursos por meio de ajustes e trocas (SPECIALSKI, 2007).

Muito importante para evitar o mau uso da rede e prover uma capacidade de planejamento. Gerenciar o desempenho dos recursos de uma rede é muito importante para identificar quais deles devem ser revistos a propósito de upgrades, ou mesmo de diminuição de custos (largura de banda desnecessária, por exemplo) (SILVA, 2007).

Segundo Comer (2001), o uso de software de gerência de rede é o mecanismo para que o administrador descubra problemas e isole sua causa. Esses tipos de softwares que são baseados principalmente no protocolo SNMP são capazes de monitorar o estado de serviços e equipamentos da rede.

3.3 SNMP

O protocolo SNMP é usado para transportar a informação de gerenciamento entre as estações de gerenciamento e os agentes existentes nos elementos de rede (SPECIALSKI, 2007).

É um protocolo de gerência típica de redes TCP/IP, da camada de aplicação que facilita o intercâmbio de informação entre os dispositivos de rede. O SNMP possibilita aos administradores de rede gerenciar o desempenho da rede, encontrar e resolver problemas de rede, e planejar o crescimento desta (COSTA, 2008).

O SNMP apresenta quatro componentes que são: nós gerenciados (estações, roteadores, pontes, impressoras, http, smtp, etc), estações de gerenciamento, informações de gerenciamento, um protocolo de gerenciamento (SANTOS, 2011).

O gerenciamento é feito por meio de estações gerentes com um software especial. Estas estações possuem processos que se comunicam com os agentes emitindo comandos e obtendo respostas (TANENBAUM, 1997).

Os alertas do SNMP padrões notificam um problema somente quando ele já atingiu uma condição extrema suficiente, a ponto de comprometer a comunicação na rede como um todo. Já o diagnóstico do problema, é uma tarefa do administrador da rede. Assim, o SNMP é simplesmente um alerta para uma condição extrema da rede (SANTOS, 2011).

Várias são as informações passíveis de obtenção por meio do relacionamento agente-gerente SNMP, como taxas de erros, status de operação de interfaces e equipamentos, taxas de utilização de interfaces, protocolos em operação e inúmeras outras. Estas informações são preciosas na atividade de gerenciamento, porém, apenas são úteis para quem sabe interpretá-las (OLIVEIRA, 2007).

3.3.1 Aplicações SNMP

As implementações básicas do SNMP permitem ao gerente monitorar e isolar falhas, já as aplicações mais sofisticadas permitem gerenciar o desempenho e a configuração da rede. Estas aplicações, normalmente, incorporam menus e alarmes para melhorar a interação com o profissional de gerência (SILVA, 2005).

Vários produtos têm surgido com a finalidade de gerenciar a rede, quase que em sua totalidade baseados no padrão SNMP e CMIP. O sucesso do SNMP se deve ao fato de ele ter sido o primeiro protocolo de gerenciamento acessível ao público, não proprietário e simples em sua implementação, o que possibilita o gerenciamento efetivo de ambientes com características não similares (SANTOS, 2011).

4 FERRAMENTA DE MONITORAÇÃO

O mercado atualmente disponibiliza inúmeras soluções para ajudar os administradores de redes a garantir o bom funcionamento das mesmas. Por esse motivo, faz-se necessário o estudo detalhado de softwares que incorporem funcionalidades que sejam fundamentais para um gerenciamento de confiança, seguro e eficiente na organização (SANTOS, 2011).

O gerenciamento de rede depende diretamente de ferramentas que possam prover a gerência, implementando o modelo de gerenciamento escolhido. São muitos os softwares livres que auxiliam nesta tarefa (OLIVEIRA, 2009).

Estão sendo utilizada uma série de programas para ter sucesso no gerenciamento de rede. Um dos sistemas de monitoramento é composto pelo Nagios e Cacti, além de vários softwares de segurança que podem ser implantados.

O monitoramento de rede e sistemas proporcionado por esta aplicação permite a verificação de equipamentos e serviços desejados, e gerar alarmes quando necessário, possibilitando definir tratadores de eventos durante o gerenciamento, o que possibilita um gerenciamento preventivo ou reativo (reativo e pró-ativo).

As detecções preventivas são aquelas que têm por objetivo evitar que o problema aconteça avisando o responsável pela rede quando algo esta preste a acontecer (OLIVEIRA, 2009).

Já as detecções reativas têm por objetivo informar que o problema está acontecendo. Indisponibilidade de comunicação e serviços são exemplos que caracterizam esta situação. Quando apresentar uma ocorrência desse tipo o responsável pela rede tem de buscar a solução no menor tempo possível, pois em geral essa situação implica em prejuízo para a empresa (OLIVEIRA, 2009).

A principal utilização do Nagios e seus *plugins* são para evitar problemas de rede por meio de monitoramento, assim evitando que algum equipamento ou toda a estrutura fique parado por minutos, horas ou até mesmo dias, já que qualquer equipamento não garante 100% (confiabilidade).

Deste modo os responsáveis pela rede terão possibilidade de atuar instantaneamente na solução dos problemas ocorridos na infraestrutura, bem como, disponibilidade de informações relativamente importantes que podem contribuir para evitar a interrupção de seus serviços de rede.

4.1 CACTI

O Cacti é uma ferramenta que recolhe e exibe informações sobre o estado de uma rede de computadores por meio de gráficos. Foi desenvolvido para ser flexível de modo a se adaptar facilmente a diversas necessidades, bem como ser robusto e fácil de usar. Monitora o estado de elementos de rede, de programas, a largura de banda utilizada e o uso da CPU (COSTA, 2008).

É uma ferramenta para gerar gráficos de desempenho. O programa funciona em cima de uma plataforma SNMP, que é um protocolo de gerenciamento. Ou seja, depois de configurado, o Cacti gerencia vários dados que o SNMP fornece, como: espaço em disco, utilização da CPU, tráfego de rede, entre outros (MATOS, 2009).

O programa gera gráfico em tempo real o que possibilita uma ação imediata perante qualquer alteração, parecido com o Nagios, o software permite por meio da configuração de *plugins* a configuração de mensagens de alertas para um melhor gerenciamento e controle das ações.

Cacti é apenas uma interface de gerenciamento. Para que seja possível o

monitoramento por meio de gráficos e visões é necessária à utilização de outra ferramenta de captura de dados, como por exemplo, o RRDTool, MRTG ou Nagios (MAJEWSKI, 2009)

4.2 NAGIOS

O Nagios é uma aplicação de código aberto desenvolvido para monitoramento de rede. Segundo Costa (2008), o Nagios foi originalmente criado sob o nome de *Netsaint*, foi escrito e é atualmente mantido por Ethan Galstad, junto com um exército de desenvolvedores que ativamente mantém *plugins* oficiais e não oficiais.

Inicialmente o Nagios foi projetado para redes de grande porte, mas seu desempenho em pequenos ambientes é excelente. Isso se comprova seja alertando para quedas de serviços ou hosts vigiados nos arquivos de configuração, seja monitorando equipamentos com suporte SNMP, este o principal agente entre o Nagios e seus hosts (ANDRADE, 2009).

Monitoramento de serviços de rede e recursos de hosts, como notificações quando apresentar problemas com serviços ou hosts e a interface web que facilita a análise do administrador podendo interpretar os dados por arquivos de logs, notificações e visualização do estado da rede, são algumas de suas principais características que tanto faz do Nagios mais respeitado e utilizado.

Com sua interface web, ele provê ao administrador uma grande variedade de informações, claramente organizadas de acordo com os assuntos envolvidos. Fornece uma página de informação individualmente estruturada caso este necessite de um resumo de toda a situação ou uma visualização de serviços problemáticos (ANDRADE, 2006).

O Nagios atua tanto na área de contabilização como no gerenciamento de falhas, verificando periodicamente o estado dos recursos monitorados, caso ocorra algum evento como uma falha, o mesmo envia um alerta ao responsável se algum valor passe do limite previamente definido pelo administrador em sua configuração. Um exemplo é que se definido

um valor máximo para utilização da memória em um servidor e esse valor ultrapassar, um alerta poderá ser enviado pelo Nagios ao responsável caso isso ocorra.

Diversas empresas utilizam o software livre Nagios nos mais diferentes segmentos que vai desde o controle de pontos de acesso, monitoramento de clientes à distância, conectividade de usuários ou servidores. Tudo vai da necessidade de cada empresa.

Serviços como HTTP, SMTP, POP3 e NNTP se definido pelo administrador de rede no Nagios são programados o monitoramento a fim de evitar o comprometimento desses serviços e de atividades essenciais à empresa. Esses serviços, no caso de imprevistos devem ficar o menor tempo possível fora de funcionamento.

Os serviços de checagem no Nagios são exercidos por *plugins* no formato CGI. Estes CGIs são armazenados em uma pasta e carregados pelo navegador, quando solicitado (ANDRADE, 2006).

Monitoramento de máquinas clientes pode ser realizado com a utilização de hosts específicos, com o objetivo de ter em tempo real, estatísticas ou monitoramento total de seus hardwares. Se destaca dentre esses recursos monitorados o monitoramento do uso do processador, uso da memória RAM, processos em execução e o espaço do disco rígido (HD).

O controle de ambientes por meio de sensores ligados em rede que possuem IP próprio permite que sejam coletados dados e com isso ter uma visão geral do ambiente monitorado. Muitas salas ou ambientes que necessitam desse controle como salas de servidores de uma empresa onde a temperatura e a humidade são controlada, o Nagios pode monitorar e ao encontrar alguma anomalia informará ao administrador o problema como programado.

Notificação ao administrador ou um grupo de contatos cadastrado é uma opção oferecida pelo Nagios em caso de ocorrência (falha ou irregularidade). Também pode ser configurado para reagir e solucionar alguns tipos de ocorrências sem deixar de informar ao

administrador o ocorrido.

Verificação de hosts é executada apenas quando necessário, mas uma verificação continua não é aconselhável, pois interfere no desempenho do Nagios mesmo tendo parâmetros que podem ser configurados para forçar a verificação continua de alguns hosts se necessário.

Os serviços são verificados pelo Nagios por meio de programas externos, os *plugins*, que são previamente configurados no computador. Para verificação de algo como utilização da memória RAM é necessário iniciar um *plugin* num host por meio de um *Shell* remoto, ou utilizar de outros métodos como o SNMP para verificar a memória RAM.

Os métodos de verificação de serviços podem ser feita de forma passiva onde o Nagios recebe apenas as informações enviadas pelo cliente por meio do programa Nagios *Service Check Acceptor* (NSCA). Outro método de verificação onde o Nagios envia comandos para testes é a verificação de forma ativa dos serviços. Este por sua vez pode executar *plugins* tanto local como remotamente utilizando o serviço Nagios *Remote Plugins Executer* (NRPE) ou consultar por meio do protocolo SNMP.

5 TRABALHOS CORRELATOS

Esta seção relaciona alguns dos trabalhos científicos com teor semelhante a esta fundamentação teórica utilizados no desenvolvimento deste projeto de pesquisa.

5.1 NAGIOS COMO SOLUÇÃO DE MONITORAMENTO DE REDE

Trabalho de Conclusão de Curso de Hetty Alves de Andrade, para obtenção do grau de Pós-Graduação Lato Sensu em Administração de Redes Linux e a obtenção do título de especialista em Administração de Redes Linux, em 2006, pela Universidade Federal de Lavras no estado de Minas Gerais.

O trabalho desenvolve um estudo do software livre Nagios, aplicativo que essencialmente monitora ativos e serviços de rede. Demonstrando seus recursos de forma prática, buscando auxiliar o administrador de rede no processo de configuração para a utilização desta ferramenta.

5.2 GERENCIAMENTO DE REDES COM A UTILIZAÇÃO DE SOFTWARE LIVRE

Artigo escrito por Cinthia Cardoso dos Santos, pelo Curso de Sistemas de Informação do Instituto de Estudos Superiores da Amazônia (IESAM) no estado do Pará.

O artigo tem como objetivo apresentação de ações e vantagens que o gerenciamento de redes deve ter para garantir aos seus usuários, a disponibilidade dos serviços locais.

5.3 INTEGRAÇÃO DAS FERRAMENTAS NAGIOS E CACTI COMO SOLUÇÃO DE MONITORAMENTO DE RECURSOS COMPUTACIONAIS EM REDES

Trabalho de Conclusão de Curso de Rômulo Alceu Rodrigues, como parte dos requisitos para a obtenção do Certificado de Conclusão de Curso da Graduação em Tecnologia em Informática com ênfase em redes de computadores, em 2010, pela Faculdade de Tecnologia Prof. Waldomiro May no estado de São Paulo.

Este trabalho trata da integração dos softwares Nagios e Cacti, uma combinação que oferece alto desempenho e baixo custo para a empresa, além de serem classificadas entre as melhores ferramentas de monitoramento do mercado.

5.4 UMA PROPOSTA DE SOLUÇÃO DE GERENCIAMENTO DE CONTABILIZAÇÃO UTILIZANDO NAGIOS E CACTI

Trabalho de Conclusão de Curso de Moisés Koch, como requisito parcial para a obtenção do grau de Especialista do Curso de Especialização em Tecnologias, Gerencia e Segurança de Redes de Computadores, em 2008, pela Universidade Federal do Rio Grande do Sul no estado do Rio Grande do Sul.

Este trabalho apresenta uma proposta de solução de gerenciamento para uma rede local de computadores, a partir do gerenciamento de contabilização. Depois de fazer uma breve revisão dos principais tópicos de gerência de redes, o trabalho concentra-se em gerenciamento de contabilização, descrevendo os princípios desta área funcional do gerenciamento e ferramentas. Além disso, também apresenta um estudo de caso com a utilização das ferramentas Nagios e Cacti, bem como uma análise dos resultados obtidos.

6 IMPLANTAÇÃO DA FERRAMENTA DE MONITORAÇÃO DE REDE NAGIOS E SOFTWARES DE APOIO CACTI

6.1 DESCRIÇÃO DO AMBIENTE A SER GERENCIADO

Este estudo tem como escopo a rede de computadores composta por dois computadores interligados via LAN 10/100 Mbps, contendo três máquinas virtuais executando nesses dois computadores. A rede provê serviços de e-mail, internet, entre outros. Todos os equipamentos estão configurados e executando sobre o protocolo TCP/IP.

O ambiente foi configurado para dar totais condições aos testes como se estivesse em uma rede corporativa padrão com todos os recursos e serviços básicos necessários.

6.2 SISTEMAS OPERACIONAIS

Servidores das máquinas virtuais estão com o sistema operacional GNU/Linux Debian 6.0 e os computadores estão com o sistema operacional MS Windows 7.

Na Figura 6 a seguir é possível observar a estrutura de rede a ser gerenciada.

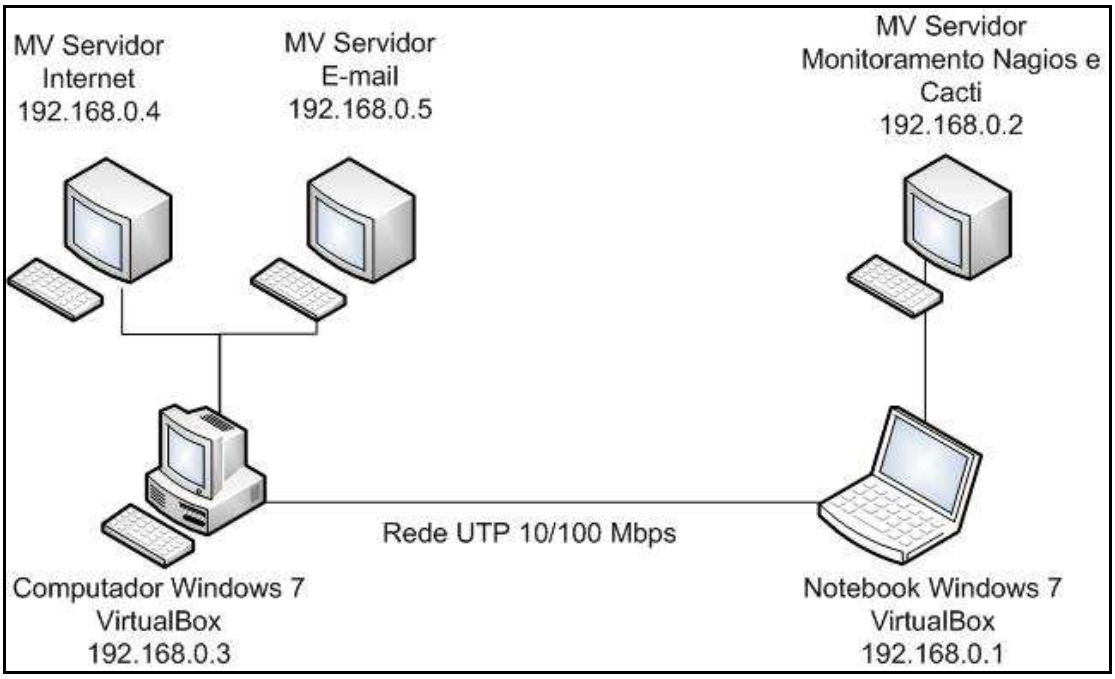


Figura 6. Estrutura de rede gerenciada

6.3 ESTADO ATUAL DOS SERVIÇOS

Há diversos serviços em execução disponíveis numa rede corporativa para atender a demanda dos usuários. O acesso à internet e o serviço de e-mail são essenciais para o andamento da rotina dos usuários. Entretanto um monitoramento efetivo desses ou de outros serviços não são empregados, tampouco dos servidores em que estão instalados.

Ao ocorrer alguma falha deixando indisponível algum serviço, seja por que o servidor que fornece está apresentando problemas ou o serviço parou ficando indisponível, o mais comum é o setor de tecnologia receber inúmeras ligações de usuários avisando que há algo de errado, ou o administrador se antecipa avisando os usuários da indisponibilidade do serviço e tomando medidas para retomar a rede ao seu estado normal.

Atualmente é difícil saber como os recursos da rede estão sendo consumidos, por ser no mínimo trabalhoso ou não ter as informações. O espaço em disco, por exemplo, é um recurso importante no caso dos servidores de ser verificados. Para obter está informação o administrador tem de acessar os servidores e verificar manualmente a quantidade de espaço livre em disco.

6.4 PROPOSTA DE SOLUÇÃO DE GERENCIAMENTO PARA AVALIAÇÃO

Esta proposta tem o objetivo de avaliar uma solução de gerenciamento de rede capaz de monitorar, notificar e contabilizar os recursos e serviços de rede ao administrador com rapidez e eficiência, quando um evento indesejado ocorrer.

Objetivo especifico do trabalho consiste em:

- Implantar as ferramentas de monitoramento Nagios e Cacti;
- monitorar os serviços e equipamentos de rede;
- simular eventos de erros relacionados ao funcionamento de serviços e equipamentos monitorados;
- enviar alertas aos administradores de rede sempre que um serviço ou equipamento estiver apresentando algum problema;
- visualizar os resultados do que está sendo monitorado;
- avaliar as ferramentas no monitoramento dos serviços e equipamentos.

6.5 IMPLANTAÇÃO DAS FERRAMENTAS DE MONITORAMENTO

O trabalho foi realizado a partir da instalação de um servidor com sistema operacional GNU/Linux Debian em uma máquina virtual o software utilizado na virtualização foi o VirtualBox. A implantação das ferramentas de monitoramento de rede Nagios e o Cacti foram instalados a partir dos passos descritos no Anexo A deste trabalho.

Com base no que foi escrito pelo autor Costa (2008) toda distribuição GNU/Linux vem por padrão com muitos drivers e serviços genéricos instalados por padrão ocasionando aumento na utilização da memória RAM ou de conter algum erro que possa comprometer a segurança do ambiente. Para evitar estes problemas é recomendado remover alguns serviços.

Ao finalizar a instalação do Debian no site do distribuidor recomenda-se atualizar

o sistema operacional, já que o projeto Debian está em constante atualização. Toda distribuição GNU/Linux possui seu próprio gerenciador de pacotes, nestes pacotes poderá ser instalado todas as dependências dos pacotes utilizados para esse Sistema Operacional.

A opção de utilizar um banco de dados garante o armazenamento das informações e processos futuros como atualizações além de facilitar o processo de transferência dos dados. Armazenar as informações no HD do servidor é possível, mas não é considerada uma prática segura, além de várias outras dificuldades que pode apresentar principalmente no caso de uma atualização do software ou troca de hardware. Neste caso foi utilizado o banco de dados MySQL para armazenar as informações e poder ter acesso nas demais aplicações que necessitam dos dados armazenados.

Além da instalação do banco de dados devem ser instalados outros aplicativos e serviços que são necessários para o funcionamento do Nagios e do Cacti. Para poder utilizar a interface Web é necessário a instalação do WebServer Apache e do PHP, assim após estar configurados pode-se obter os dados visualmente pela interface web.

Após a instalação das dependências, o Cacti é o próximo passo. Esta ferramenta vai ser utilizada para análise por meio dos gráficos, mesmo sabendo que é bem completa e com possibilidades de expansão por meio de *plugins*.

Para a monitoramento de qualquer equipamento deve ser verificado se o SNMP está corretamente instalado e configurado. Com esse processo concluído podem ser visualizados e analisados os dados capturados dos equipamentos desejados, dividindo em árvores os gráficos gerados pelo Cacti facilitando a observação caso tenha vários servidores e serviços monitorados.

O Nagios foi à última aplicação instalada e configurada, não só por sua complexidade e esforço para instalar e configurar adequadamente, mas por ser a principal ferramenta utilizada para monitorar os recursos e equipamentos. Colocar o Nagios executando

e funcionando requer muito mais tempo e com base na experiência das instalações anteriores, ajudará a ter um entendimento do ambiente de monitoramento de uma rede.

Por último foi simulado eventos com o objetivo de demonstrar o funcionamento de toda a estrutura de monitoramento da rede e a capacidade de fornecer soluções, contabilizar a utilização dos recursos, monitorar e notificar aos administradores quando ocorrer algum evento indesejado.

6.5.1 Configuração das ferramentas Nagios e Cacti

O Nagios foi configurado para alertar ao administrador sempre que um serviço não estiver respondendo ou um host perder a conectividade, alterando a cor facilitando a identificação do problema agilizando a ação do administrador.

Na Figura 7 é possível verificar o Nagios em sua relação de servidores e serviços monitorados e suas sinalizações por meio das cores.

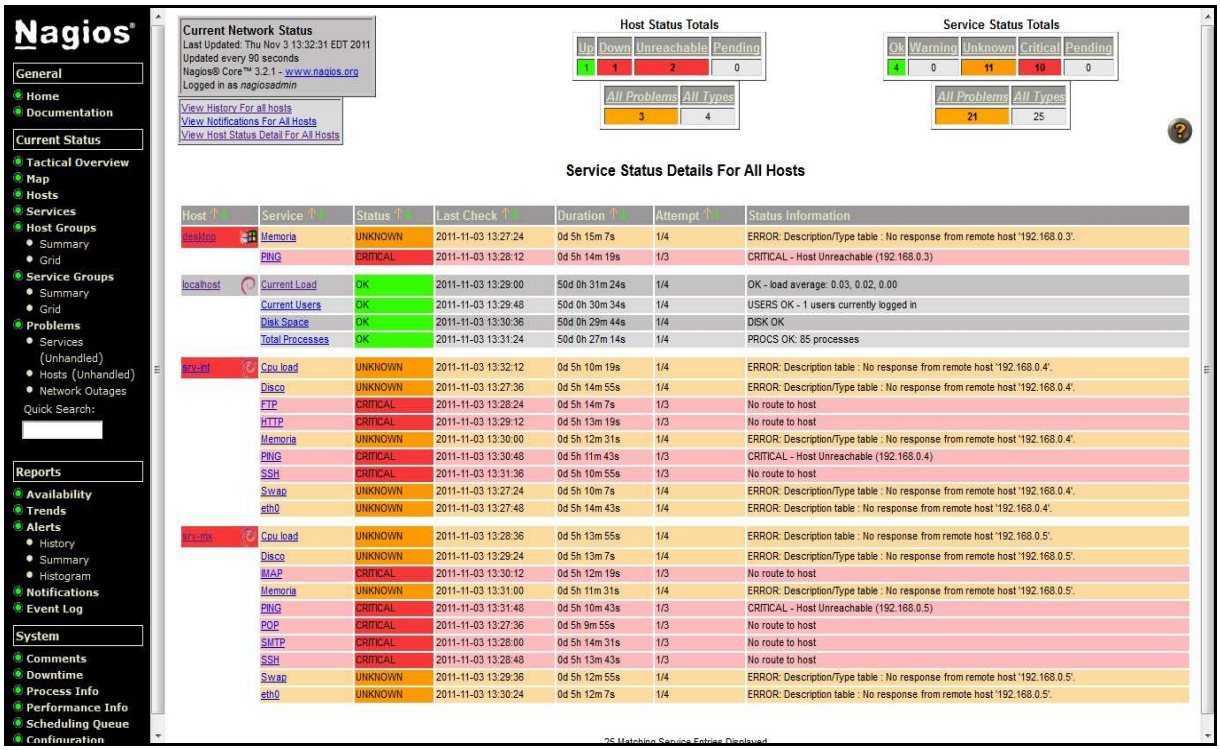


Figura 7 - Nagios, relação dos servidores e serviços monitorados.

Como parte na solução de monitoramento de rede o Cacti fica como principal método para levantamento de informações e demonstração dos dados por meio dos gráficos, demonstrando todo o histórico da utilização do serviço monitorado.

Estas informações possibilitam ao administrador verificar os pontos de maior e menor utilização de um determinado recurso, identificando problemas e podendo planejar manutenções ou investimentos para sanar o problema com maior segurança.

Na Figura 8 pode ser observado como os gráficos gerados podem auxiliar o administrador de rede na identificação de um possível problema.

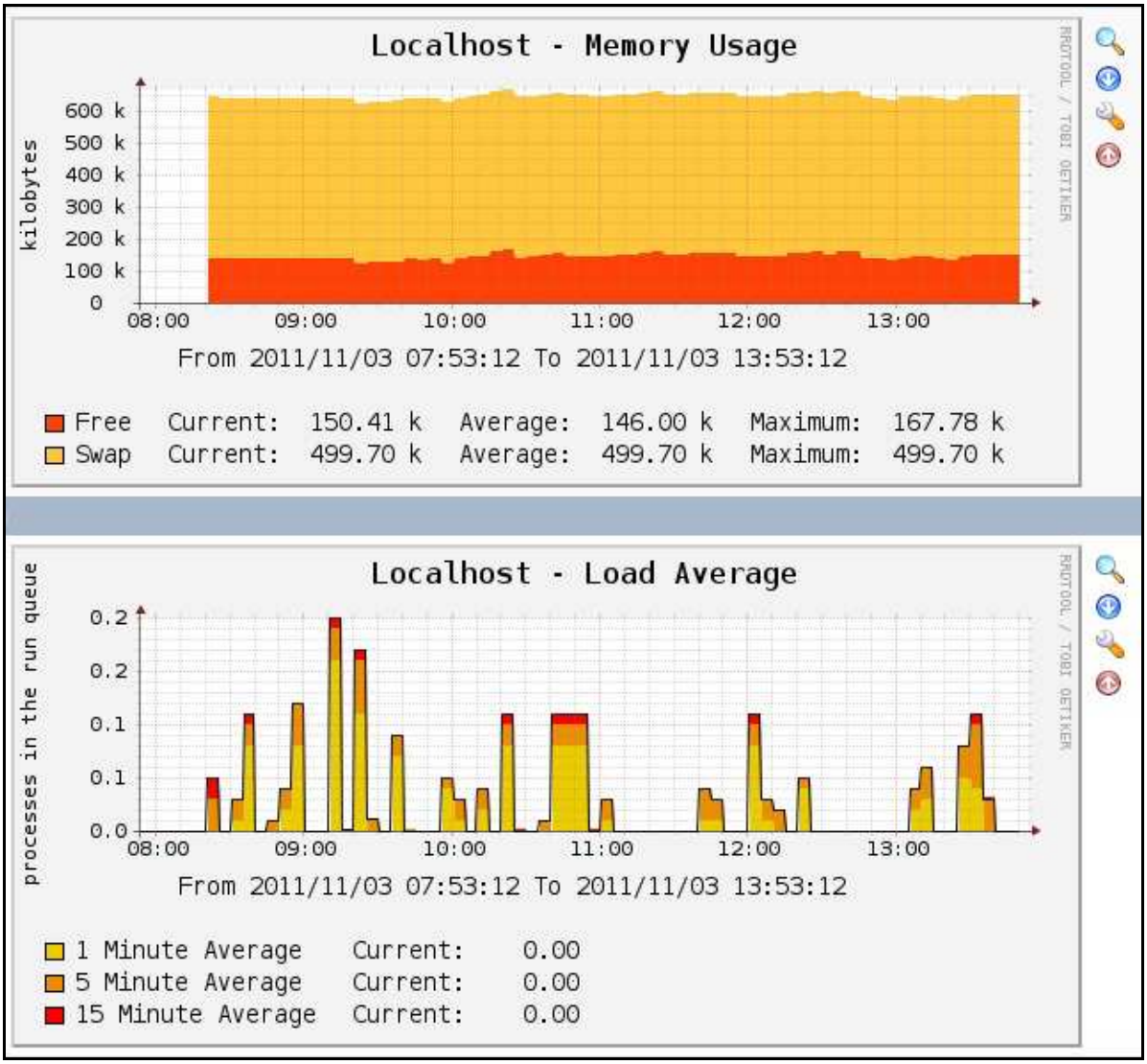


Figura 8 - Cacti, histórico de contabilização dos recursos

6.6 SIMULAÇÃO E TESTES

Os testes foram baseados na utilização da ferramenta para monitoramento de rede Nagios em conjunto com a ferramenta Cacti e alguns *plugins* que vão auxiliar na comunicação e captura dos dados.

Por meio de pesquisas na internet, livros, artigos e outros trabalhos sobre o tema, foi possível entender estas ferramentas de monitoramento de rede e sua forma de aplicar em um ambiente com estrutura complexa e obter os resultados levantados por essas ferramentas, permitindo que o administrador da rede possa avaliar e aplicar medidas contraceptivas as falhas levantadas.

O ambiente empregado as ferramentas conta com um computador com sistema operacional Microsoft Windows 7, com duas máquinas virtuais. Estes três sistemas estão sendo monitorados, além de um notebook com sistema operacional Microsoft Windows 7 e uma máquina virtual que vai ser o servidor de monitoramento.

Em uma das máquinas virtuais do computador foi instalado o sistema operacional GNU/Linux Debian como servidor de internet. Como principais serviços monitorados deste servidor estão: HTTP, FTP, SSH, CPU, HD, Memória, Swap e rede.

Na outra máquina virtual desse computador também foi instalado o sistema operacional GNU/Linux Debian como servidor de E-mail. Este servidor foi configurado para monitoramento os seguintes serviços: POP, IMAP, SMTP, SSH, CPU, HD, Memória, Swap e rede.

A máquina virtual que se encontra instalada no notebook é o servidor de monitoramento da rede onde foram instaladas e configuradas as ferramentas Nagios e Cacti. Este servidor roda sobre a plataforma GNU/Linux Debian.

Com a estrutura montada, conforme mostra a Figura 6, foi possível realizar diversos testes como simulações de eventos de erros pra isso foram criados os scripts nos

servidores de internet e E-mail, que força a parada de serviços e pode aplicar o teste de estresse de CPU, assim podendo obter dados e verificar se o monitoramento está sendo realizado de maneira satisfatória, analisando como funciona o Nagios sem interferir no ambiente da empresa e evitando comprometer serviços importantes.

Tendo o ambiente montado e configurado, foi definido que para realizar os testes seria necessário um gatilho, onde o responsável possa forçar uma situação adversa, gerando uma mensagem de alerta dos serviços monitorados.

Foi criado um script, que de forma prática possa aplicar um comando que desative ou ative um determinado serviço, como pode ser observado na Figura 9, ao rodar o script vai aparecer o menu onde contém os comandos para os testes em alguns serviços. Estes comandos são por meio de números, por exemplo, no servidor de e-mail srv-mx tem no script a opção 1 para parar e 2 para iniciar o serviço do servidor POP/IMAP.

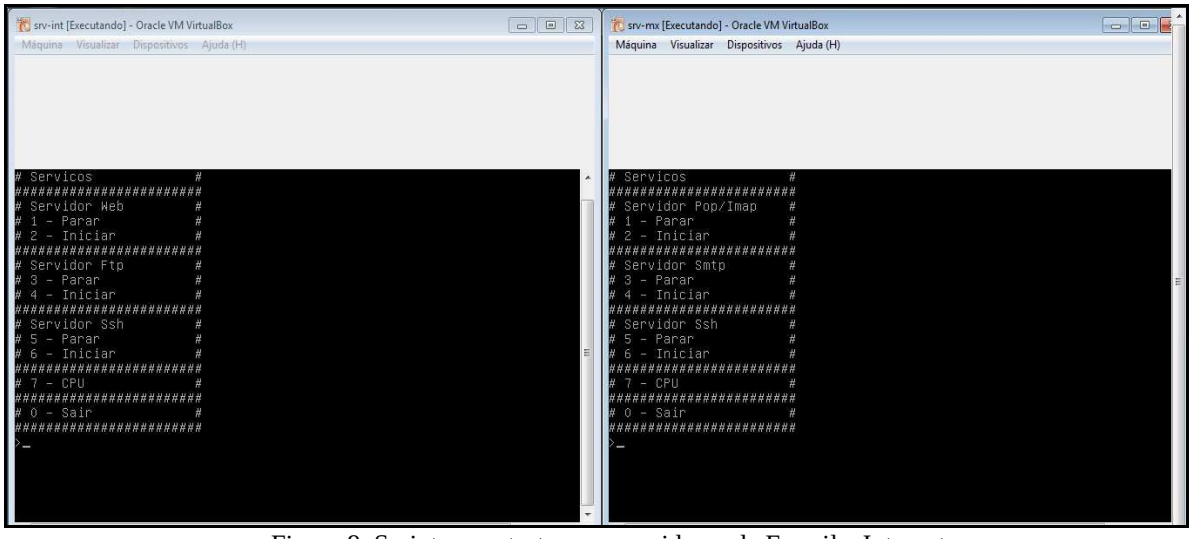


Figura 9. Scripts para testes nos servidores de E-mail e Internet

Com o Nagios já configurado e funcionando, pode ser acessada sua interface web e observar os hosts monitorados. A Figura 10 mostra a página principal do Nagios que contém as informações principais da ferramenta na parte central e na esquerda o menu onde se encontra os diversos tipos de interação e visualização dos hosts e seu estado.

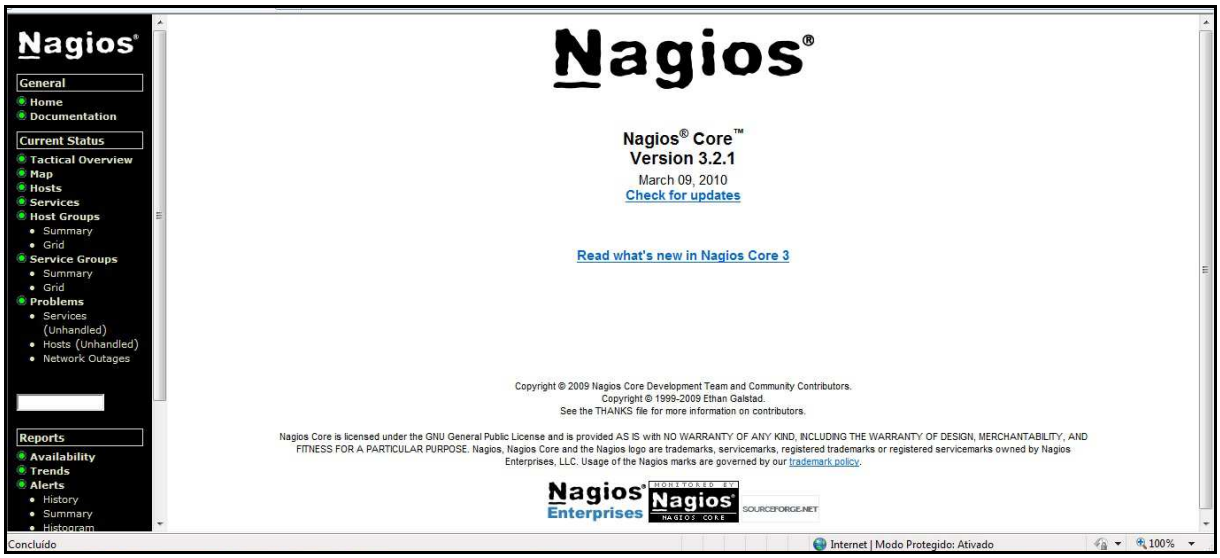


Figura 10. Nagios, interface web da tela principal

Ao executar o comando no script, que vai forçar a parada de um serviço monitorado, no menu do Nagios pode-se escolher várias formas de observar o local e o serviço que está ocorrendo o problema. Foi escolhido verificar pela opção Hosts do menu, onde é apresentado na Figura 11.

Nesta opção ficam visíveis todos os computadores monitorados e seus status. O Nagios trabalha com cores para demonstrar com está os serviços monitorados, verde para tudo certo, laranja com algum problema ou inconsistência e vermelho para serviço parado ou não respondendo.

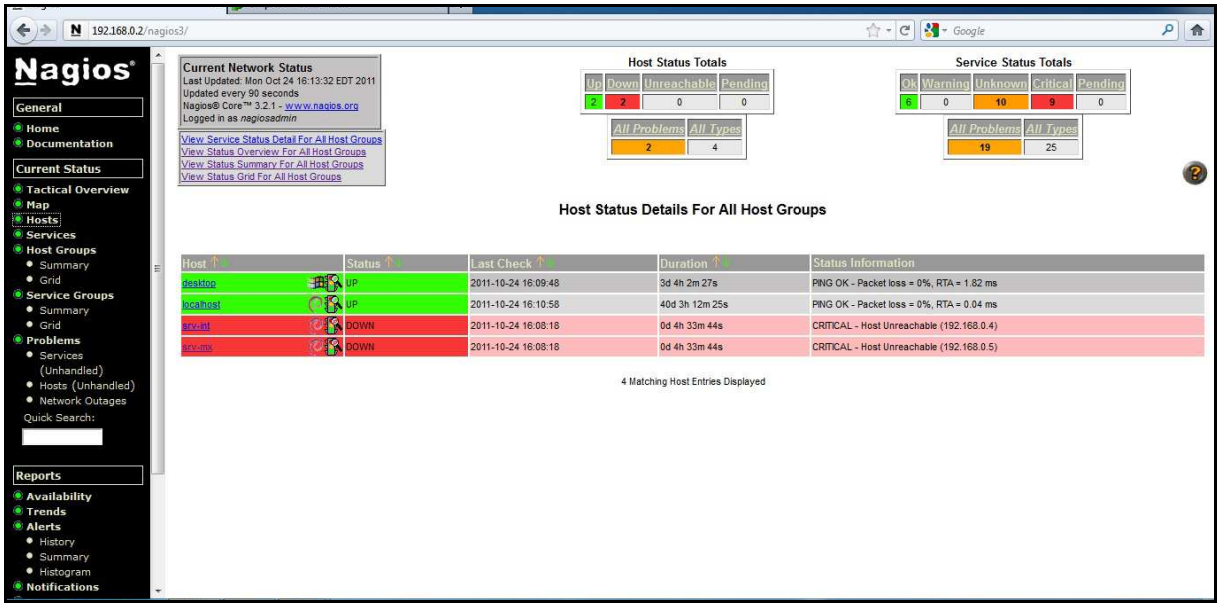


Figura 11. Nagios, página de monitoramento por Hosts

Através das simulações de eventos de erros, foi possível observar a eficiência da ferramenta de monitoramento o Nagios, mas só com ela o trabalho de análise para adotar medidas corretivas às falhas ocorridas não seria o ideal.

Com a implantação do Cacti, pode-se ter em gráficos uma visão real dos hosts e seus serviços que tem suporte a SNMP, como CPU, Memória, rede e etc. Essas informações são muito importantes para monitoramento de seus recursos e estudos do consumo destes recursos.

No Cacti em sua interface web, foi adicionado além do *localhost*, que por padrão já vêm configurado, os servidores Linux e os computadores Windows. Na Figura 13 pode ser observado a página principal do Cacti, que tem um menu há esquerda que pode ser alterado conforme a opção acima dele for escolhida, Console ou *Graphs*.

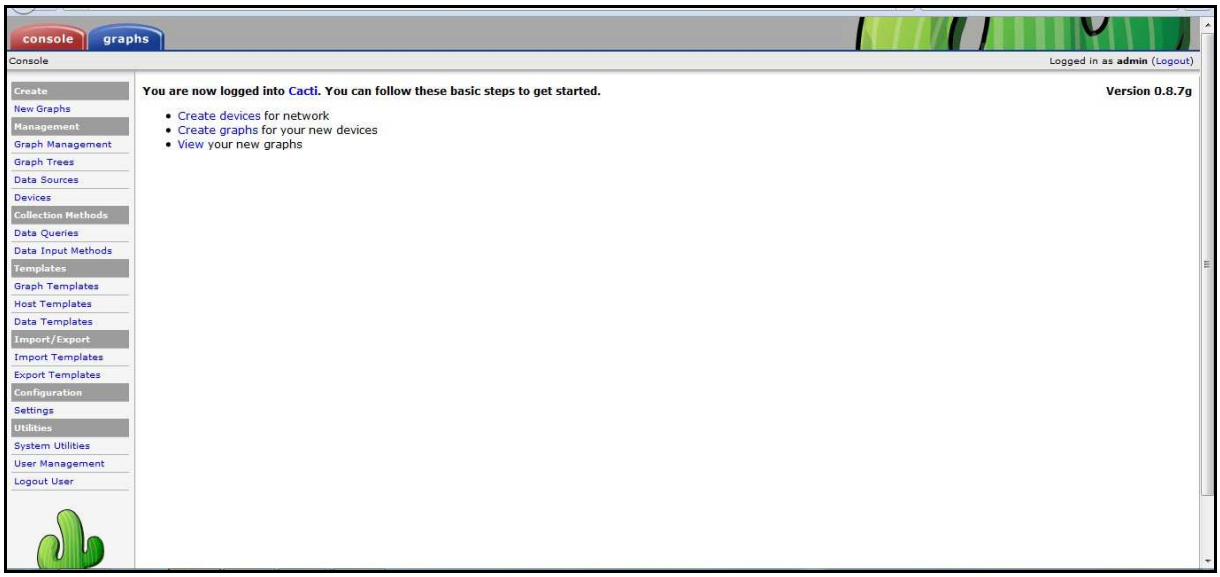


Figura 12. Cacti, interface web da página principal

Para o monitoramento é utilizado o menu *Graphs*, pois o menu Console é a parte de configuração do Cacti. O *Graphs* é a parte onde é possível observar os gráficos dos hosts monitorados e as árvores criadas para organizar o ambiente monitorado.

Foram criadas duas árvores no Cacti, a árvore srv-linux onde estão configurados

os servidores GNU/Linux que estão sendo monitorados e a árvore srv-windows que contém os computadores Microsoft Windows monitorados. Na Figura 13 abaixo pode ser observado melhor essa organização em árvores.

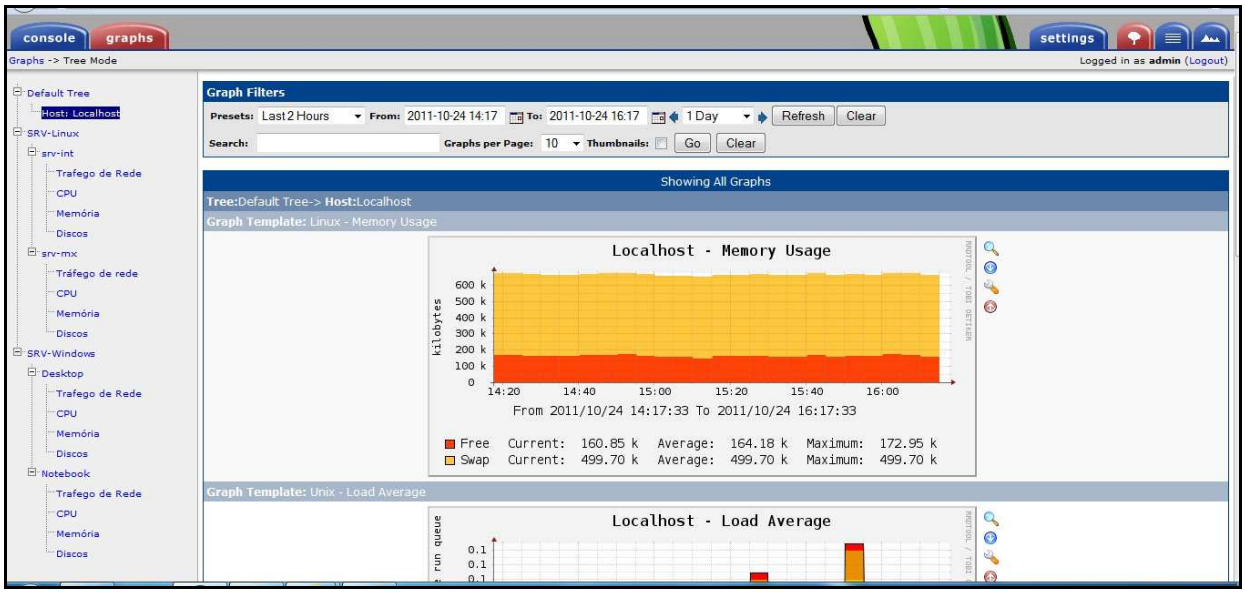


Figura 13. Cacti, ambiente organizado por árvores

Com o Nagios e o Cacti configurados e obtendo os dados, o administrador pode analisar e fazer estudos das áreas críticas ou que possam apresentar problemas futuros. Foi observado neste trabalho que com o auxílio do Cacti alguns aspectos que no modo tradicional o administrador poderia exigir muito tempo só para análise e comparação, o Cacti trouxe em pouco tempo todos os dados necessários.

Ficou clara esta vantagem nos testes realizados no servidor de e-mail srv-mx, quando foi retirada parte de sua capacidade de memória RAM demonstrando pelos gráficos esse recurso sempre no limite. Este tipo de informação é muito importante para o administrador por dar tempo para programar uma manutenção preventiva e verificar se algum recurso ou serviço possa estar consumindo todo o recurso.

Na Figura 14 a seguir é observado o gráfico que demonstra o problema relatado. Na imagem do gráfico srv-mx – Usade Space – Phisical Memory, o recurso utilizado está

próximo do limite podendo ocorrer algumas falhas paralisando os serviços ou o próprio computador.

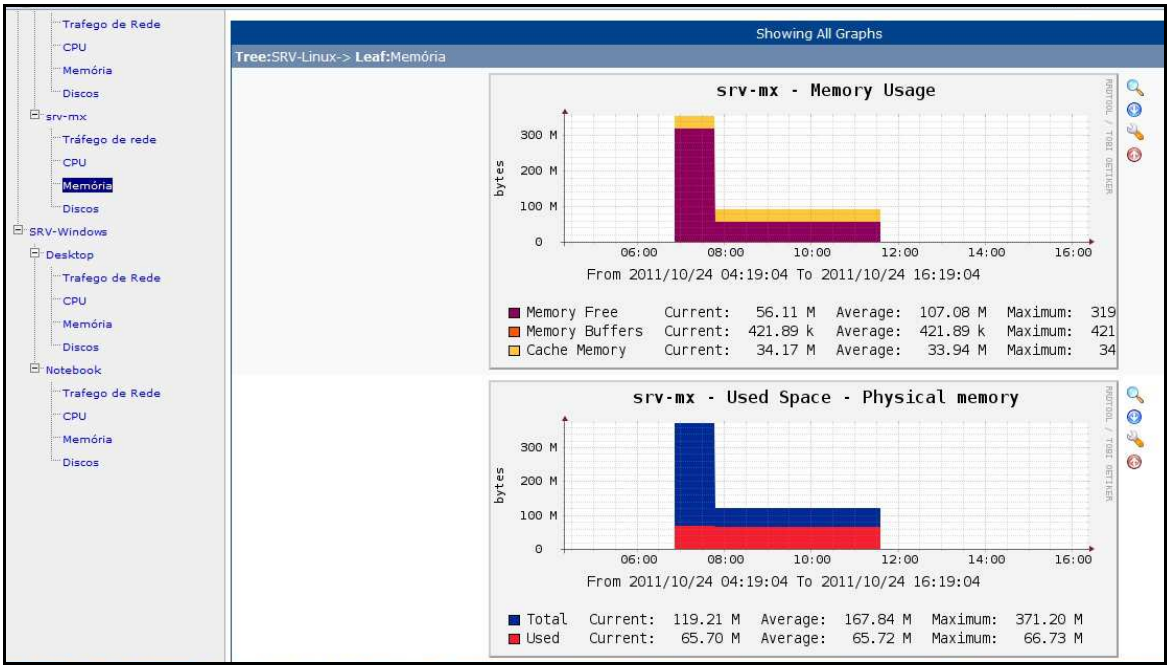


Figura 14. Cacti, gráfico monitoramento da memória RAM do servidor srv-mx

Cada administrador e empresa têm suas rotinas e prioridades, as medidas adotadas nesse trabalho podem não ser as mais adequadas para outro local. Com base nesses testes, foi possível demonstrar um pouco das possibilidades destas ferramentas de monitoramento podem proporcionar.

Além do monitoramento gráfico do Cacti, a fim de evitar situações críticas, pode agilizar o atendimento, mesmo antes dos usuários perceberem o problema e sanar as falhas ocorridas de algum equipamento ou serviço o mais rápido possível. Por isso foram adotadas algumas medidas corretivas perante alguns casos levantados.

Neste trabalho o monitoramento pela interface web do Nagios em um monitor próprio para o serviço, é uma das principais maneiras utilizadas para acompanhamento das ações e eventos da infraestrutura monitorada. Nesta interface web a opção hosts como definida como padrão para análise, com todos os *hosts* configurados aparecendo na tela

principal.

Qualquer erro fica visível na tela onde o administrador poderá verificar o erro e tomar as providências para estabelecer o mais rápido possível. Na Figura 15 pode-se observar a tela do Nagios na opção hosts com todos os servidores monitorados.

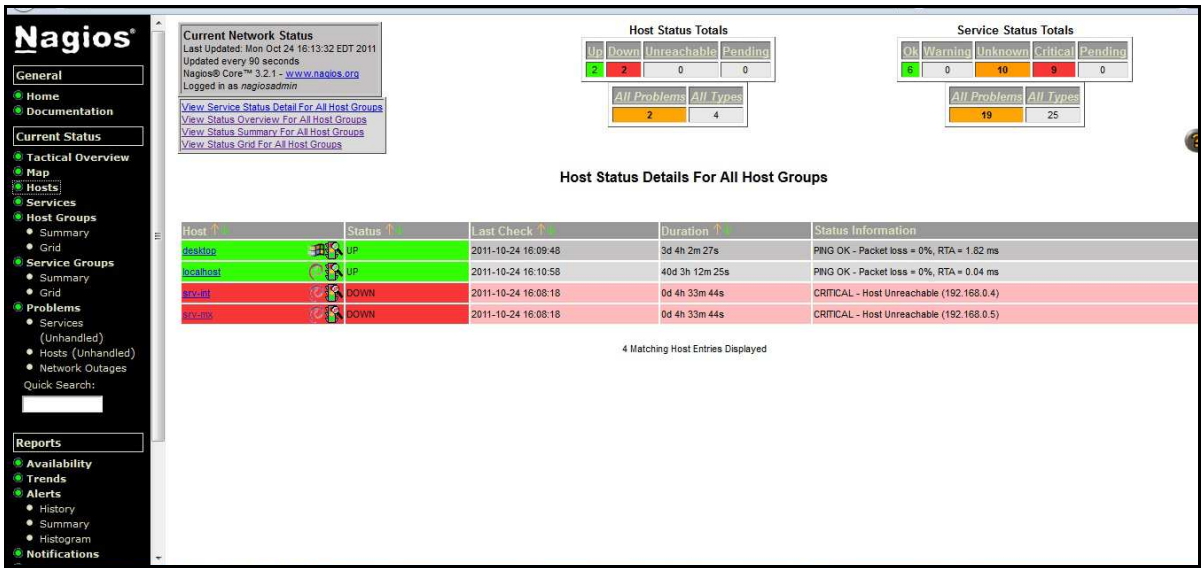


Figura 15. Nagios, tela dos Hosts monitorados

Esta é uma das diversas medidas que podem ser adotadas com a ferramenta Nagios. Outra medida muito utilizada é o envio de mensagem via e-mail. Esta medida é muito utilizada em monitoramento de equipamentos que ficam ligados 24 horas por dia, como servidores de e-mail e internet ou servidores de aplicativos sem uma equipe ou responsável no local para monitoramento desses recursos.

6.7 AVALIAÇÃO E RESULTADOS

Foram realizados diversos testes na estrutura monitorada para levantamento dos dados e poder avaliar as ferramentas de monitoramento Nagios e Cacti. Nos testes as ferramentas atenderam todos os requisitos esperado apresentando os dados e eventos

ocorridos para o administrador quase que instantaneamente.

Os testes foram realizados em serviços que estavam instalados, como também nos equipamentos. Muitos serviços como servidor web Apache foram parados e iniciados e em todos os casos foram notificados ao administrador visualmente pela interface web pelo Nagios.

Foi alterada a quantidade de memória RAM dos servidores localizados nas máquinas virtuais, e foi possível analisar a diferença nos gráficos pelo Cacti. Também foi utilizado o teste de estresse de CPU, que testa o processador ficando possível observar as variações pelos gráficos gerados pelo Cacti.

O ponto negativo é a complexidade na implantação da ferramenta Nagios, por exigir muito tempo e esforço em sua instalação e configuração. O Nagios para atender com eficiência um ambiente de rede complexo vai exigir muito estudo ou auxilio de pessoas especializadas, que possa aplicar todo o recurso oferecido pelo Nagios no monitoramento de rede.

A avaliação foi positiva da utilização das ferramentas no auxilio do monitoramento de rede. O emprego das ferramentas torna em geral a rotina complexa e de grande responsabilidade do administrador de rede mais simples, sem retirar a importância que o administrador vai ter em analisar e tomar as medidas corretas na prevenção e correção de possíveis ocorrências.

CONCLUSÃO

A implantação e configuração de ferramentas para monitoramento de redes se torna cada vez mais necessária. Com a redução de recursos humanos e a crescente complexidade das redes de computadores o monitoramento manual do sistema fica inviável.

As ferramentas de monitoramento para o administrador é a forma mais prática e eficiente de ter em mãos todas as informações necessárias para manter a estrutura funcionando e ser informado, o quanto antes, sobre problemas que estão ou vão ocorrer.

O Nagios por sua complexidade e robustez é uma das ferramentas de monitoramento de rede capaz de auxiliar o administrador de rede sobre os mais diversos problemas que possam ocorrer. O estudo desta ferramenta, aplicada ao ambiente para gestão e monitoramento da rede, permitiu a avaliação de diversos aspectos de seu funcionamento no monitoramento e gestão de redes de computadores.

Para poder contabilizar e ter maiores informações, foi instalado o software Cacti para o apoio e demonstrações via gráfico dos recursos utilizados, permitindo ao administrador analisar estas informações na manutenção de sua estrutura de rede monitorada.

A implantação destas ferramentas em uma estrutura de rede própria para realizar diversos testes e avaliar de forma eficiente a capacidade e todo o potencial do Nagios e do Cacti na pratica, sem ter de ficar esperando algum evento ocorrer em uma estrutura de rede da empresa. Como a ocorrência de certos eventos pode ser difícil de ocorrer ou imprevisível, numa estrutura montada para os testes é possível forçar diversos eventos e verificar em tempo real os efeitos do erro e as ações do Nagios em relação a essas inconsistências.

Todos os testes foram empregados em uma estrutura controlada, onde foi possível realizar diversos testes sem interferir no ambiente computacional da empresa, com isso as ferramentas foram bem avaliadas dando um resultado satisfatório para utilização no auxílio

dos administradores de rede.

Os resultados alcançados com a implantação das ferramentas de monitoramento de rede atingiram seu objetivo que é o suporte no monitoramento de ambientes complexos onde cada vez mais o numero de equipamentos eletrônicos cresce e sobrecarregando a equipe responsável.

Muitos outros serviços e equipamentos poderiam estar incluídos neste trabalho, mas para fim de testes e avaliação das ferramentas, o ambiente relacionado atingiu todos os requisitos e demonstrou como podem ser úteis estas duas ferramentas de monitoramentos trabalhando em conjunto no auxílio do administrador no monitoramento de ambientes de rede.

Certamente uma ferramenta de monitoramento de rede implantada como solução, não vai substituir o administrador de rede, está solução vai apenas facilitar e somar em suas atividades se tornando mais uma ferramenta para auxiliar na administração da rede.

As ferramentas para monitoramento de rede, cada vez mais se faz necessário, e com isso, muitas opções estão aparecendo e outras estão evoluindo, com o intuito de melhorar e facilitar o trabalho do administrador de rede. Hoje o Nagios é uma das ferramentas mais completas e robustas, mas existem outras ferramentas que podem ser tão boas quanto o Nagios, dependendo da necessidade do administrador e de sua estrutura de rede para poder testar e implantar a ferramenta ou as ferramentas no auxilio de seu trabalho, mantendo sua rede estável e confiável evitando problemas desagradáveis que possam afetar parte da empresa ou toda ela.

Outros estudos podem ser realizados comparando as ferramentas Cacti e Nagios utilizadas nesse estudo com outras ferramentas de monitoramento de rede, podendo diferenciar suas qualidades e dificuldades no auxilio ao administrador de rede em suas tarefas.

Com esse trabalho foi possível conhecer melhor sobre gerenciamento de rede por meio de ferramentas de monitoramento de rede. A utilização destes recursos se torna

fundamental no dia-a-dia do administrador de rede que com pouco investimento e pessoal poderá administrar sua estrutura de rede com segurança e agilidade na prevenção e resolução dos problemas.

REFERÊNCIAS

ANDRADE, Hetty Alves de. **Nagios como Solução de Monitoramento de Rede.** Disponível em: < http://www.ginux.ufla.br/files/mono-HettyAndrade.pdf/> Acesso em: 02 jun. 2011.

CANTÚ**,** Evandro. **Redes de Computadores e Internet** – CEFET/SC São José. 2003. Disponível em: <http://www.riopomba.ifsudestemg.edu.br/dcc/dcc/materiais/ 428029062_apostila-redes.pdf > Acesso em: 18 abr. 2011.

CARVALHO, João Antônio. **Internet - TCP/IP – Protocolo de Comunicação da Internet.** 2009. Disponível em: <http://www.algosobre.com.br/informatica/ internet-tcp-ip-protocolo-de-comunicacao-da-internet.html> Acesso em: 18 abr. 2011.

CARVALHO, João Antônio. **Redes de Computadores – Noções Básicas.** 2009. Disponível em: <http://www.algosobre.com.br/informatica/redes-de-computadores-nocoes-basicas.html> Acesso em: 18 abr. 2011.

COMER, Douglas E. **Redes de Computadores e Internet**. Porto Alegre: PERSON, 2ª ed., 2001.

COMER, Douglas E. **Redes de Computadores e Internet.** BOOKMAN, 4ª edição, 2007.

COMER, Douglas E. STEVENS, David L. **Interligação em rede com TCP/IP** vol 2. CAMPUS, 1999.

COSTA, Felipe. **Ambiente de Rede Monitorado com Nagios e Cacti.** Rio de Janeiro: MODERNA, 2008.

LOPES, Raquel T.; SUAVÉ, Jacques Philippe; Nicolletti, Pedro. S. **Melhores Práticas para Gerência de Redes de Computadores**. CAMPUS, 2003.

LOZANO, Fernando**. Arquitetura de Redes TCP/IP**. 1998. Disponível em: <http://www.clubedohardware.com.br/artigos/Arquitetura-de-Redes-TCP-IP/329/3> Acesso em: 01 mai. 2011.

MAJEWSKI, Roberto. **Sistemas de Monitoração de Rede.** 2009. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Roberto%20Majewski%20-%20Artigo.pdf >Acesso em: 01 jun. 2011.

MATOS, Leonardo Kolisnik de. **Gerenciamento de equipamentos de rede utilizando o software CACTI**. 2009. Disponível em: < http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Leonardo%20Kolisnik%20de%20Matos%20-%20Artigo.pdf> Acesso em: 23 mai 2011.

MENDES, Douglas Rocha. **Redes de Computadores – Teoria e Prática.** NOVATEC, 2007.

MENEZES, Elionildo da Silva. SILVA Pedro Luciano Leite. **Gerenciamento de Redes: Estudo de Protocolos.** UFP Pernambuco. 1998. Disponível em: <http://www.di.ufpe.br/~flash/ais98/gerrede/gerrede.html> Acesso em: 29 abr. 2011.

OLIVEIRA, Frederico S. Guimarães. **Gerenciamento de Redes de Computadores com o uso do Raciocínio Baseado em casos e Ferramentas Auxiliares.** 2007. Disponível em: <http://www.coc.ufrj.br/index.php?option=com_docman&task=doc_view&gid=1643> Acesso em: 25 mai. 2011.

OLIVEIRA, Jeferson Soares. MENEZES, Wagner Vidal. **Gerência de Rede com Suporte Baseado na Gestão do Conhecimento**. 2009. Disponível em: < http://monografias.cic.unb.br/dspace/bitstream/123456789/226/1/TCC_GRGC.pdf> Acesso em: 16 de nov. 2011.

OLONCA, Ricardo Lino. **Entendendo o TCP/IP.** 2007. Disponível em: <http://www.vivaolinux.com.br/artigo/Entendendo-o-TCP-IP?pagina=3> Acesso em: 01 mai. 2011.

PINHEIROS, José Mauricio Santos. **Gerenciamento de Redes de Computadores.** 2002. Disponível em: < http://www.allnetcom.com.br/upload/GerenciamentodeRedes.pdf> Acesso em: 16 nov. 2011.

PINHEIROS, José Mauricio Santos. **Gerenciamento de Redes de Computadores: Uma Breve Introdução.** 2006. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_gerenciamento_de_redes_de_computadores.php> Acesso em: 29 abr. 2011.

SANTOS, Cinthia Cardoso dos. **Gerenciamento de Redes com a Utilização de Software**

Livre. Disponível em: <http://www3.iesam-pa.edu.br/ojs/index.php/sistemas/article/viewFile/442/374 > Acesso em: 25 mai 2011.

SILVA, José Messias Alves da. **Construção de Agentes SNMP em Ambientes Linux.** 2005. Disponível em: < http://www.ginux.ufla.br/files/mono-JoseSilva.pdf> Acesso em: 25 mai. 2011.

SILVA, Ronaldo. **Gerenciamentos de redes de Computadores.** 2010. Disponível em: <http://www.rdsinfor.com.br/gerenciamento-de-redes-de-computadores/> Acesso em: 09 mai. 2011.

SPECIALSKI, Elizabeth Sueli. **Gerência de Redes de Computadores e de Telecomunicações.** 2007. Disponível em: <http://cassio.orgfree.com/disciplinas/gredes/ApostilaGerenciamento.pdf> Acesso em: 11 mai. 2011.

STALLINGS, William. **SNMP, SNMPv2, SNMPv3, and RMON 1 and 2.** 3a Ed. ADDISON-WESLEY, 1999.

TANENBAUM, Andrew S. **Redes de Computadores.** Rio de Janeiro: CAMPUS. 1997.

TEIXEIRA JÚNIOR, José H.; SUAVÉ, Jacques Philippe; MOURA, José A. Beltrão; TEIXEIRA, Suzana de Queiroz Ramos. **Redes de Computadores.** São Paulo: MAKRON, 1999.

TORRES, Gabriel; LIMA, Cássio. **O Modelo de Referência OSI para Protocolos de Rede**. 2007 <http://www.clubedohardware.com.br/printpage/O-Modelo-de-Referencia-OSI-para-Protocolos-de-Rede/1349> Acesso em: 19 de abr. 2011.

APÊNDICE A – ARTIGO

Implantação da Ferramenta Nagios para Monitoração de Rede e Análise e Tratamento dos Eventos por Meio de Softwares de Apoio

Leandro Koehler Cardoso[1]

[1]Curso de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma – SC – Brasil.

Leandrocardoso82@gmail.com

Abstract. *This study aims to evaluate the behavior of Nagios in the data collection of problems detected on the network. The study was conducted in a controlled environment, suitable for tests simulating various events and errors, making it possible to check the performance of the network and equipment's monitored by Nagios and Cacti support software. Tools were evaluated in order to demonstrate the operation and effectiveness in helping practitioners who want to deploy this technology as a free software solution to monitor network and equipment. A study of the functioning of the network structure and protocols was conducted, as well as methods for monitoring and network management in order to have a broad foundation to implement network management tools and can safely perform the tests and to be able to collect data that indicate whether the use of Nagios in conjunction with Cacti can actually assist in managing a complex network environment.*

Keywords*: Cacti, Network Management, Monitoring, Nagios, Free Software.*

Resumo. Este trabalho tem como objetivo avaliar o comportamento do Nagios no levantamento de dados dos problemas detectados na rede. O estudo foi realizado em um ambiente controlado, próprio para testes simulando diversos eventos e erros, assim podendo verificar o desempenho da rede e dos equipamentos monitorados dos erros levantados pelo Nagios e o software de apoio Cacti. Foram avaliadas as ferramentas com o intuito de comprovar o funcionamento e a eficácia no auxílio dos profissionais que desejam implantar esta tecnologia, como solução de software livre para monitorar rede e equipamentos. Foi realizado um estudo do funcionamento da rede, sua estrutura e protocolos, como também métodos de monitoramento e gerenciamento de rede a fim de ter um embasamento amplo para implementar as ferramentas de gerenciamento de rede e poder realizar os testes com segurança e levantar os dados que indicarão se a utilização do Nagios em conjunto com Cacti realmente podem auxiliar na administração de um ambiente de rede complexo.

Palavras-Chave: Cacti, Gerenciamento de rede, Monitoramento, Nagios, Software livre.

1 Introdução

Com elevado número de máquinas interligadas e distribuídas numa grande estrutura, fica quase impossível gerenciar e monitorar todos os eventos ocorridos em uma rede de computadores, onde se tem de ficar conectado 24 horas por dia e 7 (sete) dias por semana. Por isso, utilizar uma ferramenta de monitoração seria de fundamental importância para poder sanar o mais rápido possível, eventuais problemas que possam ocorrer nesta estrutura.

A utilização da ferramenta Nagios, trata-se de uma solução gratuita e extremamente eficiente e flexível, tendo algumas das características como: o monitoramento de serviços de rede, monitoramento de recursos de servidores como CPU, memória, disco e processos. Tem a capacidade de definir hierarquia da rede, enviar notificações imediatamente sobre problemas na rede via e-mail e Pager.

O Nagios pode tomar contramedidas de acordo com o problema na rede, gerar relatórios, gráficos e históricos dos acontecimentos. É versátil, flexível e verifica constantemente a disponibilidade dos serviços e hosts.

Com isso, é possível demonstrar diversas maneiras de interagir com os problemas utilizando a ferramenta Nagios e alguns softwares de apoio, no monitoramento de serviços, hardware e softwares analisando e tratando os eventos apresentados. A principal utilização desta ferramenta está em evitar problemas de rede por meio de monitoramento evitando que algum equipamento ou toda estrutura fique parada por minutos, horas ou até mesmo dias, já que todo equipamento não dá 100% de garantia de sua utilização.

2 Implantação da Ferramenta de Monitoração de Rede Nagios e Softwares de Apoio Cacti

2.1 Descrição do Ambiente a ser Gerenciado

Este estudo tem como escopo a rede de computadores composta por dois computadores interligados via LAN 10/100 Mbps, contendo três máquinas virtuais executando nesses dois computadores. A rede provê serviços de e-mail, internet, entre outros. Todos os equipamentos estão configurados e executando sobre o protocolo TCP/IP.

O ambiente foi configurado para dar totais condições aos testes como se estivesse em uma rede corporativa padrão com todos os recursos e serviços básicos necessários.

Servidores das máquinas virtuais estão com o sistema operacional GNU/Linux Debian 6.0 e os computadores estão com o sistema operacional MS Windows 7.

Na Figura 1 a seguir é possível observar a estrutura de rede a ser gerenciada.

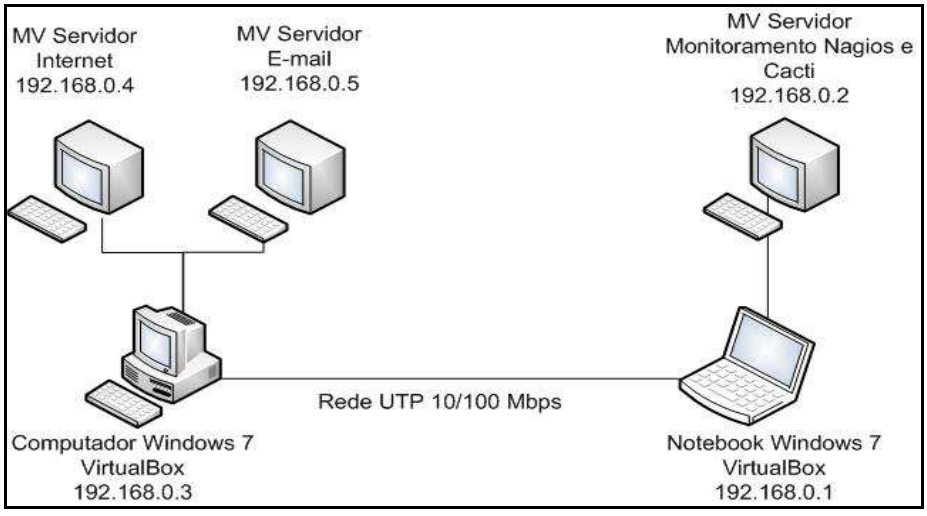


Figura 1. Estrutura de rede gerenciada

2.2 Estado Atual dos Serviços

Há diversos serviços em execução disponíveis numa rede corporativa para atender a demanda dos usuários. O acesso à internet e o serviço de e-mail são essenciais para o andamento da rotina dos usuários. Entretanto um monitoramento efetivo desses ou de outros serviços não são empregados, tampouco dos servidores em que estão instalados.

Ao ocorrer alguma falha deixando indisponível algum serviço, seja por que o servidor que fornece está apresentando problemas ou o serviço parou ficando indisponível, o mais comum é o setor de tecnologia receber inúmeras ligações de usuários avisando que há algo de errado, ou o administrador se antecipa avisando os usuários da indisponibilidade do serviço e tomando medidas para retomar a rede ao seu estado normal.

Atualmente é difícil saber como os recursos da rede estão sendo consumidos, por ser no mínimo trabalhoso ou não ter as informações. O espaço em disco, por exemplo, é um recurso importante no caso dos servidores de ser verificados. Para obter está informação o administrador tem de acessar os servidores e verificar manualmente a quantidade de espaço livre em disco.

2.3 Proposta de Solução de Gerenciamento para Avaliação

Esta proposta tem o objetivo de avaliar uma solução de gerenciamento de rede capaz de monitorar, notificar e contabilizar os recursos e serviços de rede ao administrador com rapidez e eficiência, quando um evento indesejado ocorrer.

Objetivo especifico do trabalho consiste em:

- Implantar as ferramentas de monitoramento Nagios e Cacti;
- monitorar os serviços e equipamentos de rede;
- simular eventos de erros relacionados ao funcionamento de serviços e equipamentos monitorados;
- enviar alertas aos administradores de rede sempre que um serviço ou equipamento estiver apresentando algum problema;
- visualizar os resultados do que está sendo monitorado;
- avaliar as ferramentas no monitoramento dos serviços e equipamentos.

2.4 Implantação das ferramentas de Monitoramento

O trabalho foi realizado a partir da instalação de um servidor com sistema operacional GNU/Linux Debian em uma máquina virtual o software utilizado na virtualização foi o VirtualBox.

Com base no que foi escrito pelo autor Costa (2008) toda distribuição GNU/Linux vem por padrão com muitos drivers e serviços genéricos instalados por padrão ocasionando aumento na utilização da memória RAM ou de conter algum erro que possa comprometer a segurança do ambiente. Para evitar estes problemas é recomendado remover alguns serviços.

Ao finalizar a instalação do Debian no site do distribuidor recomenda-se atualizar o sistema operacional, já que o projeto Debian está em constante atualização. Toda

distribuição GNU/Linux possui seu próprio gerenciador de pacotes, nestes pacotes poderá ser instalado todas as dependências dos pacotes utilizados para esse Sistema Operacional.

A opção de utilizar um banco de dados garante o armazenamento das informações e processos futuros como atualizações além de facilitar o processo de transferência dos dados. Armazenar as informações no HD do servidor é possível, mas não é considerada uma prática segura, além de várias outras dificuldades que pode apresentar principalmente no caso de uma atualização do software ou troca de hardware. Neste caso foi utilizado o banco de dados MySQL para armazenar as informações e poder ter acesso nas demais aplicações que necessitam dos dados armazenados.

Além da instalação do banco de dados devem ser instalados outros aplicativos e serviços que são necessários para o funcionamento do Nagios e do Cacti. Para poder utilizar a interface Web é necessário a instalação do WebServer Apache e do PHP, assim após estar configurados pode-se obter os dados visualmente pela interface web.

Após a instalação das dependências, o Cacti é o próximo passo. Esta ferramenta vai ser utilizada para análise por meio dos gráficos, mesmo sabendo que é bem completa e com possibilidades de expansão por meio de *plugins*.

Para a monitoramento de qualquer equipamento deve ser verificado se o SNMP está corretamente instalado e configurado. Com esse processo concluído podem ser visualizados e analisados os dados capturados dos equipamentos desejados, dividindo em árvores os gráficos gerados pelo Cacti facilitando a observação caso tenha vários servidores e serviços monitorados.

O Nagios foi à última aplicação instalada e configurada, não só por sua complexidade e esforço para instalar e configurar adequadamente, mas por ser a principal ferramenta utilizada para monitorar os recursos e equipamentos. Colocar o Nagios executando e funcionando requer muito mais tempo e com base na experiência das instalações anteriores, ajudará a ter um entendimento do ambiente de monitoramento de uma rede.

Por último foi simulado eventos com o objetivo de demonstrar o funcionamento de toda a estrutura de monitoramento da rede e a capacidade de fornecer soluções, contabilizar a utilização dos recursos, monitorar e notificar aos administradores quando ocorrer algum evento indesejado.

2.4.1 Configuração das ferramentas Nagios e Cacti

O Nagios foi configurado para alertar ao administrador sempre que um serviço não estiver respondendo ou um host perder a conectividade, alterando a cor facilitando a identificação do problema agilizando a ação do administrador.

Na Figura 2 é possível verificar o Nagios em sua relação de servidores e serviços monitorados e suas sinalizações por meio das cores.

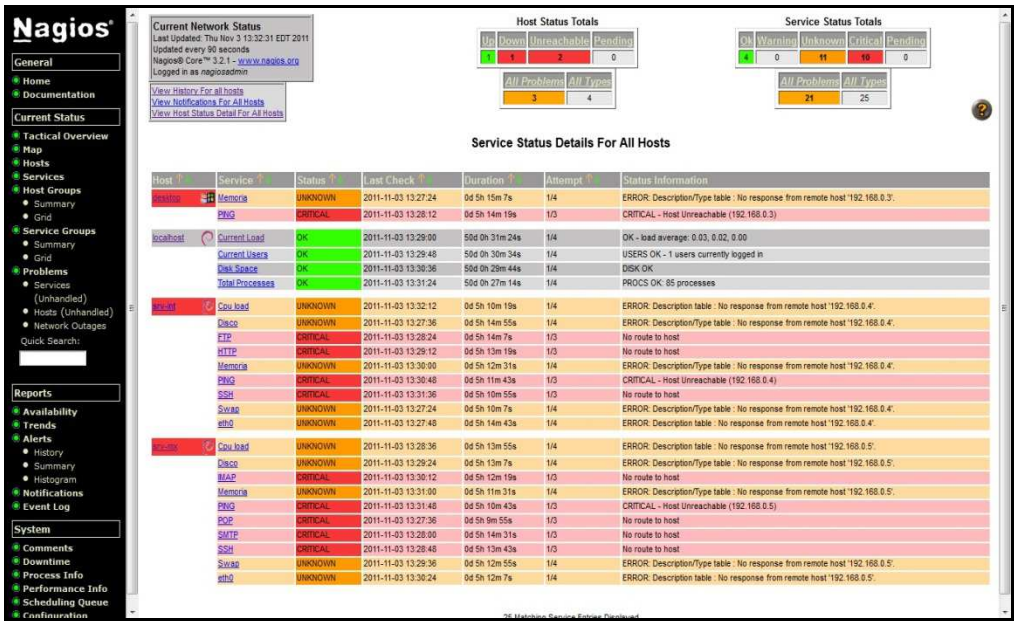


Figura 2 - Nagios, relação dos servidores e serviços monitorados.

Como parte na solução de monitoramento de rede o Cacti fica como principal método para levantamento de informações e demonstração dos dados por meio dos gráficos, demonstrando todo o histórico da utilização do serviço monitorado.

Estas informações possibilitam ao administrador verificar os pontos de maior e menor utilização de um determinado recurso, identificando problemas e podendo planejar manutenções ou investimentos para sanar o problema com maior segurança.

Na Figura 3 pode ser observado como os gráficos gerados podem auxiliar o administrador de rede na identificação de um possível problema.

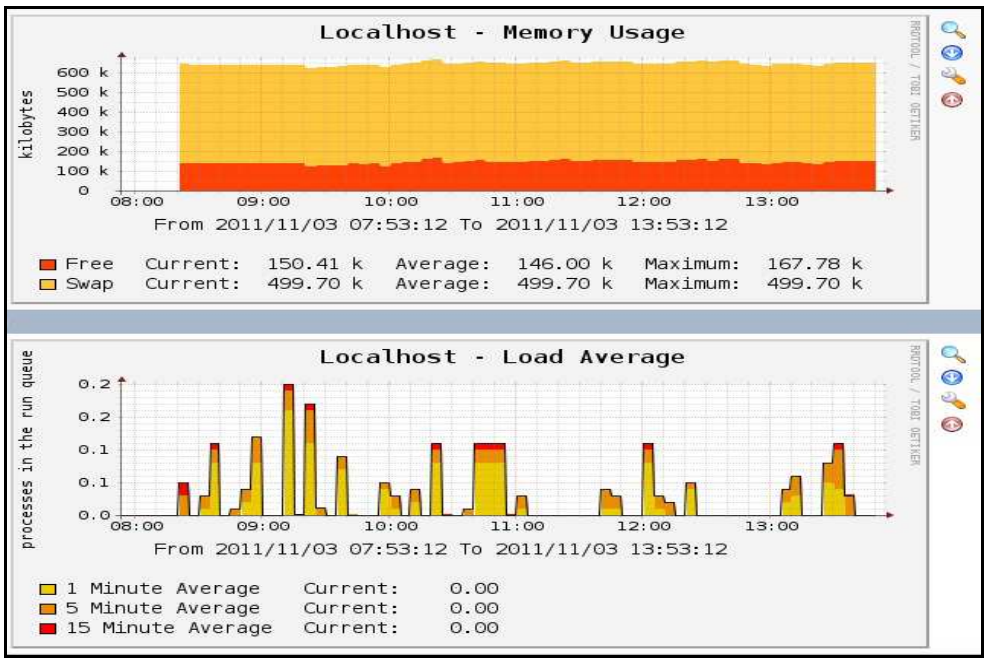


Figura 3 - Cacti, histórico de contabilização dos recursos

2.5 Simulação e Testes

Os testes foram baseados na utilização da ferramenta para monitoramento de rede Nagios em conjunto com a ferramenta Cacti e alguns *plugins* que vão auxiliar na comunicação e captura dos dados.

Por meio de pesquisas na internet, livros, artigos e outros trabalhos sobre o tema, foi possível entender estas ferramentas de monitoramento de rede e sua forma de aplicar em um ambiente com estrutura complexa e obter os resultados levantados por essas ferramentas, permitindo que o administrador da rede possa avaliar e aplicar medidas contraceptivas as falhas levantadas.

O ambiente empregado as ferramentas conta com um computador com sistema operacional Microsoft Windows 7, com duas máquinas virtuais. Estes três sistemas estão sendo monitorados, além de um notebook com sistema operacional Microsoft Windows 7 e uma máquina virtual que vai ser o servidor de monitoramento.

Em uma das máquinas virtuais do computador foi instalado o sistema operacional GNU/Linux Debian como servidor de internet. Como principais serviços monitorados deste servidor estão: HTTP, FTP, SSH, CPU, HD, Memória, Swap e rede.

Na outra máquina virtual desse computador também foi instalado o sistema operacional GNU/Linux Debian como servidor de E-mail. Este servidor foi configurado para monitoramento os seguintes serviços: POP, IMAP, SMTP, SSH, CPU, HD, Memória, Swap e rede.

A máquina virtual que se encontra instalada no notebook é o servidor de monitoramento da rede onde foram instaladas e configuradas as ferramentas Nagios e Cacti. Este servidor roda sobre a plataforma GNU/Linux Debian.

Com a estrutura montada, conforme mostra a Figura 6, foi possível realizar diversos testes como simulações de eventos de erros pra isso foram criados os scripts nos servidores de internet e E-mail, que força a parada de serviços e pode aplicar o teste de estresse de CPU, assim podendo obter dados e verificar se o monitoramento está sendo realizado de maneira satisfatória, analisando como funciona o Nagios sem interferir no ambiente da empresa e evitando comprometer serviços importantes.

Tendo o ambiente montado e configurado, foi definido que para realizar os testes seria necessário um gatilho, onde o responsável possa forçar uma situação adversa, gerando uma mensagem de alerta dos serviços monitorados.

Foi criado um script, que de forma prática possa aplicar um comando que desative ou ative um determinado serviço, como pode ser observado na Figura 4, ao rodar o script vai aparecer o menu onde contém os comandos para os testes em alguns serviços. Estes comandos são por meio de números, por exemplo, no servidor de e-mail srv-mx tem no script a opção 1 para parar e 2 para iniciar o serviço do servidor POP/IMAP.

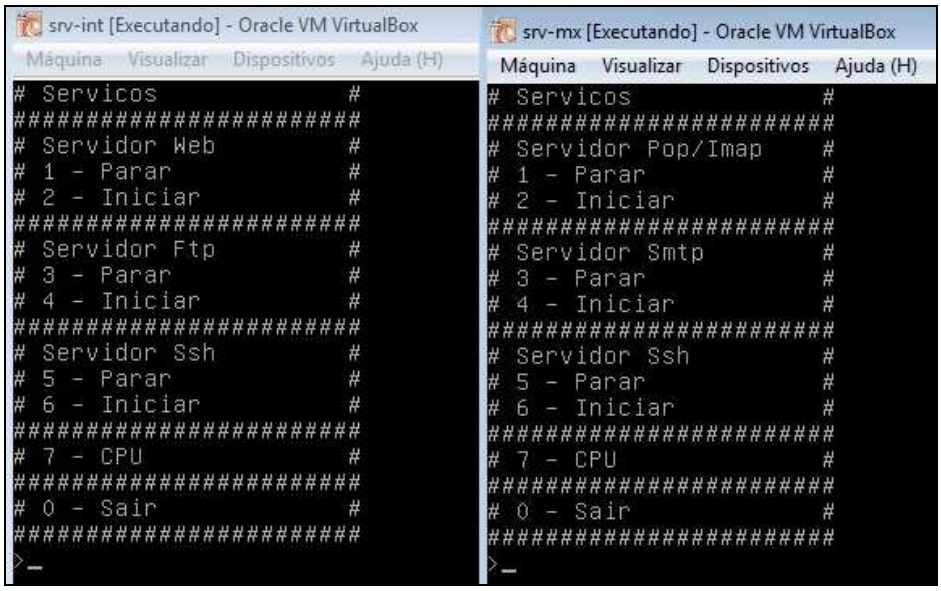


Figura 4. Scripts para testes nos servidores de E-mail e Internet

Com o Nagios já configurado e funcionando, pode ser acessada sua interface web e observar os hosts monitorados. A Figura 5 mostra a página principal do Nagios que contém as informações principais da ferramenta na parte central e na esquerda o menu onde se encontra os diversos tipos de interação e visualização dos hosts e seu estado.

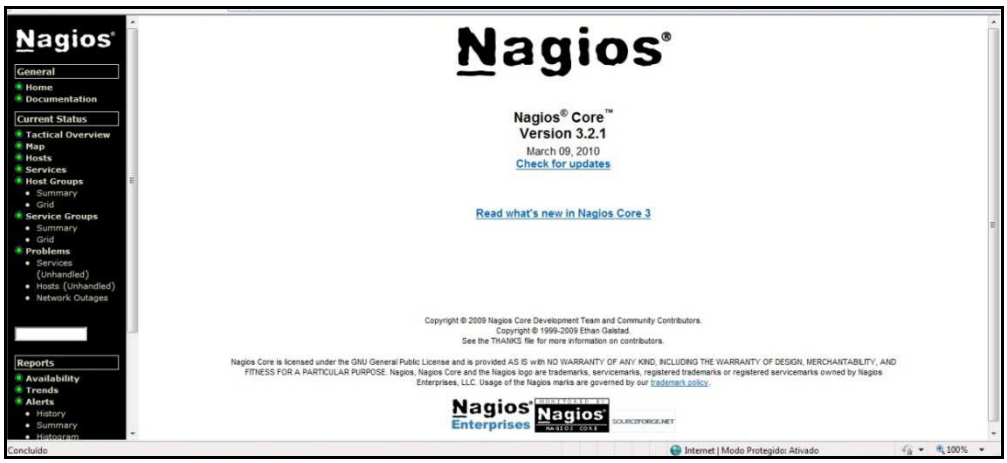


Figura 5. Nagios, interface web da tela principal

Ao executar o comando no script, que vai forçar a parada de um serviço monitorado, no menu do Nagios pode-se escolher várias formas de observar o local e o serviço que está ocorrendo o problema. Foi escolhido verificar pela opção Hosts do menu, onde é apresentado na Figura 6.

Nesta opção ficam visíveis todos os computadores monitorados e seus status. O Nagios trabalha com cores para demonstrar com está os serviços monitorados, verde para tudo certo, laranja com algum problema ou inconsistência e vermelho para serviço parado ou não respondendo.

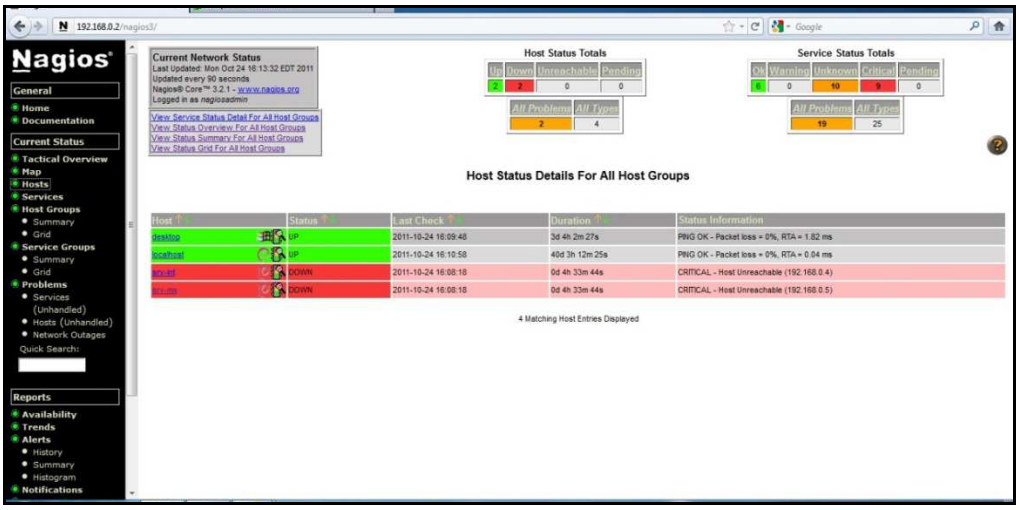


Figura 6. Nagios, página de monitoramento por Hosts

Através das simulações de eventos de erros, foi possível observar a eficiência da ferramenta de monitoramento o Nagios, mas só com ela o trabalho de análise para adotar medidas corretivas às falhas ocorridas não seria o ideal.

Com a implantação do Cacti, pode-se ter em gráficos uma visão real dos hosts e seus serviços que tem suporte a SNMP, como CPU, Memória, rede e etc. Essas informações são muito importantes para monitoramento de seus recursos e estudos do consumo destes recursos.

No Cacti em sua interface web, foi adicionado além do *localhost*, que por padrão já vêm configurado, os servidores Linux e os computadores Windows. Na Figura 7 pode ser observado a página principal do Cacti, que tem um menu há esquerda que pode ser alterado conforme a opção acima dele for escolhida, Console ou *Graphs*.

Figura 7. Cacti, interface web da página principal

Para o monitoramento é utilizado o menu *Graphs*, pois o menu Console é a parte de configuração do Cacti. O *Graphs* é a parte onde é possível observar os gráficos dos hosts monitorados e as árvores criadas para organizar o ambiente monitorado.

Foram criadas duas árvores no Cacti, a árvore srv-linux onde estão configurados os servidores GNU/Linux que estão sendo monitorados e a árvore srv-windows que contém os computadores Microsoft Windows monitorados. Na Figura 8 abaixo pode ser observado melhor essa organização em árvores.

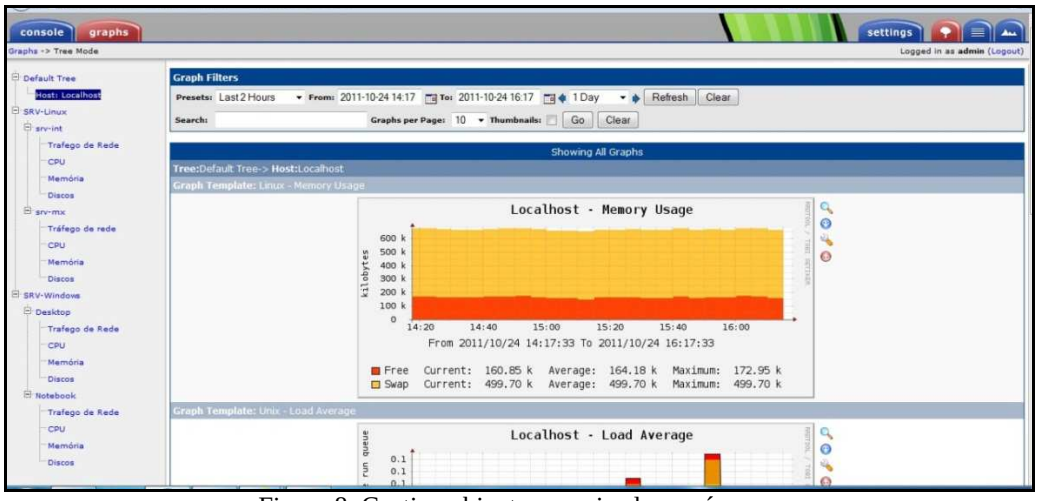


Figura 8. Cacti, ambiente organizado por árvores

Com o Nagios e o Cacti configurados e obtendo os dados, o administrador pode analisar e fazer estudos das áreas críticas ou que possam apresentar problemas futuros. Foi observado neste trabalho que com o auxílio do Cacti alguns aspectos que no modo tradicional o administrador poderia exigir muito tempo só para análise e comparação, o Cacti trouxe em pouco tempo todos os dados necessários.

Ficou clara esta vantagem nos testes realizados no servidor de e-mail srv-mx, quando foi retirada parte de sua capacidade de memória RAM demonstrando pelos gráficos esse recurso sempre no limite. Este tipo de informação é muito importante para o administrador por dar tempo para programar uma manutenção preventiva e verificar se algum recurso ou serviço possa estar consumindo todo o recurso.

Na Figura 9 a seguir é observado o gráfico que demonstra o problema relatado. Na imagem do gráfico srv-mx – Usade Space – Phisical Memory, o recurso utilizado está próximo do limite podendo ocorrer algumas falhas paralisando os serviços ou o próprio computador.

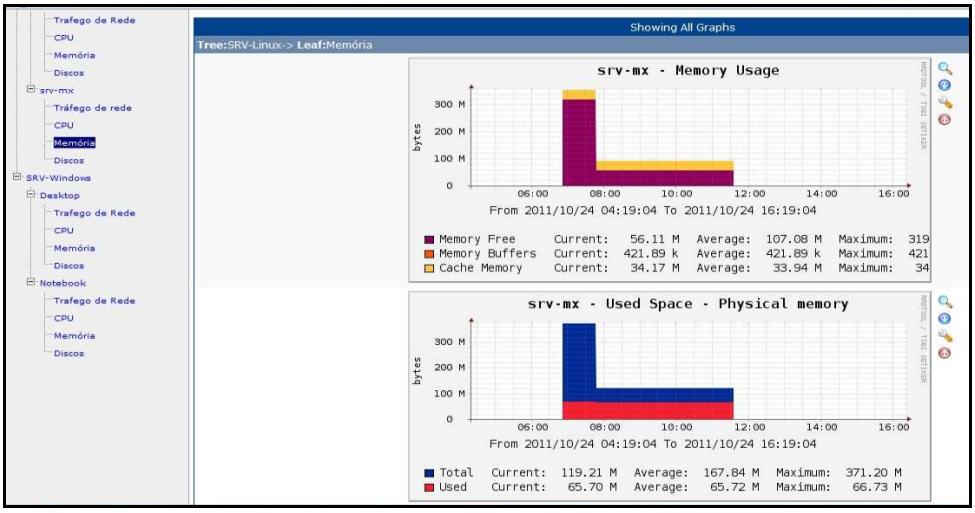


Figura 9. Cacti, gráfico monitoramento da memória RAM do servidor srv-mx

Cada administrador e empresa têm suas rotinas e prioridades, as medidas adotadas nesse trabalho podem não ser as mais adequadas para outro local. Com base nesses testes, foi possível demonstrar um pouco das possibilidades destas ferramentas de monitoramento podem proporcionar.

Além do monitoramento gráfico do Cacti, a fim de evitar situações críticas, pode agilizar o atendimento, mesmo antes dos usuários perceberem o problema e sanar as falhas ocorridas de algum equipamento ou serviço o mais rápido possível. Por isso foram adotadas algumas medidas corretivas perante alguns casos levantados.

Neste trabalho o monitoramento pela interface web do Nagios em um monitor próprio para o serviço, é uma das principais maneiras utilizadas para acompanhamento das ações e eventos da infraestrutura monitorada. Nesta interface web a opção hosts como definida como padrão para análise, com todos os *hosts* configurados aparecendo na tela principal.

Qualquer erro fica visível na tela onde o administrador poderá verificar o erro e tomar as providências para estabelecer o mais rápido possível. Na Figura 10 pode-se observar a tela do Nagios na opção hosts com todos os servidores monitorados.

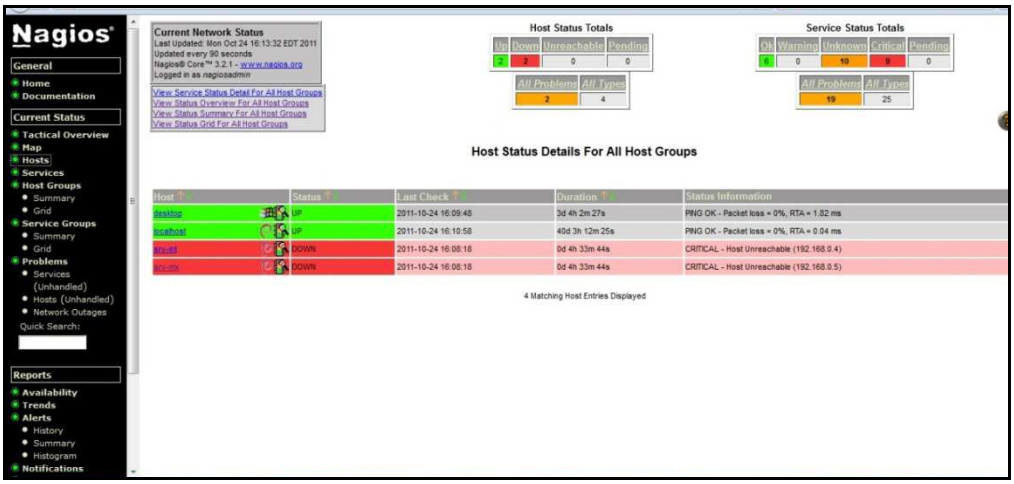


Figura 10. Nagios, tela dos Hosts monitorados

Esta é uma das diversas medidas que podem ser adotadas com a ferramenta Nagios. Outra medida muito utilizada é o envio de mensagem via e-mail. Esta medida é muito utilizada em monitoramento de equipamentos que ficam ligados 24 horas por dia, como servidores de e-mail e internet ou servidores de aplicativos sem uma equipe ou responsável no local para monitoramento desses recursos.

2.6 Avaliação e Resultados

Foram realizados diversos testes na estrutura monitorada para levantamento dos dados e poder avaliar as ferramentas de monitoramento Nagios e Cacti. Nos testes as ferramentas atenderam todos os requisitos esperado apresentando os dados e eventos ocorridos para o administrador quase que instantaneamente.

Os testes foram realizados em serviços que estavam instalados, como também nos equipamentos. Muitos serviços como servidor web Apache foram parados e iniciados e em todos os casos foram notificados ao administrador visualmente pela interface web pelo Nagios.

Foi alterada a quantidade de memória RAM dos servidores localizados nas máquinas virtuais, e foi possível analisar a diferença nos gráficos pelo Cacti. Também foi utilizado o teste de estresse de CPU, que testa o processador ficando possível observar as variações pelos gráficos gerados pelo Cacti.

O ponto negativo é a complexidade na implantação da ferramenta Nagios, por exigir muito tempo e esforço em sua instalação e configuração. O Nagios para atender com eficiência um ambiente de rede complexo vai exigir muito estudo ou auxilio de pessoas

especializadas, que possa aplicar todo o recurso oferecido pelo Nagios no monitoramento de rede.

A avaliação foi positiva da utilização das ferramentas no auxilio do monitoramento de rede. O emprego das ferramentas torna em geral a rotina complexa e de grande responsabilidade do administrador de rede mais simples, sem retirar a importância que o administrador vai ter em analisar e tomar as medidas corretas na prevenção e correção de possíveis ocorrências.

3 Conclusão

A implantação e configuração de ferramentas para monitoramento de redes se torna cada vez mais necessária. Com a redução de recursos humanos e a crescente complexidade das redes de computadores o monitoramento manual do sistema fica inviável.

As ferramentas de monitoramento para o administrador é a forma mais prática e eficiente de ter em mãos todas as informações necessárias para manter a estrutura funcionando e ser informado, o quanto antes, sobre problemas que estão ou vão ocorrer.

O Nagios por sua complexidade e robustez é uma das ferramentas de monitoramento de rede capaz de auxiliar o administrador de rede sobre os mais diversos problemas que possam ocorrer. O estudo desta ferramenta, aplicada ao ambiente para gestão e monitoramento da rede, permitiu a avaliação de diversos aspectos de seu funcionamento no monitoramento e gestão de redes de computadores.

Para poder contabilizar e ter maiores informações, foi instalado o software Cacti para o apoio e demonstrações via gráfico dos recursos utilizados, permitindo ao administrador analisar estas informações na manutenção de sua estrutura de rede monitorada.

A implantação destas ferramentas em uma estrutura de rede própria para realizar diversos testes e avaliar de forma eficiente a capacidade e todo o potencial do Nagios e do Cacti na pratica, sem ter de ficar esperando algum evento ocorrer em uma estrutura de rede da empresa. Como a ocorrência de certos eventos pode ser difícil de ocorrer ou imprevisível, numa estrutura montada para os testes é possível forçar diversos eventos e verificar em tempo real os efeitos do erro e as ações do Nagios em relação a essas inconsistências.

Os resultados alcançados com a implantação das ferramentas de monitoramento de rede atingiram seu objetivo que é o suporte no monitoramento de ambientes complexos onde cada vez mais o numero de equipamentos eletrônicos cresce e sobrecarregando a equipe responsável.

Muitos outros serviços e equipamentos poderiam estar incluídos neste trabalho, mas para fim de testes e avaliação das ferramentas, o ambiente relacionado atingiu todos os requisitos e demonstrou como podem ser úteis estas duas ferramentas de monitoramentos trabalhando em conjunto no auxílio do administrador no monitoramento de ambientes de rede.

Certamente uma ferramenta de monitoramento de rede implantada como solução, não vai substituir o administrador de rede, está solução vai apenas facilitar e somar em suas atividades se tornando mais uma ferramenta para auxiliar na administração da rede. A utilização destes recursos se torna fundamental no dia-a-dia do administrador de rede que com pouco investimento e pessoal poderá administrar sua estrutura de rede com segurança e agilidade na prevenção e resolução dos problemas.

Referências

ANDRADE, Hetty Alves de. **Nagios como Solução de Monitoramento de Rede.** Disponível em: < http://www.ginux.ufla.br/files/mono-HettyAndrade.pdf/> Acesso em: 02 jun. 2011.

COSTA, Felipe. **Ambiente de Rede Monitorado com Nagios e Cacti.** Rio de Janeiro: MODERNA, 2008.

LOPES, Raquel T.; SUAVÉ, Jacques Philippe; Nicolletti, Pedro. S. **Melhores Práticas para Gerência de Redes de Computadores**. CAMPUS, 2003.

MAJEWSKI, Roberto. **Sistemas de Monitoração de Rede.** 2009. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Roberto%20Majewski%20-%20Artigo.pdf >Acesso em: 01 jun. 2011.

MATOS, Leonardo Kolisnik de. **Gerenciamento de equipamentos de rede utilizando o software CACTI**. 2009. Disponível em: < http://www.ppgia.pucpr.br/~jamhour/RSS/ TCCRSS08A/Leonardo%20Kolisnik%20de%20Matos%20-%20Artigo.pdf> Acesso em: 23 mai 2011.

MENEZES, Elionildo da Silva. SILVA Pedro Luciano Leite. **Gerenciamento de Redes: Estudo de Protocolos.** UFP Pernambuco. 1998. Disponível em: <http://www.di.ufpe.br/ ~flash/ais98/gerrede/gerrede.html> Acesso em: 29 abr. 2011.

OLIVEIRA, Frederico S. Guimarães. **Gerenciamento de Redes de Computadores com o uso do Raciocínio Baseado em casos e Ferramentas Auxiliares.** 2007. Disponível em: <http://www.coc.ufrj.br/index.php?option=com_docman&task=doc_view&gid=1643> Acesso em: 25 mai. 2011.

PINHEIROS, José Mauricio Santos. **Gerenciamento de Redes de Computadores.** 2002. Disponível em: < http://www.allnetcom.com.br/upload/GerenciamentodeRedes.pdf> Acesso em: 16 nov. 2011.

SANTOS, Cinthia Cardoso dos. **Gerenciamento de Redes com a Utilização de Software Livre.** Disponível em: <http://www3.iesam-pa.edu.br/ojs/index.php/sistemas/article/ viewFile/442/374 > Acesso em: 25 mai 2011.

SILVA, Ronaldo. **Gerenciamentos de redes de Computadores.** 2010. Disponível em: <http://www.rdsinfor.com.br/gerenciamento-de-redes-de-computadores/> Acesso em: 09 mai. 2011.

ANEXO A – INSTALAÇÃO DAS FERRAMENTAS NAGIOS E CACTI.

1 CONFIGURANDO SISTEMA OPERACIONAL DEBIAN PARA INSTALAÇÃO DOS SPFTWARES DE MONITORAÇÃO

1.1 AJUSTANDO SISTEMA OPERACIONAL DEBIAN

O primeiro passo ao finalizar a instalação do Debian é configurar os repositórios dos pacotes, para isto deve ser atualizado o arquivo *source.list*.

vi /etc/apt/sources.list

deb http://mirrors.kernel.org/debian main contrib non-free
deb-src http://mirros.kernel.org/debian main contrib non-free
deb http://security.debian.org /updates main contrib non-free
deb-src http://security.debian.org /updates main contrib non-free
deb http://ftp.br.debian.org/debian stable main
deb-src http://ftp.br.debian.org/debian stable main
deb http://packages.dotdeb.org stable all
deb-src http://packages.dotdeb.org stable all

Como o projeto Debian está em constante atualização é recomendável sempre manter seu sistema operacional atualizado executando os seguintes comandos:

Apt-get update
Apt-get upgrade

Para remover alguns serviços que não vai ser utilizado e evitar alguns problemas de com drivers e serviços.

update-rc.d –f portmap remove
update-rc.d –f nfs-common remove
update-rc.d –f exim4 remove
update-rc.d –f ppp remove
update-rc.d –f inetd remove
update-rc.d –f ldp remove
update-rc.d –f makedev remove
update-rc.d –f atd remove

Instalação das dependências necessárias para implementar as ferramentas de monitoramento Nagios e Cacti, será por meio do gerenciador de pacotes ATP do Debian.

Build-essential
Apt-get install build-essential

Vim
Apt-get install vim

Rcconf
Apt-get install rcconf

Ncurses
Apt-get install libncurses5
Apt-get install libncurses5-dev

Libxml2
Apt-get install libxml2
Apt-get install libxml2-dev

Libgd e libgd-dev
Apt-get install libgd1
Apt-get install libgb-dev

Libxpm-dev
Apt-get install libxpm-dev

Libpng12-0-dev
Apt-get install libpng12-0-dev

Libgdbm-dev
Apt-get install libgdbm-dev

Rrdtool
Apt-get install rrdtool

Snmp e snmpd
Apt-get install snmp
Apt-get install snmpd

1.2 INSTALANDO O MYSQL

aptitude install mysql-server mysql-client

1.3 INICIALIZANDO O MYSQL

/etc/init.d/mysql start

1.4 INSTALANDO WEBSERVER APACHE

apt-get update
apt-get install apache2

1.5 INICIALIZANDO O APACHE2

/etc/init.d/apache2 start

1.6 INSTALANDO DO PHP

apt-get install libapache-mod-php4
/etc/init.d/apache stop
/etc/init.d/apache start
apt-get install php4-mysql php4-curl php4-gd
extension=mysql.so
extension=curl.so
extension=gd.so

2 INSTALAÇÃO DO CACTI

Com as dependências instaladas e testadas pode ser iniciada a nova fase de instalação das ferramentas de monitoramentos. Vai ser instalada primeiramente o Cacti.

apt-get install cacti

Instalado o Cacti agora deve ser configurado o acesso ao banco de dados MySQL, por meio do diretório:

cd /var/www/cacti

Executar os seguintes comandos:

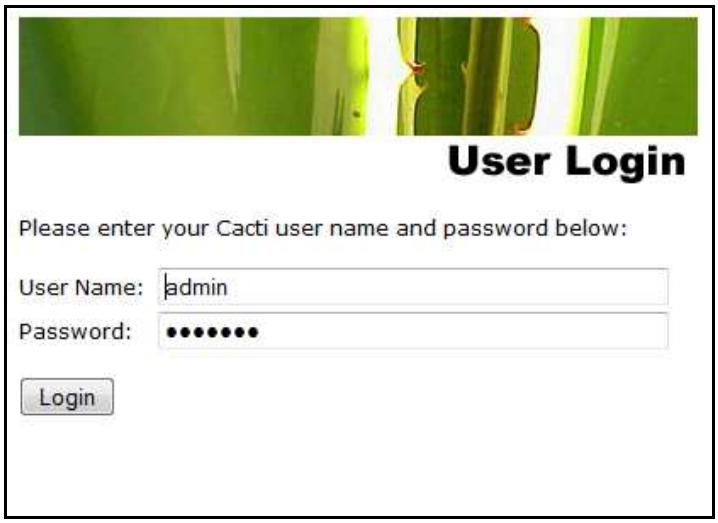
mysqladmin --user=root create cacti – para criar o banco de dados.
mysql cacti < cacti.sql – importa a estrutura do banco de dados.

Após instalação acessar via navegador para finalizar a configuração do Cacti. Para acessar entrar com o endereço do servidor de monitoramento, por exemplo: 10.1.1.1.

http://10.1.1.1/cacti/install/index.php

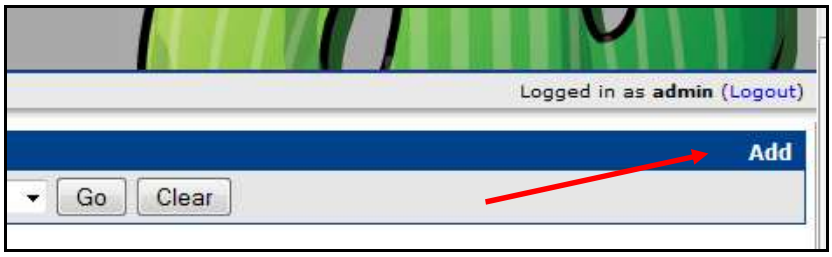
A primeira imagem mostra algumas informações sobre a ferramenta Cacti, clicando em *next* para avançar até encontrar a tela com os softwares necessários, caso não algum softwares desses não esteja listado voltar ao inicio da instalação e verificar os passos seguidos com cuidado. Se estiver tudo certo finalizar a instalação.

Finalizando a instalação vai aparecer a tela de acesso que por padrão do Cacti é *admin* tanto para Usuário como para senha. Acessando com estas informações é necessário redefinir a senha do *admin* colocando a senha que for mais conveniente.

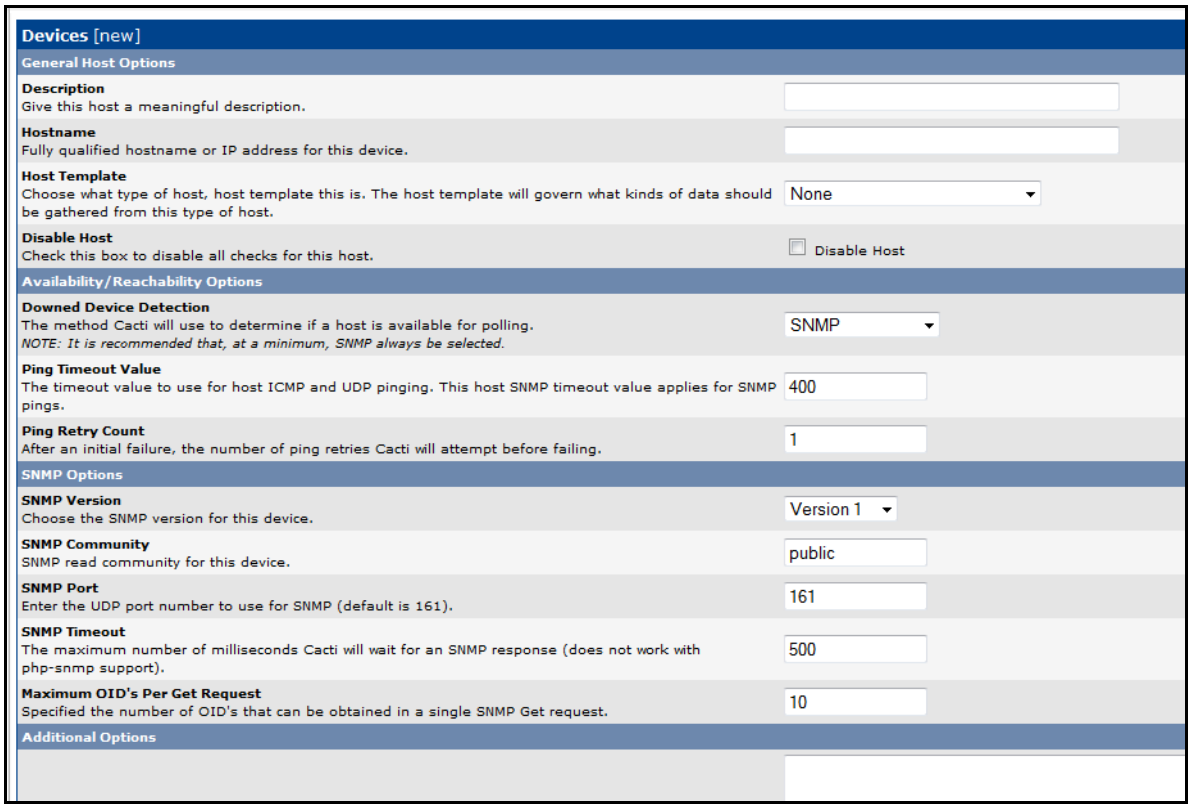


A partir deste momento o Cacti já está instalado com sucesso e inicia o processo de configuração do ambiente. A utilização da ferramenta se dá na tela principal clicando no campo *Create Devices*. Por padrão o Cacti já vem com o *localhost* configurado, para

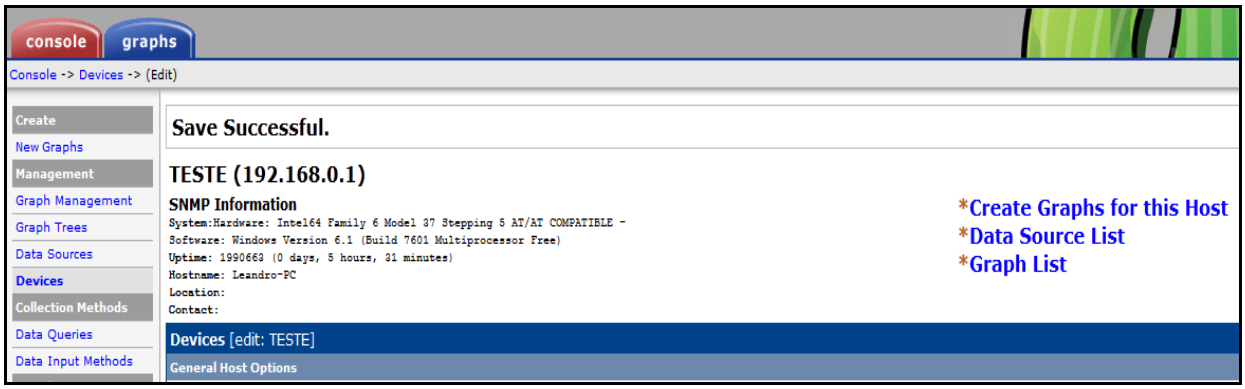
adicionar novo Host clique em *Add* no canto superior direito da tela.



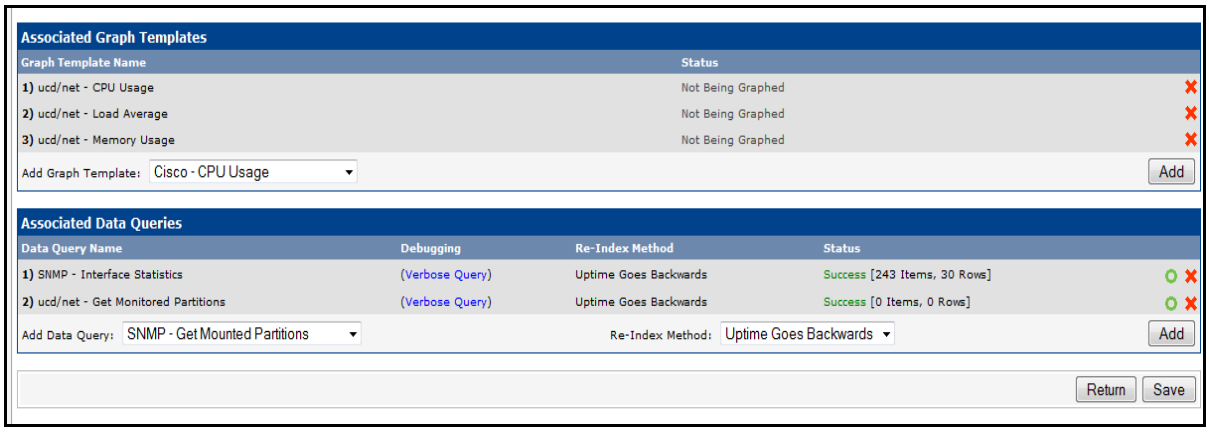
Preencher com os dados do servidor a ser monitorado. No campo *Host Template*, selecione *ucd/net SNMP Host* e clique em *create*.



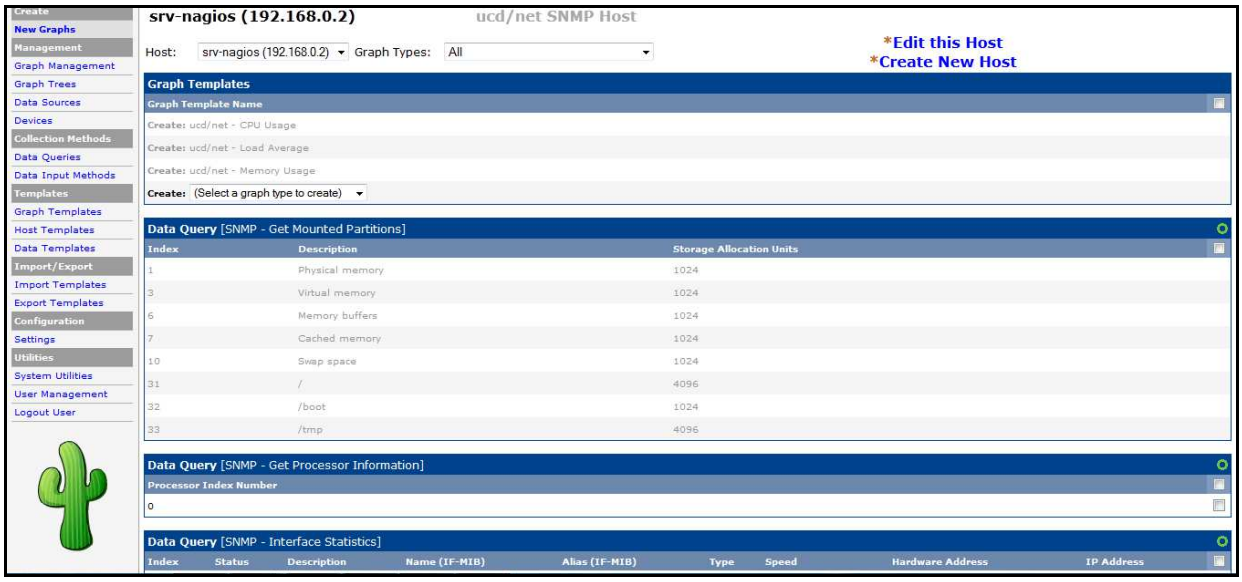
Em caso de sucesso na consulta ao SNMP, o cabeçalho aparecerá informando que a consulta está acontecendo corretamente com o servidor requisitado.



Na parte inferior da mesma tela, em *Add Data Query* selecionar *SNMP-Get Monted Partitions* para monitorar os discos do servidor. Para finalizar clicar em *Add* e depois salvar. Com esses passos realizados acessar o nome do servidor que acabou de ser criado para criar os gráficos referentes ao mesmo clicando em *Create Graphs for this host.*



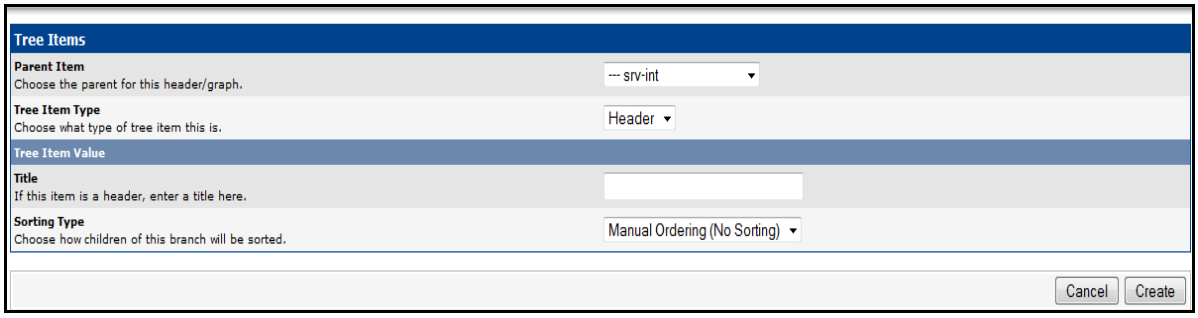
É necessário marcar todos os campos que são interessantes para o monitoramento. Depois de marcado, basta apertar em *Create*.



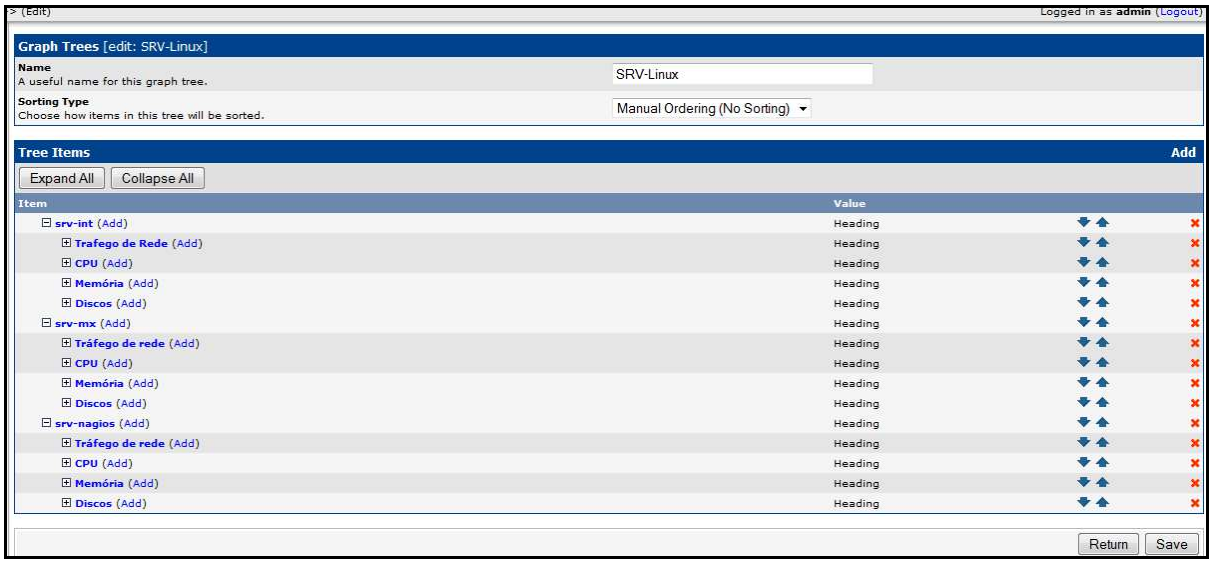
Concluindo a criação dos gráficos que serão os responsáveis por passar as informações coletadas. É necessário definir as árvores para organizar a visualização dos servidores monitorados clicando no campo *Graph Trees*.

Neste trabalho foram definidas duas árvores uma para os servidores Windows e outra para os servidores Linux. Está pode ser uma forma útil se pretender monitorar diversos servidores de empresas em um único ambiente de monitoração. Pode-se montar várias arvores, cada uma com o nome da empresa e dentro de cada árvore adicionar os servidores que pertencem a cada uma delas.

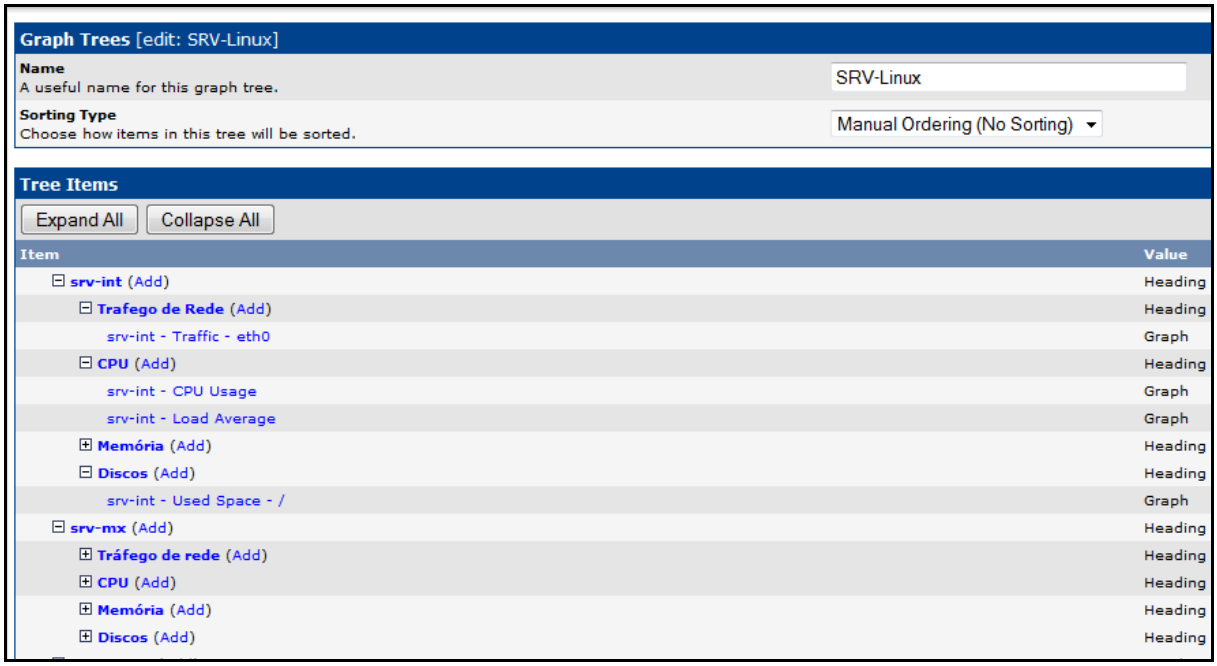
Clicando em *Add* para adicionar o servidor GNU/Linux a ser monitorado, após isso preencher o campo *Title* com o nome do *host* do servidor a ser monitorado e depois clique em *Create*.



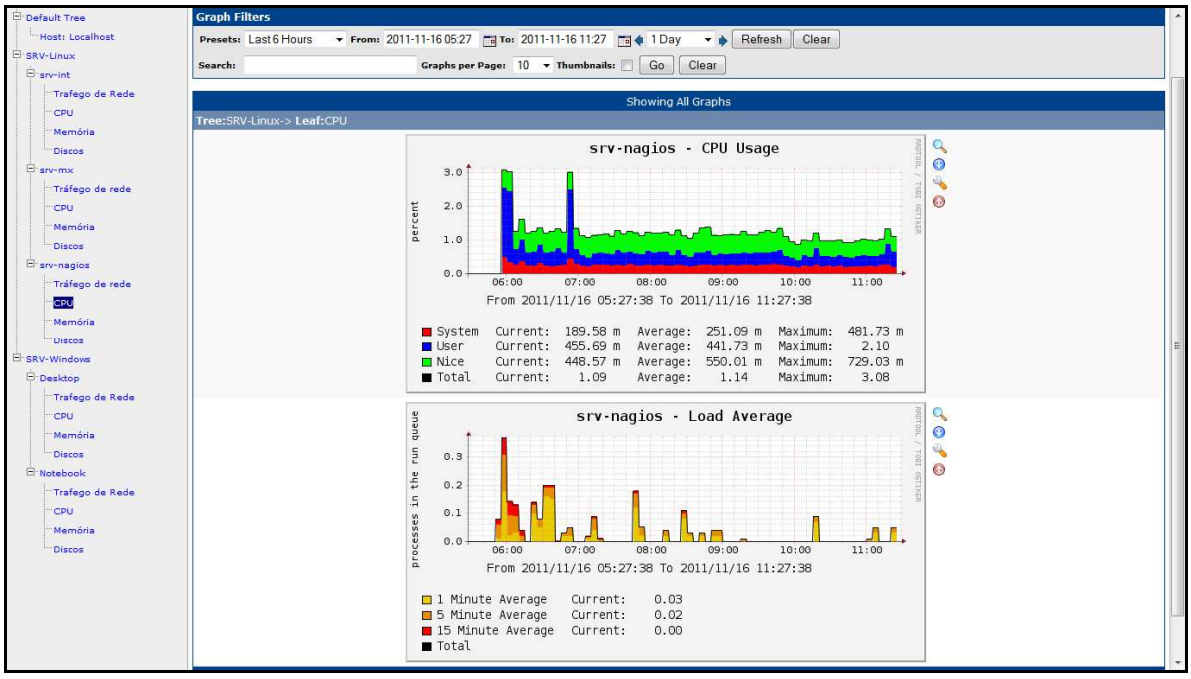
Clicando no campo Add ao lado do host com o nome do servidor que acabou de ser criado, vai ser possível incluir os itens que serão monitorados como, Tráfego de rede, Uso de CPU, Uso de Memória, Espaço utilizado.



Dentro de cada item como Tráfego de Rede adicionar os itens já marcados anteriormente que vai aparecer deixando separados e organizados para melhor observação dos dados coletados. Após todos os itens incluídos clicar em salvar.



Estes são os passos para acrescentar os servidores e os itens para monitoramentos no Cacti. Para visualizar os gráficos gerados pela ferramenta, basta clicar no campo *Graph*. No campo a esquerda é possível ver as árvores que foram criadas neste trabalho como mostra a figura abaixo.


Default Tree
Host: Localhost
SRV-Linux
srv-int
Trafego de Rede
CPU
Memória
Discos
srv-mx
Tráfego de rede
CPU
Memória
Discos
srv-nagios
Tráfego de rede
CPU
Memória
Discos
SRV-Windows
Desktop
Trafego de Rede
CPU
Memória
Discos
Notebook
Trafego de Rede
CPU
Memória
Discos
Graph Filters
Presets: Last 6 Hours
From: 2011-11-16 05:27
To: 2011-11-16 11:27
1 Day
Refresh
Clear
Search:
Graphs per Page: 10
Thumbnails:
Go
Clear
Showing All Graphs
Tree:SRV-Linux-> Leaf:CPU
srv-nagios - CPU Usage
percent
3.0
2.0
1.0
0.0
06:00
07:00
08:00
09:00
10:00
11:00
From 2011/11/16 05:27:38 To 2011/11/16 11:27:38
System Current: 189.58 m Average: 251.09 m Maximum: 481.73 m
User Current: 455.69 m Average: 441.73 m Maximum: 2.10
Nice Current: 448.57 m Average: 550.01 m Maximum: 729.03 m
Total Current: 1.09 Average: 1.14 Maximum: 3.08
srv-nagios - Load Average
processes in the run queue
0.3
0.2
0.1
0.0
06:00
07:00
08:00
09:00
10:00
11:00
From 2011/11/16 05:27:38 To 2011/11/16 11:27:38
1 Minute Average Current: 0.03
5 Minute Average Current: 0.02
15 Minute Average Current: 0.00
Total

3 INSTALAÇÃO DO NAGIOS

3.1 VERIFICAR SE AS DEPENDÊNCIAS E ARQUIVOS NECESSÁRIOS ESTÃO INSTALADOS

Para iniciar a instalação do Nagios vamos verificar se está tudo instalado e configurado para evitar problemas mais a frente nas configurações.

O comando abaixo é responsável por baixar as últimas atualizações salvando no arquivo APT de bibliotecas do Debian.

echo "deb http://ftp.debian.org/debian stable main" > /etc/apt/sources.list

apt-get update

Instalando as dependências

 # apt-get -y install apache2 build-essential libgd2-xpm-dev
 # apt-get -y install libjpeg62 libjpeg62-dev libpng12-dev
 # apt-get -y install snmp libsnmp-base
 # apt-get -y install libssl-dev openssl
 # apt-get -y install mc rsh-server openssh-server
 # apt-get -y install php5 php-pear libsnmp9-dev rcconf
 # apt-get -y install libsasl2-2 libsasl2-modules sasl2-bin mutt postfix

3.2 INSTALANDO O NAGIOS

Quem busca uma ferramenta eficaz e poderosa para monitoramento de servidores uma solução de grande utilidade é o Nagios.

Cria usuário Nagios com senha Nagios:

useradd -m -s /bin/bash nagios
passwd nagios

Cria grupo Nagios:

groupadd nagios

```
# usermod -G nagios nagios
```

Cria grupo grupo:

```
# groupadd grupo
# usermod -a -G grupo nagios
# usermod -a -G grupo www-data
```

Criar diretório dados. Nesse ponto inicia a instalação do Nagios propriamente dita. É recomendável, por questões de organização, que se crie um diretório de armazenamento antes de fazer o download dos fontes. O diretório criado foi */dados*.

```
# mkdir /dados
```

Acessa diretório dados:

```
# cd /dados
```

Baixar Nagios 3:

```
# wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-3.2.1.tar.gz
```

Descompacta nagios:

```
# tar xzf nagios-3.2.1.tar.gz
# cd nagios-3.2.1
```

Compilação e instalação do nagios:

```
# ./configure --with-command-group=grupo
# make all
# make install
# make install-init
# make install-config
# make install-commandmode
# make install-webconf
```

Cria usuário nagiosadmin para acesso a web:

htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

Reinicia apache:

/etc/init.d/apache2 restart

A partir deste momento, você já consegue acessar o Nagios via browser digitando:

http://ipdoservidornagios/nagios

Utilizando o usuário nagiosadmin e senha definida acima.

3.3 INSTALANDO OS PLUGINS DO NAGIOS

Os plugins do Nagios são os responsáveis pelos comandos a serem executados nos servidores clientes, você pode instalar vários outros plugins ou até mesmo criar os seus.

Neste site existe vários plugins para Windows/Linux prontos, acessem e dêem uma olhada em:

http://www.monitoringexchange.org/

Instalação dos *plugins* padrões do Nagios.

Acessar diretório dados:

 # cd /dados

Baixar plugins do Nagios 1.4.15:

 # wget http://prdownloads.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.15.tar.gz

Descompacta plugins:

 # tar -xvf nagios-plugins-1.4.15.tar.gz

Acessa diretório nagios-plugins-1.4.15:

 # cd nagios-plugins-1.4.15

Instalando o nagios-plugins:

 # ./configure --prefix=/usr/local/nagios --with-nagios-user=nagios --with-nagios-group=nagios
 # make
 # make install

Atualiza rc.d:

 # update-rc.d icinga defaults

Ajustes finais
Alterar a permissão do diretório Nagios:

 # chown nagios.nagios -R /usr/local/nagios

Reiniciar os serviços do Apache e do Nagios.

Reiniciar Apache:

 # /etc/init.d/apache2 restart

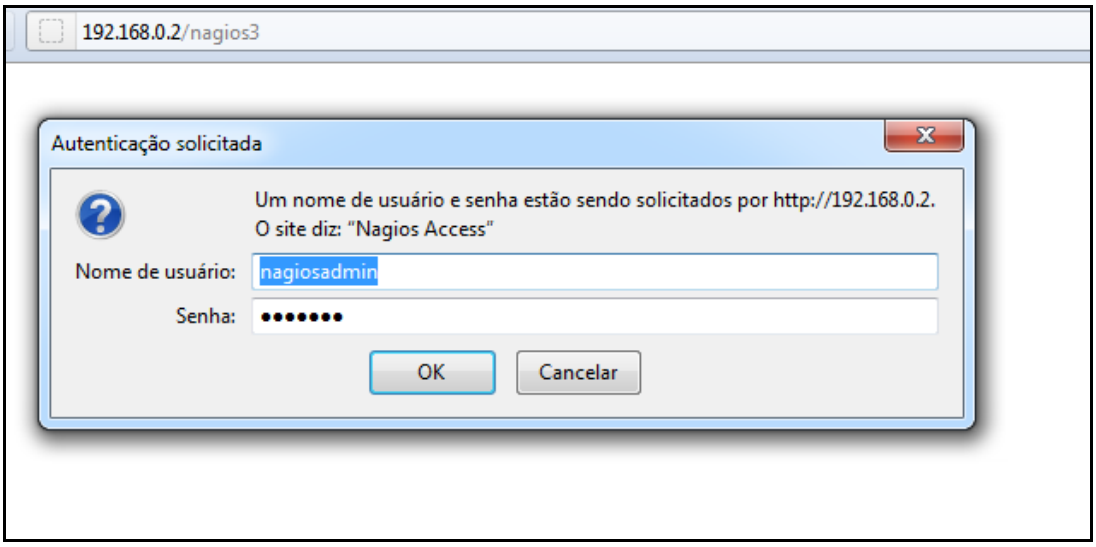
Reiniciar Nagios:

 # /etc/init.d/nagios restart

Acessar o seguinte endereço no browser para ingressar no Nagios. Ele já deve está monitorando a máquina local (*localhost*).

http://ip_do_servidor_nagios/nagios/

Usar o usuário e senha do *nagiosadmin* criado anteriormente.



3.4 INSTALAÇÃO DOS *PLUGINS* EM MÁQUINAS LINUX

Nesta parte pode ser observado como instalar os *plugins* do Nagios em máquina Linux. Será Usado os *plugins* do Nagios e o NRPE. A partir daqui iremos trabalhar nas máquinas a serem monitoradas. Os comandos a seguir devem ser passados nas máquinas clientes (a serem monitoradas).

Antes de instalar os *plugins*, certifique-se de que foram preenchidos os requisitos abaixo:

Acesso administrativo (root) nas máquinas a serem monitoradas;
Senha da conta Nagios do servidor de monitoramento (máquina que roda o Nagios).

Se não preencher os requisitos acima favor não continuar até que eles sejam preenchidos.

Se você preenche os pré-requisitos para a instalação dos *plugins* em máquinas Linux, siga os passos abaixo para instalar os *plugins* para monitorar os recursos locais das máquinas.

Para criar uma conta e senha para o Nagios use os seguintes comandos:

 # /usr/sbin/useradd nagios
 # passwd nagios

Instalação dos *plugins* no servidor a ser monitorado.

 # cd /dados

Até o momento da criação desse documento a versão mais nova é a 1.4.12. Para verificar as versões mais novas acesse:

http://www.nagios.org/download

Baixando os fontes:

 # wget http://osdn.dl.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.12.tar.gz

Extrair, compilar e instalar os fontes.

 # tar xzf nagios-plugins-1.4.12.tar.gz
 # cd nagios-plugins-1.4.12
 # ./configure
 # make
 # make install

Dar as permissões necessárias ao usuário e grupo Nagios nos diretórios dos *plugins*.

 # chown nagios.nagios /usr/local/nagios
 # chown -R nagios.nagios /usr/local/nagios/libexec

Instalando o Xinetd:

 # apt-get install xinetd

Instalar o NRPE. Até o momento da criação desse documento a versão mais nova é a 2.12. Para verificar as versões mais novas acesse o site de downloads do Nagios citado acima.

Baixar o Fonte do NRPE e descompactar:

 # cd /dados
 # wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nrpe-2.12.tar.gz

 # tar xzf nrpe-2.12.tar.gz
 # cd nrpe-2.12

Compilando e instalando o NRPE:

 # ./configure
 # make all
 # make install-plugin
 # make install-daemon
 # make install-daemon-config

Instalando o NRPE para rodar sob o xinetd:

 # make install-xinetd

Edite o arquivo /etc/xinetd.d/nrpe e adicione o endereço IP do servidor do Nagios na diretiva only_from.

DIRETIVA ORIGINAL:

only_from = 127.0.0.1

DIRETIVA MODIFICADA:

only_from = 127.0.0.1 <ip_do_nagios>

Adicione a seguinte entrada para o NRPE *daemon* em */etc/services*:

nrpe 5666/tcp # NRPE

Reiniciando o serviço do *xinetd*:

 # /etc/init.d/xinetd restart

Certifique-se se o NRPE *daemon* está rodando sob o *xinetd* corretamente:

 # netstat -at | grep nrpe

A saída do comando terá que ser semelhante a essa:

*tcp 0 0 *:nrpe *:* LISTEN*

Se a saída do comando não for essa ou houver algum erro cheque o seguinte:

Se foi adicionada a entrada NRPE no arquivo */etc/services/*;
Se a diretiva *only_from* em */etc/xinetd.d/nrpe* possui a entrada 127.0.0.1;
Se o *xinetd* está instalado e iniciado.

Caso ainda assim não funcione, verificar novamente todos os requisitos e passos já mencionados.

Checar se o NRPE está funcionando corretamente. O comando abaixo irá rodar o *check_nrpe* localmente a título de teste.

 # /usr/local/nagios/libexec/check_nrpe -H localhost

A saída do comando terá que ser semelhante a essa:

NRPE v2.12

Caso a máquina possua firewall ativado, terá que criar uma regra permitindo o acesso do *NRPE daemon* aos servidores remotos. Nesse caso a regra abaixo terá que ser adicionada ao */etc/init.d/firewall/:*

iptables -I RH-Firewall-1-INPUT -p tcp -m tcp –dport 5666 -j ACCEPT

Pronto, os plugins já estão instalados. Para customizar os comandos do NRPE edite o arquivo *nrpe.cfg em /usr/local/nagios/etc/.*

 # vi /usr/local/nagios/etc/nrpe.cfg

O próximo passo mostrará a instalação dos *plugins* em máquinas Windows.

Instalação dos plugins em máquinas Windows. Assim como nos *plugins* do Linux esses comandos deverão ser passados na máquina Windows a ser monitorada.

Primeiro baixar o *NsClient++* do endereço abaixo:

http://webftp.seduc.ce.gov.br/Nagios/NSClient++.zip

Descompactar em um diretório qualquer (exemplo C:) da máquina a ser monitorada. Retirar todos os comentários das *DLLs* na seção modules do arquivo *NSC.ini* que se encontra dentro da pasta *NSClient++* com exceção da *CheckWMI.dll* e da *RemoteConfiguration.dll*.

Em *allowed_host* na seção *Settings* retirar o comentário da linha e colocar o IP do servidor Nagios.

Exemplo: allowed_hosts=192.168.0.5/32.

Na seção *NSClient* retirar o comentário da diretiva *allowed_hosts* e colocar também o IP do servidor Nagios como no item acima.

Se houver algum tipo de firewall entre a comunicação do servidor Nagios e o host a ser monitorado será necessário liberar a porta 12489 e retirar o comentário da diretiva *port* na seção *NSClient*.

Instalar o *plugin* para rodar como serviço nas máquinas Windows que serão monitoradas. Após descompactar o arquivo baixado anteriormente, encontraremos dentro da pasta *NSClient++* um executável chamado *NSClient++*.exe.

Executar esse arquivo via linha de comando pelo prompt de comando. A linha de comando para instalar o NSClient++ como serviço via prompt de comando é a seguinte:

NSClient++.exe -install

A partir de agora ele estará instalado como serviço. Agora abra a console de serviços do Windows em "Painel de Controle" e dê um clique duplo no serviço "NSClientpp". Na aba General certifique-se de que o serviço esteja marcado como automático, se não tiver marque-o.

Na aba "*log On*" marque a opção "*Allow Service to interact with desktop*" para interagir com o desktop.

Após a configuração do serviço descrito acima iniciar com o seguinte comando no *prompt* do Windows:

 # NSClient++.exe -start

Esse comando terá que ser passado de dentro da pasta do NSClient++.

Pronto, depois desses passos o *plugin* do Nagios está instalado e iniciado na máquina Windows e pode ser monitorado os recursos locais da máquina tais como CPU, processos, memória etc.

3.5 ARQUIVOS DE CONFIGURAÇÃO DO NAGIOS

Nessa parte serão mostrados os principais arquivos de configuração do Nagios.

3.5.1 NAGIOS.CFG

O nagios.cfg é o principal arquivo de configuração do Nagios, nele se encontram todas as configurações básicas do mesmo. Nele pode-se configurar o local onde se encontram os arquivos de configuração dos servidores de rede ou qualquer outro ativo de rede gerenciável. Veja um exemplo abaixo:

cfg_file=/usr/local/nagios/etc/seduc/servidores/servidor1.cfg
cfg_file=/usr/local/nagios/etc/seduc/servidores/servidor2.cfg
cfg_file=/usr/local/nagios/etc/seduc/servidores/servidor3.cfg

Pode-se também especificar os arquivos de configuração a serem usados para funções específicas. Observar o exemplo abaixo:

cfg_file=/usr/local/nagios/etc/seduc/commands.cfg
cfg_file=/usr/local/nagios/etc/seduc/contacts.cfg
cfg_file=/usr/local/nagios/etc/seduc/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/seduc/misccommands.cfg

Essas são apenas algumas das várias funções do *nagios.cfg*. Para maiores detalhes acessar o site oficial do Nagios em:

http://www.nagios.org

3.5.2 COMMANDS.CFG

Nesse arquivo ficam as definições dos comandos a serem executados para monitoramento. Cada comando usado no parâmetro *check_command* dos *hosts*, deverá estar configurado nesse arquivo. Segue um exemplo abaixo do arquivo *commands.cfg*:

```
# Definição do comando 'check_ftp'
define command{
      command_name    check_ftp
      command_line    $USER1$/check_ftp -H $HOSTADDRESS$ $ARG1$
}

# Definição do comando 'check_http'
define command{
      command_name    check_http
      command_line    $USER1$/check_http -I $HOSTADDRESS$ $ARG1$
}

define command{
      command_name    URL_Sauweb
      command_line    $USER1$/check_http -H endereco1.dominio.com.br
}

define command{
      command_name    URL_WebFTP
      command_line    $USER1$/check_http -H endereco2.dominio.com.br
}

define command{
      command_name    Porta_SQL
      command_line    $USER1$/check_tcp -H $HOSTADDRESS$ -p 1433
}

define command{
      command_name    Porta_Oracle
      command_line    $USER1$/check_tcp -H $HOSTADDRESS$ -p 1521
}
```

3.5.3 CONTACTS.CFG

Nesse arquivo ficam os contatos cadastrados no sistema. Esses contatos serão notificados caso algum erro aconteça na rede. Exemplo:

```
define contact {
    contact_name            administrador
    alias                   Administrador do Sistema
    service_notification_period   24x7
    host_notification_period      24x8
    service_notification_options  w,u,c,r
    host_notification_options     d,u,r
    service_notification_commands notify-by-email
    host_notification_commands    host-notify-by-email
    email                   administrador@dominio.com.br
}

define contact {
    contact_name            administrador2
    alias                   Administrador do Sistema 2
    service_notification_period   24x7
    host_notification_period      24x8
    service_notification_options  w,u,c,r
    host_notification_options     d,u,r
    service_notification_commands notify-by-email
    host_notification_commands    host-notify-by-email
    email                   administrador2@dominio.com.br
}
```

Pode-se também cadastrar nesse mesmo arquivo grupos que irão receber um e-mail no caso de falha de algum host ou serviço.

```
define contactgroup{
    contactgroup_name       admins
    alias               Nagios Administradores
    members             administrador,administrador2,administrador3
}
```

```
define contactgroup{
    contactgroup_name       informatica
    alias                   Informática Administradores
    members                 administrador,administrador2
}
```

3.5.4 MISCCOMMANDS.CFG

Esse é o arquivo onde ficam os comandos de envio de notificação para os contatos cadastrados no *contacts.cfg*. Não há muita necessidade de configurá-lo, pois ele já vem pronto para ser usado. Apenas deverá, como todos os outros, ser *setado* no arquivo *nagios.cfg* para que funcione corretamente.

3.5.5 TIMEPERIODS.CFG

Nesse arquivo pode-se configurar os períodos em que os serviços serão monitorados e que será enviada notificação de falha. É muito útil para serviços que não são 24x7. Esses ficam sendo monitorados apenas no horário comercial. O *timeperiods* pode ser configurado no parâmetro *notification_period* de cada *host*.

```
define timeperiod{
    timeperiod_name         24x7
    alias                   24 Hours A Day, 7 Days A Week
    sunday                  00:00-24:00
    monday                  00:00-24:00
    tuesday                 00:00-24:00
    wednesday               00:00-24:00
    thursday                00:00-24:00
    friday                  00:00-24:00
    saturday                00:00-24:00
}

define timeperiod{
    timeperiod_name         comercial
    alias           Horario Comercial
    monday          08:00-17:00
    tuesday             08:00-17:00
    wednesday       08:00-17:00
```

thursday 08:00-17:00
friday 08:00-17:00
}