BEATRIZ DE ALBUQUERQUE

MONITORAMENTO DE REDES DE COMPUTADORES UTILIZANDO A INTEGRAÇÃO DAS FERRAMENTAS NAGIOS E CACTI

INCONFIDENTES-MG

2013

BEATRIZ DE ALBUQUERQUE

MONITORAMENTO DE REDES DE COMPUTADORES UTILIZANDO A INTEGRAÇÃO DAS FERRAMENTAS NAGIOS E CACTI

Trabalho de Conclusão de Curso apresentado como pré-requisito de conclusão do curso de Graduação Tecnológica em Redes de Computadores no Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais – Câmpus Inconfidentes, para obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: Prof. Vinícius Ferreira de Souza

INCONFIDENTES-MG

2013

BEATRIZ DE ALBUQUERQUE

MONITORAMENTO DE REDES DE COMPUTADORES UTILIZANDO A INTEGRAÇÃO DAS FERRAMENTAS NAGIOS E CACTI

Data de aprovação: _____/____/____

Orientador: Vinícius Ferreira de Souza

(IFSULDEMINAS – Câmpus Inconfidentes)

Prof.: Bruno Amarante Couto Rezende

(IFSULDEMINAS – Câmpus Inconfidentes)

Me.: Luiz Carlos Branquinho Caixeta Ferreira

(IFSULDEMINAS – Câmpus Inconfidentes)

AGRADECIMENTOS

Agradeço a Deus por ser a base nas horas difíceis, meus pais Angélica Heloisa da S. de Albuquerque e Carlos Alberto de Albuquerque, minha sogra Ana Lúcia Leite Ramos de Camargo e meu sogro Sandro Rogério de Camargo, aos amigos pelo apoio e compreensão. Agradeço meu futuro marido César Henrique de Camargo.

RESUMO

Neste trabalho será apresentada a integração das ferramentas de software livre Nagios e Cacti, que hoje são muito utilizadas no mercado por serem mais flexíveis e de código aberto,e sendo assim, o usuário administrador pode criar um ambiente da maneira que desejar. A integração foi feita utilizando os dados de saída do Nagios como forma de dados de entrada no Cacti, assim, os dados do Nagios são exibidos em forma de gráfico na ferramenta Cacti. A integração é feita através de um script que realiza a conversão dos dados do Nagios para serem lidas no Cacti. A pesquisa é baseada em livros e artigos com informações sobre as ferramentas, o funcionamento das mesmas, e como são desenvolvidas. Para a conclusão do projeto será feito um trabalho prático implementando a integração.

ABSTRACT

In this work will be approached the integrarion of free softwares tools Nagios and Cacti, which are the most used in the market because they are more flexible and open code, this way, the administrator user is able to create a space in whatever way needed. The integration was performed using the output data of Nagios as a form of input data in Cacti, so Nagios data are displayed in graphical form on the tool Cacti. The integration process will be done through a script that performs the conversion of data from Nagios to be read in Cacti. The research used is based in books and articles with information about the tools, the way they work, how they are developed; documents and reports from users about the particularity of each tool. For the project's conclusion, will be done a practical work about the tooks integraion.

LISTA DE FIGURAS

Figura 1: Interface do programa Cacti 24
Figura 2: interface do programa Nagios 29
Figura 3: Teste de funcionamento do Nagios 44
Figura 4: Tela de instalação do Cacti 47
Figura 5: Tela de instalação do Cacti 47
Figura 6: Tela de instalação do Cacti 48
Figura 7: Tela de login do Cacti 48
Figura 8: Host em funcionamento no Cacti 49
Figura 9: Tela de criação de devices 50
Figura 10: Apresentação dos *devices* 50
Figura 11: Funcionamento do script 51
Figura 12: Tela de criação do Data Input 53
Figura 13: Criação do novo Data Source 53

SUMÁRIO

1. INTRODUÇÃO **10**
2. ESTADO DA ARTE 12
3. GERENCIAMENTO DE REDES 14
3.1 A necessidade de monitorar redes de computadores 14
3.2 O início das redes de computadores 16
3.3. O motivo para integrar as ferramentas 18
4. FERRAMENTAS UTILIZADAS 20
4.1 VirtualBox 20
4.2 Apache 21
4.3 PHP 21
4.4 NSClient++ 21
4.5 SNMP 22
4.6 RRDTOOL 22
4.7 *Linux Ubuntu* 23
4.8 CACTI 24
4.8.1 As Vantagens da Ferramenta Cacti 25
4.8.2 As Desvantagens do Cacti 26
4.8.3 Funcionamento da Ferramenta Cacti 26
4.8.3.1 Obtenção de dados 27
4.8.3.2 Armazenamento de dados 27
4.9 Nagios 28
4.9.1 As Vantagens da Ferramenta Nagios 29
4.9.2 As Desvantagens da Ferramenta Nagios: 30
4.9.3 Recursos e serviços mais utilizados oferecidos pelo software Nagios : 31
5. AMBIENTE DE TESTE 33
6. DESENVOLVIMENTO 35
6.1 Instalação das ferramentas Nagios e Cacti 36
6.1.1 Instalação da ferramenta Nagios 36
6.1.2 Adicionar um host Windows para ser monitorado 40
6.2 Instalação do Cacti 44
6.2.1 Adicionar um host windows para ser monitorado pelo Cacti 49

6.3 Integração das ferramentas 51
7. DICAS DE PROCEDIMENTO 55
CAPÍTULO 8 - CONCLUSÃO 57
8.1 Trabalhos futuros 57

1. INTRODUÇÃO

O monitoramento de redes de computadores tornou-se muito importante nos dias de hoje, pelo fato de que estar conectado é um grande investimento em qualquer circunstância. Trabalhar com tecnologia traz grandes benefícios para um bom desenvolvimento em qualquer área de atuação. Para obterem-se resultados esperados, desenvolver um monitoramento sobre as redes de computadores é muito importante, pois assim pode-se evitar futuros problemas, corrigir erros que podem ocasionar uma falha grave e ate mesmo deixar a rede inoperante. O trabalho de um administrador de redes é fazer com que os recursos computacionais estejam em pleno funcionamento e para executar essa função, usar ferramentas de gerencia de redes torna o trabalho do administrador mais prático. O monitoramento com ferramentas adequadas vai desde um simples monitoramento de um host na rede até solução de graves problemas que podem prejudicar o funcionamento da rede.

A integração consiste em enviar os dados do Nagios em formato rrd para serem feitos gráficos para serem exibidos na ferramenta Cacti. É necessário a conversão dos dados do Nagios para que o Cacti consiga ler e produzir os gráficos.

No capítulo 2 é apresentado o estado da arte, onde é feita a referencia de outros trabalhos e artigos dentro da área de monitoramento de redes com as ferramentas de software livres.

O capítulo 3 trata do gerenciamento de redes, mostrando a necessidade de monitorar as redes de computadores, o baixo custo e os benefícios de se ter um ambiente monitorado com as ferramentas Nagios e Cacti.

O capítulo 4 descreve as ferramentas utilizadas no processo de integração dos softwares Nagios e Cacti, e também mostra particularidades das ferramentas Nagios e Cacti.

O ambiente de teste é descrito no capítulo 5, onde é mostrado a como foram feitos os testes.

A forma como foi feito o trabalho é detalhada no capitulo 6, que aborda o desenvolvimento desde a instalação de cada ferramenta até a integração das mesmas.

A instalação e integração das ferramentas é trabalhosa, e por isso o capítulo 7 é dedicado a apresentar alguns problemas com suas respectivas soluções, e dicas de procedimentos para evitar problemas maiores na configuração das ferramentas.

2. ESTADO DA ARTE

Pereira e Moura (2008) afirmam que a ferramenta Cacti é considerada muito eficiente para monitoramento de redes locais, sendo uma ferramenta de que exibe informações e gráficos de forma clara, objetiva, bem organizada e estruturada, porém, o Cacti necessita de certo tempo de utilização para poder explorar de forma adequada suas funcionalidades. Ainda segundo os autores que fizeram a analise, o Cacti deixa a desejar no quesito de não informar ao administrador sobre a falta de algum serviço ou resposta por parte da rede ou do hardware que esta monitorando.

Campos (2007) fez uma avaliação sobre a ferramenta Nagios para apresentar o funcionamento da ferramenta, junto com seus componentes administrativos e benefícios para o monitoramento de redes corporativas. De acordo com a análise feita, pode se afirmar que através dos recursos oferecidos pela ferramenta Nagios é possível ter uma visão global da rede que está sendo monitorada, entretanto, a instalação da ferramenta é considerada complexa, a falta de gráficos também é um ponto negativo encontrado na avaliação da ferramenta.

Segundo Rodrigues (2010), a integração das duas ferramentas de monitoramento de software livre é uma solução eficiente e de baixo custo, e como as ferramentas Nagios e Cacti são consideradas as mais eficientes no mercado atual, fazer a integração entre elas é viável pois, além de serem as mais utilizadas para o monitoramento cada uma tem sua funcionalidade especifica. O maior benefício oferecido pela integração é que uma ferramenta é o complemento da outra.

Santos (2010) afirma que o mercado atualmente disponibiliza inúmeras soluções para ajudar os administradores de redes a garantir o bom funcionamento das mesmas. Por esse motivo, é necessário o estudo detalhado de softwares que incorporem funcionalidades que sejam fundamentais para um gerenciamento de confiança, seguro e eficiente na organização. A maioria das soluções de gerência que são de natureza proprietária, além de terem um alto custo, são complexas, muitas vezes não se adaptando agilmente às mudanças de tecnologia e de requisitos de gerência dos usuários. A flexibilidade, o baixo ou nenhum custo são apenas algumas das inúmeras vantagens que o software livre proporciona.

Koch (2008) apresenta uma proposta de solução de gerenciamento para uma rede local de computadores, a partir do gerenciamento de contabilização, descrevendo os princípios desta área funcional do gerenciamento de ferramentas. Além disso, apresenta um estudo de caso com as ferramentas Nagios e Cacti.

Majewski (2009) o autor retrata no artigo a necessidade de monitorar os equipamentos de rede. E para tornar esse gerenciamento mais fácil e ágil, existem varias ferramentas, o autor apresenta uma comparação, descritiva técnica de três sistemas: Nagios, Zabbix e Cacti.

Neto e Uchôa (2009), os autores fizeram uma analise sobre ferramentas de monitoração de servidores, serviços e ativos de rede, sendo que o objetivo principal do artigo foi o de comparar as ferramentas distribuídas livremente que atendam os quesitos de monitoração cumulativa, geração de gráficos e alertas ao administrador.

Para Souza (2009) com o crescimento das redes corporativas em pequenas empresas, uma solução viável, eficiente e de baixo custo para o monitoramento e controle do ambiente de rede, a ferramenta Nagios é uma solução, pois com ele é possível fazer monitoração de aplicações ou condições de recursos computacionais.

3. GERENCIAMENTO DE REDES

Este capítulo mostra a necessidade de monitorar redes de computadores, e aborda um pouco do início de redes de computadores

3.1 A Necessidade de Monitorar Redes de Computadores

Atualmente as empresas dependem de suas redes corporativas, que são instrumentos fundamentais para o desenvolvimento do negócio. Cada vez mais áreas diversas estão ficando dependentes de tecnologia, e junto com o crescimento da dependência tecnológica, devem aproveitar os recursos computacionais para impedir imprevistos, no funcionamento das redes de computadores.

O rápido crescimento e a proliferação de novas tecnologias têm mudado as características das redes de computadores nos últimos anos. O monitoramento, em tempo real, da infraestrutura de redes e seus ativos vêm se tornando indispensável na gestão da tecnologia da informação. Este monitoramento permite obter as informações necessárias sobre estes equipamentos de modo rápido, sintético, preciso e confiável, facilitando as tomadas de decisão do gestor no momento do planejamento, adequação e expansibilidade do parque tecnológico.

O avanço da tecnologia na sociedade trouxe grandes impactos à comunicação, redes foram surgindo para atender à demanda de comunicação das empresas e do público, o que gerou uma grande necessidade de gerência, "organizar", para atender assim os requisitos das empresas com um bom desempenho. [11]

A verificação do desempenho de serviços e a resolução de problemas diversos, como conectividade e integração de plataformas, também ocorrem mais facilmente. Segundo Menezes & Silva (1998) O gerenciamento de redes pode ser entendido como o processo de controlar uma rede de computadores de tal modo que seja possível maximizar sua eficiência e produtividade.

As ferramentas disponíveis no mercado para monitoramento de sistemas e servidores permitem realizar uma análise nos processos e seus serviços de forma a identificar o mais cedo possível qualquer falha, buscando assim uma solução do problema antes mesmo que qualquer usuário possa ter notado. O monitoramento de serviços e ativos de rede é uma técnica que busca fazer um monitoramento ostensivo para que, quando houver um problema, os administradores de rede sejam os primeiros a serem notificados [11].

Um sistema de gerenciamento consiste em hardware e software adicionais implementados nos equipamentos da rede. O software utilizado para o gerenciamento da rede é implementado em servidores, estações e processadores de comunicação. O software é instalado de maneira a ter uma visão geral da rede, como uma arquitetura unificada, com endereços e rótulos associados aos dispositivos da rede. Segundo Pereira (2001), o gerenciamento de desempenho é um conjunto de funções responsável por garantir que não ocorra insuficiência de recursos quando sua utilização se aproxima da capacidade total do sistema.

Através de um monitoramento de rede correto e contínuo, é possível prever problemas e solucionar o erro sem que prejudique o funcionamento do sistema. Um sistema de monitoramento configurado de maneira correta, evita falhas no desempenho da rede, e proporciona uma melhor qualidade de serviço, pois haje de maneira pró-ativa. A origem de problemas ocorridos é facilmente identificada com um sistema de monitoramento, fazendo com que as ações de manutenção sejam pontuais e eficientes.

A proposta deste trabalho é uma solução de baixo custo e eficaz para monitoramento redes local com ferramentas de software livre Nagios e Cacti. Fazendo a integração das ferramentas, para usufruir dos melhores recursos específicos de cada software. O gerenciamento de rede está associado ao controle de atividades e ao monitoramento do uso de recursos da rede. De forma simples, as tarefas básicas da gerência em redes são: obter informações da rede, tratar estas informações possibilitando um diagnóstico e encaminhar as soluções dos problemas. Para isso,

funções de gerência devem ser embutidas nos diversos componentes de uma rede, para que possibilitem descobrir, prever e reagir a anomalias, Duarte [5].

3.2 O Início das Redes de Computadores

Redes de computadores estabelecem uma forma padrão de interligar computadores para o compartilhamento de recursos físicos ou lógicos. Esses recursos podem ser definidos como unidades de CD-ROM, diretórios do disco rígido, impressoras, scanners, placa de fax modem entre outros.[14]

A tecnologia de rede chegou ao estágio da massificação quando os computadores começaram a se espalhar pelo mundo comercial, ao mesmo tempo em que programas complexos multiusuários começaram a serem desenvolvidos (e-mail, banco de dados, Internet). Os componentes para sua montagem (hardware, software, infraestrutura e acessórios) podem ser encontrados em qualquer loja especializada em informática, sendo esses elementos procedentes de dezenas de fabricantes. Esse processo gerou um fato interessante: baixo custo dos componentes proporcionado pela concorrência entre os fabricantes em um primeiro estágio e baixo valor final proporcionado pela concorrência entre as diversas lojas de informática. Aliada a tudo isso, a evolução tecnológica trouxe simplicidade ao processo, o que torna o trabalho técnico mais fácil e com maior número de possibilidades. No entanto, nem sempre o custo e a interoperabilidade dos equipamentos de redes estiveram à mão dos administradores de redes de forma barata e flexível. [14]

No início da concepção das redes, cada fabricante possuía a sua forma de trabalho e sua própria linha de desenvolvimento de tecnologia. Como exemplo, podemos citar a placa de rede do fabricante “x” que só poderia estar conectada a uma placa do mesmo fabricante, por um meio físico (fio) também desenvolvido por ele. [14]

Caso houvesse problemas relacionados a preços ou relacionamento entre as partes, a empresa detentora dos equipamentos não tinha como procurar outra opção. A única alternativa existente naquela época era a substituição de todo o parque de

hardware e software instalado por equipamentos de outro fabricante. Dessa forma, o problema não era resolvido, mas contornado, e os prejuízos eram grandes. [14]

A fim de resolver esta situação de incompatibilidade entre fabricantes, na década de 1970 a ISO (International Organization for Standardization) criou um padrão universal para troca de informações entre e dentro das redes e também por meio de fronteiras geográficas. Esse padrão para arquitetura de redes era o Modelo de Referência OSI, estabelecido em sete camadas, o qual incentivou a padronização de redes de comunicação e controle de processos distribuídos. O fato de estar desenhado em sete camadas se dá em virtude de o modelo da IBM, o Modelo de Referência SNA, ter essas características. A IBM no início das redes era uma das maiores empresas ligadas a essa área e uma das integrantes do processo de padronização das redes e de criação do modelo de referência OSI. [14]

Um fato importante a ser considerado quanto ao padrão OSI foi o seu longo tempo para a sua definição. Durante esse período, o Departamento de Defesa do Governo dos Estados Unidos da América (DoD – Department of Defense) desenvolveu o Modelo de Referência TCP/IP com o objetivo principal de manter conectados seus equipamentos mesmo, que apenas em parte. [14]

Esse padrão ficou conhecido como o Modelo de Referência TCP/IP estabelecido em quatro camadas. Como alguns fabricantes iniciaram o desenvolvimento de equipamentos seguindo esse padrão, quando o padrão OSI foi finalizado, muitos equipamentos já estavam funcionando no Modelo de Referência denominado TCP/IP, logo, o Modelo de Referência OSI nasceu e não se tornou um padrão da indústria de rede. As instituições acadêmicas não aceitaram substituir seus equipamentos, pois isso demandaria um alto custo e muito tempo perdido para treinamento e novas configurações. [14]

O nome TCP/IP refere-se à uma pilha de protocolos que tem como principais protocolos o TCP (Transmission Control Protocol) e o IP (Internet Protocol) além de outros protocolos conhecidos tais como ARP, RARP, UDP e ICMP. Logo não devemos confundir a pilha de protocolos TCP/IP com os protocolos TCP e o protocolo IP, que possuem características de funcionamento bem distintos um do outro. A Internet que surgiu baseada nas redes de instituições acadêmicas dos Estados Unidos é um bom exemplo de rede que utiliza a pilha de protocolos TCP/IP. [14]

Na década de 1990, com a abertura do acesso à Internet, tudo ganhou uma nova dimensão e as redes se multiplicaram de forma assustadora, já que não demorou muito para todos perceberem que ter uma rede local era a forma mais barata de conectar todos os computadores da rede à Internet. Com o crescimento dos usuários na rede, aumentou também, os problemas causados por usuários com más intenções, e na maioria das vezes a própria infraestrutura da rede, então surgem os administradores de rede, que controlam o trafego e monitoram o desempenho da rede[14].

Administrar uma rede não refere-se somente à manter seu funcionamento, mas também manter os recursos computacionais em ordem, com total funcionamento de acorda com a necessidade desejada, ter obter um melhor resultado no desempenho de uma rede está totalmente direcionado com o monitoramento.

As ferramentas Nagios e Cacti são muito utilizadas no mercado por serem consideradas as mais completas, por isso, muitos administradores de rede fazem o uso delas para monitoramento.[3]

Além do mercado exigir um monitoramento correto, que prevê problemas, e encontra a origem do erro para ser resolvido, o custo também é um dos fatores fundamentais para a implementação de um sistema de monitoramento, por isso, a integração das ferramentas será de grande benefício para essa área de atuação.

3.3. O Motivo para Integrar as Ferramentas

O mercado está cada vez mais exigente em relação ao desempenho, performance, disponibilidades e um ambiente seguro, com menor custo possível na área de tecnologia da informação.

Os profissionais desta área têm a necessidade de garantir um bom monitoramento para evitar erros desnecessários que podem atrapalhar uma determinada produção, ou até mesmo deixar um setor totalmente inoperante, já que diversas áreas em diversos tipos diferentes de mercado se tornam dependente da TI (Tecnologia da Informação) uma produção mais eficaz.

Muitas vezes a TI é o suporte para garantir o sucesso de uma organização, e as redes de computadores estão se tornando maiores e mais complexas, transportando dados,vídeo e voz, um erro de configuração ou na falha da segurança das informação pode prejudicar o desempenho, tendo como retorno uma situação desagradável para a instituição.

Ter um monitoramento completo e detalhado de uma rede e de seus componentes é uma tarefa difícil para um administrador, pois a quantidade de dados e informações a serem analisadas é grande, e também se usa muito tempo para fazer uma minuciosa analise de todas as configurações.

Por isso, os profissionais que trabalham na área de monitoramento, devem utilizar ferramentas que ajudam ao máximo a solucionar problemas gerados no ambiente, essas ferramentas devem ser de fácil entendimento para o administrador e também que mostre o estado real da rede e de cada componente monitorado.

4. FERRAMENTAS UTILIZADAS

Para o trabalho foram utilizadas algumas ferramentas, este capítulo detalha melhor cada uma das ferramentas usadas para a integração do Nagios e o Cacti.

4.1 VirtualBox

VirtualBox é um software de virtualização para arquitetura x86 desenvolvido pela empresa *Innotek GmbH*, com sede na Alemanha. Desde janeiro de 2007 possui uma versão que é open source de licença GNU GPL. [18]

Essa ferramenta utiliza a técnica da virtualização total, emulando componentes chaves do hardware. Com isso, não há necessidade de que os sistemas operacionais convidados sejam modificados para que executem em uma máquina virtual.[18]

No software, os discos são emulados num recipiente especial chamado Virtual Disk Imagem (arquivos *VDI*), o qual até o momento é incompatível com formatos usados por outras soluções. O *VirtualBox* possui uma funcionalidade que pode conectar dispositivos *iSCSI* e usá-los como discos virtuais [18].

4.2 Apache

É um software livre para servidores http de código aberto para plataformas Unix,são os mais utilizados na internet.[1]

Para se ter o acesso a qualquer site, precisa-se de um servidor que é responsável por disponibilizar as paginas de internet entre outros recursos, ou seja., é um servidor web que processa informações HTTP (***H****yper-****T****ext* ***T****ransfer* ***P****rotocol*), que é o protocolo padrão da web [1] .

O Apache é um dos servidores web mais utilizados,pois tem compatibilidade com diversas plataformas, e por ser muito conhecido.[1]

4.3 PHP

É uma linguagem de programação interpretada, originalmente desenvolvida para criação de páginas Web dinâmica, nos casos das ferramentas requeridas, servirá para realizar uma interpretação extra dos dados das ferramentas (Nagios, Cacti e NagiosQL) via interface gráfica [13].

4.4 NSClient++

São *plugins* utilizado para fazer a comunicação e monitoração de maquinas Windows,utilizando servidores cliente Linux. É necessário a instalação da versão compatível com a versão do Windows utilizada, caso seja instalado uma versão diferente da compatível,ocorrerá erro quando for feito o monitoramento deste host. [4]

4.5 SNMP

O protocolo *SNMP (Simple Network Management Protocol)* é um protocolo da camada de aplicação criado para transportar informações de gerência de rede entre os dispositivos gerenciados e os sistemas de gestão de redes, ele possibilita que administradores de rede gerenciem o desempenho da uma rede monitorando interfaces, processadores, memórias de equipamentos como roteadores, *switches*, dispositivos *wireless* e servidores. [22].

Os administradores de redes conseguem visualizar o status atual da rede, manter um histórico de atividades, bem como receber avisos de forma imediata para ajudar na resolução de problemas. [22].

A primeira versão do SNMP foi adotada como padrão em 1989 e quatro anos depois teve uma atualização para a versão 2. O SNMPv2 (versão 2) fornece gerenciamento de rede centralizado e distribuído incluindo aprimoramentos na sua estrutura e gerenciamento. Ambas as versões 1 e 2 do SNMP não são seguras. [22].

O SNMPv3 (versão 3), foi criado para solucionar as questões de segurança, fornecendo acesso seguro às informações de gerenciamento por meio de autenticação e criptografia de pacotes. [22].

Embora os recursos do SNMP sejam potentes para lidar com questões que envolvem o gerenciamento de redes heterogêneas o SNMP é um protocolo simples, com finalidade única: Transportar as informações de gerenciamento [22].

4.6 RRDTOOL

RRD é a sigla para *Round Robin Database*. O RRD é um sistema para armazenar e mostrar dados em série obtidos em um determinado período de tempo (banda de rede, temperatura da máquina, etc). Os dados são armazenados de maneira

bastante compacta e não aumentam com o tempo (por isso que o banco é dito "circular") [4].

A ferramenta RRDTOOL permite ter um bando de dados, onde pode-se criar varias filas, porém com precisões diferentes. Um dado inserido recentemente possui uma precisão maior, mas, com o passar do tempo, ele acaba convergindo para uma fila de menor precisão. O RRDtool também permite que sejam gerados gráficos a partir dos dados armazenados. Esses gráficos são bastante dinâmicos, sendo possível até mesmo incluir várias entradas de bancos de dados diferentes em um único gráfico. [4].

Uma das grandes vantagens do RRDtool está nas interfaces de programação. Ao mesmo tempo o RRDtool possui interfaces para as linguagens C/C++, *Perl* e Tcl, além de permitir que todas as funções sejam realizadas através da linha de comando de um *shell*, fazendo com que praticamente todas as linguagens capazes de fazer chamadas do externas através de pipes sejam capazes de utilizar as suas facilidades. [4].

4.7 *Linux Ubuntu*

Esta distribuição existe desde 2004, é uma distribuição baseada no Debian, também utilizando o gerenciador de pacotes APT, tem tido grande destaque no mercado Linux nos últimos três anos, apresentando grandes facilidades na sua instalação e uso para desktops, as versões do Ubuntu são lançadas a cada seis meses sempre no mês quatro e no mês dez. O número das versões obedece a este padrão começando na versão 4.10(ano 2004, mês 10), 5.04 (ano 2005, mês 04) e assim sucessivamente. O Ubuntu costuma trazer inovações interessantes aos usuários de desktop a cada nova versão, sendo considero o Linux “mais fácil de usar”, devido as suas ferramentas intuitivas e bem construídas graficamente [16].

4.8 CACTI

O Cacti, é um *frontend* para o *RRDTOOL* (*Round Robin Database*) desenvolvido em *PHP* com utilização do *SGBD MySQL*, ele utiliza o *RRDTool* para a confecção de arquivos de dados e geração de gráficos informativos [15]. O Cacti foi desenvolvido inicialmente por Ian Berry, a última versão estável é na versão 0.8.8a [2]. A Figura 1 mostra a tela inicial do cacti.

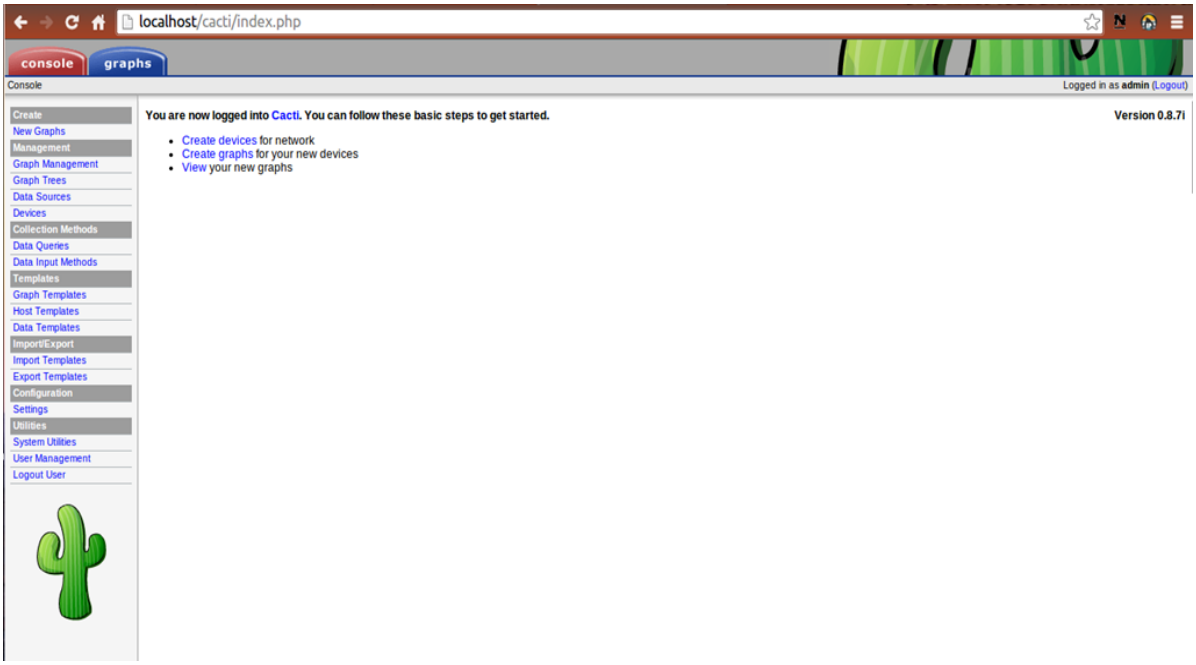

Figura 1: Interface do programa Cacti. Fonte: Cacti

O Cacti apresenta um número ilimitado de itens visuais que pode ser definido para cada gráfico, agrupamento automático de dados possibilitando a continuidade de informação no mesmo gráfico, com legendas claras o que gera conforto na visualização do monitoramento, todos dados é permitido sua manipulação utilizando funções matemáticas do RRDtools, o que o torna uma ferramenta eficiente. Também o fato de permitir criar usuários e atribuir níveis de permissão por gráficos diferentes para

cada um e cada usuário é permitido a variação de suas visualizações o torna mais atraente [12].

Seu desempenho é muito interessante, pois permite recolher dados locais e remotamente, arquivos com mais de uma fonte de dados podem ser armazenados e disponibilizados na forma de gráficos em tempo real, com a possibilidade de definir scripts personalizados para coleta e recuperação de informações onde cada um pode conter argumentos para cada fonte de dados. Sua opção *Árvore* permite a apresentação de gráficos de uma maneira hierárquica deixando de maneira ágil e fácil o gerenciamento e organização de um grande número deles. Também permiti visualizar os usuários a escolher as áreas que deseja visualizar em gráficos menores [12].

A aplicação utiliza-se de *scripts* em *Bash*, *Perl*, XML, dentre outros para colher dados localmente, ou remotamente utilizando SNMP (*Simple Network Management Protocol*). O RRDTool, por sua vez, foi desenvolvido por Tobias Oetiker e constitui um pacote de ferramentas para gerar e interpretar informações em arquivos de dados, assim como a geração de gráficos estatísticos com base nesses arquivos [15].

Consultar informações em elementos de redes e/ou programas que suportam tal protocolo, esta ferramenta se mostra de extrema importância no gerenciamento de corporações onde se deseja monitorar de forma eficiente todos os tipos de processos relativos a rede e também o desempenho do equipamento, no caso seu hardware, que faz parte da interface da rede.[15]

Em qualquer plataforma na qual está sendo executado pode desempenhar a mesma tarefa de forma eficiente, o que lhe dá segurança e portabilidade, desta forma qualquer ambiente pequeno ou grande se torna um atrativo para a utilização do Cacti [12].

4.8.1 As Vantagens da Ferramenta Cacti

A ferramenta possui as seguintes vantagens: [14]

- Fácil acesso, via browser;
- Tem um sistema de permissão que autoriza apenas usuários de um grupo,ou apenas o usuários administrador, a visualizar os gráficos de informações;
- Por ser de código aberto permite a instalação de vários *plugins* de acordo com a necessidade do administrador;
- O custo, por ser um software livre tem baixo custo, apenas o custo do equipamento que será usado na instalação da ferramenta(hardware).

4.8.2 As Desvantagens do Cacti

A ferramenta cacti apresenta algumas desvantagens: [14]

- O intervalo padrão das verificações é igual a 5 minutos, e quando modificado pode apresentar dados incoerentes;
- São necessárias três verificações para que o administrador possa começar a visualizar os dados;
- A interface web é confusa no que se refere a algumas funções;
- Não realiza o resumo de múltiplos recursos, o que torna confuso o acompanhamento de clusters.

4.8.3 Funcionamento da Ferramenta Cacti

O funcionamento da ferramenta Cacti se divide em duas partes, a obtenção de dados, e o Armazenamento de dados.

4.8.3.1 Obtenção de Dados

O Cacti obtém dados utilizando um *"poller"*, ou seja, uma aplicação executada de acordo com um período de tempo e é registrada como um serviço que depende da plataforma utilizada. Uma estrutura de redes contém diferentes dispositivos como roteadores, switches, impressoras, servidores, além de outros equipamentos como *firewals* e *IPS's* (*Intrusion Prevention Systems*). Para obter dados destes dispositivos remotos, o sistema utiliza SNMP, ou seja, dispositivos com funcionalidades SNMP podem ser monitorados pelo Cacti [14].

4.8.3.2 Armazenamento de Dados

Há várias opções no que diz respeito ao armazenamento de dados com o Cacti, como bases de dados SQL e arquivos de texto. No entanto, o sistema utiliza a ferramenta RRDTool, a qual se discute nas próximas seções deste trabalho. Basicamente, o padrão RRD armazena e exibe as informações obtidas através do SNMP e as consolida utilizando funções como AVERAGE (Média), MINIMUM (Mínimo), MAXIMUM (Máximo), entre outras. Isto faz com o que este sistema seja muito rápido e utilize o mínimo de espaço em disco. Apresentação de dados - A função mais importante do Cacti e da ferramenta RRDTool é a construção de gráficos. As funções integradas de ambas as ferramentas possibilitam a criação de gráficos com base em um único item, ou vários itens, assim como legendas, máximo, média etc [3].

De acordo com o *site* oficial do Cacti [21], os requerimentos necessários para a instalação e utilização da ferramenta são:

- Um servidor com sistema operacional Linux ou variação Unix;
- Acesso à rede;
- RRDTool 1.0.49 or 1.2.x ou superior;

- MySQL 4.1.x or 5.x ou superior;
- PHP 4.3. ou superior, 5.x ou superior para funções avançadas;
- Um *Web Server* como Apache ou IIS.

4.9 Nagios

Como o Nagios é uma ferramenta de software livre, pode ser desenvolvida pelo próprio usuário, e tem como função informar ao usuário ou a um grupo de usuários cadastrados no Nagios para receber informações sobre o estado da rede e os hosts específicos cadastrados. Essas informações sobre o estado da rede ou de hosts podem ser recebidas pelo usuário de destino através de *e-mail*, *SMS (Short Message Service)* e entre outros métodos definidos.

O Nagios constitui-se em um software para monitoramento de redes, que podem possuir infraestrutura de WAN, LAN e MAN. Possui uma GUI (Graphical User Interface). Criado originalmente com o nome Netsaint, ele opera sob a plataforma GNU/LINUX e é distribuído sob os termos da lei de copyleft contidos na licença GNU GPL. Sua aplicação é designada a redes de grande porte, porém seu desempenho é excelente em redes de pequeno porte. Foi desenvolvido por Ethan Galstad, com a função de verificar constantemente a disponibilidade do serviço, local ou remoto e avisar via e-mail ou celular alertas sobre problemas ocorridos na rede [8]. A figura 2, mostra a tela inicial do Nagios.

Figura 2: interface do programa Nagios. Fonte: autor.

Machado (2013) destaca que o fato do Nagios ser um programa Open Source resguarda a grande vantagem de possuir diversos colaboradores espalhados por todo o mundo adicionando a esta ferramenta novas sugestões, correções de bugs, desenvolvimento de interface web, tradução de documentação e novas funcionalidades na forma de *plugins*, já que são considerados complementos do Nagios, que o usuário administrador pode configurar de acordo com sua necessidade para obter melhor desempenho no monitoramento.

Através dos arquivos de configuração, o administrador da rede poderá determinar quais serviços ou equipamentos serão monitorados, alertando assim sua disponibilidade (quando eles caírem ou retornarem). Além disso, permite o monitoramento de ativos de rede com suporte a protocolos SNMP, que é caracterizado como o principal agente de troca de informações entre o Nagios e seus hosts monitorados [14].

4.9.1 As Vantagens da Ferramenta Nagios

O Nagios apresenta as seguintes vantagens: [14]

- É um dos softwares de monitoração de rede mais utilizado;
- Assim como o Cacti, tem código aberto, pode ser alterado de acordo com a necessidade do usuário administrador;
- Tem fácil acesso, também via browser, é uma ferramenta fácil de mexer;
- Gera alarmes e avisos para usuários cadastrados;
- Baixo custo é baixo.

4.9.2 As Desvantagens da Ferramenta Nagios:

O programa Nagios possui as desvantagens: [14]

- O foco do sistema é a verificação de disponibilidade de hosts e serviços, portanto, o Nagios não gera gráficos. Faz-se necessário o uso de uma segunda ferramenta;
- A configuração através de arquivos de texto é complexa e facilita a ocorrência de erros;
- Muitas vezes os plugins desenvolvidos por usuários não são bem programados e apresentam falhas;
- O entendimento da função de cada plugin consome grande quantidade de tempo, principalmente de usuários iniciantes. Por exemplo: check_http80!win2003k!do!10!30!body;
- Algumas verificações são executadas no servidor Nagios, (a maioria é executada através dos addons NRPE e NSClient++) o que resulta em uma carga muito maior sobre o equipamento, principalmente quando muitos hosts e serviços são monitorados [14].

4.9.3 Recursos e serviços mais utilizados oferecidos pelo software Nagios :

Os recursos mais utilizados para monitorar uma rede com o Nagios são: [25]

- Monitoração de serviços de rede como HTTP, SMTP, SSH, Telnet, etc;
- Monitoração dos recursos dos servidores, como espaço em disco, carga de processamento e etc;
- Monitoramento de Computadores: verificando carga em processador, uso de disco ou memória, entre outros;
- Apresentação de notificações (em tempo real) em caso de falhas na rede através de e-mail, sms, celular;
- Interface Web opcional para visualizar todo o processo de monitoramento e assim o administrador pode identificar de maneira mais fácil os problemas presentes na rede;
- Desenho simples de plugins que permitem aos administradores desenvolverem os seus próprios verificadores de serviços;
- Verificadores de serviços em paralelo;
- Definição de hierarquia entre hosts de redes, permitindo a detecção e distinção dos hosts abaixo daqueles não alcançáveis;
- Definição de eventos para serem executados durante os serviços ou eventos de hosts para resolução de problemas;
- Uso de tratadores de eventos para corrigir ou resolver automaticamente um problema. Por exemplo: reiniciar o servidor web caso ele não esteja respondendo;
- Possibilita o desenvolvimento de plugins customizados;

- Rotatividade automática de logs.

5. AMBIENTE DE TESTE

Para um ambiente de teste foram utilizados dois hosts, sendo um Linux Ubuntu 12.04 e o outro com Windows 7 Home Premium. No host Linux Ubuntu 12.04 foram instaladas Nagios, Cacti, Msql e todos os outros serviços descritos anteriormente. No host Windows foi instalado o plugin NSClient ++ e o protocolo *Simple Network Management Protocol* (SNMP), o plugin faz com que o host Windows aceite as mensagens de SNMP.

A rede foi montada utilizando um dispositivo wireless, Segundo Torres, as redes sem fio são baseadas no padrão IEEE (*Institute of Electrical and Electronics Engineers*) 802.11 e consistem em estações de comunicação com rádios que transmitem em 2.4GHz ou 5.8GHz de banda. O IEEE 802.11 é o padrão que regula as normas de uso da tecnologia *wireless* [21].

Em todos os testes realizados para configurar e utilizar as ferramentas manteve-se a mesma configuração. Não foi realizado nenhum tipo de virtualização, para não existir influência de atraso (*delay)* nos programas Nagios e Cacti, como objetivo é a integração dos programas, o mínimo atraso na operação é muito importante, pois o monitoramento pode-se tornar falho.

O Nagios abrange uma arquitetura servidor/cliente, sendo executado em um servidor específico e seus *plugins*, que lhe enviam as informações, nos servidores remotos que precisam ser monitorados [9]. Segundo Vaz (2010), o Nagios trabalha com dois tipos de checagem, sendo elas o ativo, onde o processo de checagem é iniciado pelo próprio Nagios, e o passivo, que compreende o uso de arquivos de comandos

externos para o envio dos resultados para o Nagios. Após todas as configurações feitas, foi adicionado o host Windows para ser monitorado pela ferramenta Nagios [20].

Para o host Windows ser monitorado pela ferramenta Cacti, foi habilitado no próprio host o protocolo SNMP.

A ferramenta Cacti foi configurada na versão Cacti-0.8.8 a, Cacti é traduzida como uma ferramenta que busca e exibe em forma de gráficos as informações de uma rede de computadores, também é definido como uma solução completa de gráficos de rede, recolhendo e exibindo informações sobre seu estado [21].

Para a configuração do Cacti foi executada uma janela do terminal, logo informado o comando para instalação (Sudo apt-get install apache2 mysql-sever php5 php5-common php5-cgi php5-cli php5-mysql php5-gd snmp rrdtool cacti), o qual depois de concluído nos obriga a configurar suas ferramentas de apoio do software, são elas o banco de dados Mysql e o servidor Web (Apache2). Para a execução das duas ferramentas, Nagios e Cacti, é necessário um browser, neste caso, optou-se pelo navegador Mozilla Firefox. E assim, quando iniciado o navegador, HTTP: //localhost/cacti/, é iniciada a primeira tela de configuração do *login* do Cacti [12].

Depois de ser autenticado com *login* e senha, todas as funcionalidades do software são disponibilizadas. Neste ponto, é necessário fazer configurações relacionadas à rede onde estão conectados os equipamentos.

O Cacti apresenta um número ilimitado de itens visuais que pode ser definido para cada gráfico, agrupamento automático de dados possibilitando a continuidade de informação no mesmo gráfico, com legendas claras o que gera conforto na visualização do monitoramento, todos dados é permitido sua manipulação utilizando funções matemáticas do RRDtools, o que o torna uma ferramenta eficiente [12].

Para o monitoramento do Cacti ou do Nagios em hosts com o sistema operacional Windows, é preciso ativar os recursos do sistema,para a habilitar o serviço SNMP, que por padrão vem desabilitado,caso não habilite este recurso,o monitoramento não poderá ocorrer de forma adequada.

6. DESENVOLVIMENTO

As duas ferramentas, Nagios e Cacti, fazem o uso de *plugins*, e é através dos *plugins* que são feitas as checagens dos serviços do Nagios. Esses *Plugins* são em geral pequenos scripts, shell, Perl ou C que são executados pelos Softwares (Nagios e Cacti) para obter resultados e exibir na tela, notificar o responsável ou executar algum procedimento[4].

Protocolo SNMP (*Simple Network Management Protocol*) é utilizado para obter informações através de agentes espalhados em uma rede TCP/IP (*Transmission Control Protocol* / Internet Protocol).É um protocolo de gerência definido em nível de aplicação.

Os dados são obtidos através de requisições requisições de um gerente a um ou mais agentes utilizando os serviços do protocolo de transporte UDP (*User Datagram Protocol*) para enviar e receber suas mensagens através da rede [4].

A utilização de *plugins* em ambos os softwares é muito importante para fazer o monitoramento desejado, o profissional que gerencia a rede,instala os *plugins* de acordo com o que deseja monitorar, essa opção de instalar ou não os *plugins*, torna o Nagios e o Cacti bem flexíveis, porém o uso desses programas de monitoramento é indicado apenas a redes de pequena ou médio porte.

6.1 Instalação das ferramentas Nagios e Cacti

Neste item é apresentado os passos para a instalação das ferramentas, e configurações das ferramentas.

6.1.1 Instalação da ferramenta Nagios

Primeiramente, foi instalado o Nagios e o Cacti, a instalação correta de ambos os programas é fundamental para o funcionamento dos mesmos, e da própria integração.

Antes da instalação, é necessário atualizar o sistema operacional, tanto para o nagios, quanto par ao cacti, no exemplo os comandos para atualizar o linux ubuntu.

sudo apt-get update

sudo apt-get upgrade -y

1º passo. Instalar as dependências do Nagios, que envolve o apache, php, entre outras dependências.

sudo apt-get install build-essential apache2 php5-gd wget libgd2-xpm libgd2-xpm-dev libapache2-mod-php5 libssl-dev

2º passo. Criar grupo e usuario do nagios.

sudo mkdir -p /etc/nagios /var/nagios

sudo groupadd --system --gid 9000 nagios

sudo groupadd --system --gid 9001 nagcmd

sudo adduser --system --gid 9000 --home /usr/local/nagios nagios

sudo usermod --groups nagcmd nagios

sudo usermod --append --groups nagcmd www-data

sudo chown nagios:nagios /usr/local/nagios /etc/nagios /var/nagios

3º passo. Baixar o arquivo fonte do nagios, e também os plugins do programa, sem estes plugins o nagios não funciona corretamente**.**

cd /usr/local/src/

wget http://.sourceforge.net/projects/nagios/files/nagios-3.x/nagios-3.4.4/nagios-3.4.4.tar.gz

wget http://sourceforge.net/projects/nagiosplug/files/nagiosplug/1.4.16/nagios-plugins-1.4.16.tar.gz

4º passo. Extrair, compilar e instalar o nagios 3.4.4

sudo tar -xzvf /usr/local/src/nagios-3.4.4.tar.gz

cd /usr/local/src/nagios

sudo ./configure --sysconfdir=/etc/nagios --localstatedir=/var/nagios --prefix=/usr/local/nagios --with-nagios-user=nagios --with-nagios-group=nagios --with-command-group=nagcmd --with-openssl=/usr/bin/openssl --enable-perl-modules --with-mail=/usr/bin/sendemail

sudo make all

sudo make install

sudo make install-init

sudo make install-config

sudo make install-commandmode

A tabela 01, apresenta informações dos arquivos de configuração do Nagios.

Tabela 01 – Arquivos de configurações do Nagios.

Arquivo	Função
Nagios.cfg	Arquivo mestre responsável por sincronizar os outros arquivos.
Cgi.cfg	Arquivos de configuração dos programas “cgi`s”.
Host.cfg	Contém informações dos hosts a serem monitorados.

Hostgroups.cfg	Contém informações dos hosts separados por grupos.
Contacts.cfg	Contém os contatos de notificação em caso de problemas.
Contactsgroups.cfg	Contém os contatos separados por grupos
Services.cfg	Contém os serviços que deverão ser monitorados.
Timeperiods.cfg	Contém informações de períodos de monitoramentos.
Commands.cfg	Contém os comandos que devem ser executados pelo Nagios.
Templats.cfg	Contém os exemplos de configuração dos arquivos.

Fonte: Autor

5º passo. Este passo não é obrigatório, porém é aqui que onde se configura o e-mail, para onde é enviado os alertas que o Nagios emite. Edite o arquivo /etc/objetos/contacts.cfg para alterar o endereço de e-mail que está associado com nagiosadmin, e então coloque no contato o e-mail em que deseja receber os alertas.

sudo nano /etc/objects/contacts.cfg

Exemplo:

define contact{

contact_name nagiosadmin ;

use generic-contact ;

alias Ubuntu Precise ;

e-mail admin@gmail.com ;

}

6º passo. Edite o arquivo */etc/nagios/objects/commands.cfg* para ficar correto de acordo com o que foi configurado no passo anterior.

sudo nano /etc/nagios/objects/commands.cfg

define command{

command_name notify-host-by-email

command_line /usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type:$NOTIFICATIONTYPE$\nHost:$HOSTNAME$\nState: $HOSTSTATE$\nAddress:$HOSTADDRESS$\nInfo: $HOSTOUTPUT$\n\nDate/Time: $LONGDATETIME$\n" | /usr/bin/sendemail -s srv-mail:25 -f "admin <admin@ubuntuprecise.net>" -t $CONTACTEMAIL$ -u "** $NOTIFICATIONTYPE$ Host Alert: $HOSTNAME$ is $HOSTSTATE$ **"

}

define command{

command_name notify-service-by-email

command_line /usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type:$NOTIFICATIONTYPE$\n\nService:$SERVICEDESC$\nHost: $HOSTALIAS$\nAddress:$HOSTADDRESS$\nState: $SERVICESTATE$\n\nDate/Time:$LONGDATETIME$\n\nAdditional Info:\n\n$SERVICEOUTPUT$" | /usr/bin/sendemail -s srv-mail:25 -f "admin <admin@ubuntuprecise.net>" -t $CONTACTEMAIL$ -u "** $NOTIFICATIONTYPE$ Service Alert: $HOSTALIAS$/$SERVICEDESC$ is $SERVICESTATE$ **"

}

7º passo. Configurar o Nagios para acessar na interface web:

instalar o arquivo de configuração web na pasta do *apache:*

cd /usr/local/src/nagios

sudo make install-webconf

Criar senha para nagiosadmin conta para entrar na interface web do Nagios. Essa senha será utilizada no acesso ao programa.

sudo htpasswd -c /etc/nagios/htpasswd.users nagiosadmin

sudo /etc/init.d/apache2 reload

edite o arquivo /etc/apache2/apache2.conf

sudo nano /etc/apache2/apache2.conf

e adicione a seguinte linha:

DirectoryIndex index.html index.php index.cgi

8º passo. O próximo comando é para verificar se o arquivo de configuração do nagios, possui algum erro:

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

9º passo. Extrair, compilar e instalar os Plugins do nagios:

cd /usr/local/src

wget http://prdownloads.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.16.tar.gz

sudo tar -zxvf /usr/local/src/nagios-plugins-1.4.16.tar.gz

cd /usr/local/src/nagios-plugins-1.4.16

sudo ./configure --sysconfdir=/etc/nagios --localstatedir=/var/nagios --with-nagios-user=nagios --with-nagios-group=nagios

sudo make

sudo make install

10º passo. Iniciar o Nagios para iniciar junto com o sistema:

sudo /usr/sbin/update-rc.d -f nagios defaults 99

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

sudo /etc/init.d/nagios restart

Se toda a configuração feita estiver correta, já é possível acessar o Nagios pela interface web, acesse por:

http://localhost/nagios/

6.1.2 Adicionar um host Windows para ser monitorado

Esta etapa mostra um exemplo de host Windows para ser monitorado pelo Nagios, o exemplo também pode ser utilizado em outros host ou servidores Windows, para monitorar um host ou servidor, para adicionar no nagios sistemas Linux pode-se usar o modelo que fica no /usr/local/nagios/etc/objects no arquivo localhost.cfg.

Características da máquina a ser monitorada:

S.O: Windows XP SP3

IP: 192.168.0.250

Hostname: Winxp

Serviços a serem monitorados: *Ping, CPU Load, Memory Usage, Uptime, Disk Space*

Entrar no diretório onde o Nagios armazena os hosts que serão monitorados:

cd /usr/local/nagios/etc/objects

Dentro desse diretório, criar e editar um arquivo chamado Windows.cfg:

nano Windows.cfg

Adicionar informações da máquina no arquivo:

define host {

use windows-server

host_name Winxp

alias Winxp

address 192.168.0.250

}

onde:

- Define host - Indica que será aberta a sessão de configuração de uma máquina (host).
- Use Template - Que será utilizado (referenciado no arquivo templates.cfg).
- Host_name - Nome da máquina cliente (hostname).
- Alias - Apelido para máquina cliente.
- Address - Endereço IP da máquina cliente.

define service {

use generic-service

```
host_name Winxp
service_description PING
check_command check_ping!100.0,20%!500.0,60%
}
define service {
use generic-service
host_name Winxp
service_description UPTIME
check_command check_nt!UPTIME
}
define service{
use generic-service
host_name Winxp
service_description CPU Load
check_command check_nt!CPULOAD!-l 5,80,90
}
define service{
use generic-service
host_name Winxp
service_description Memory Usage
check_command check_nt!MEMUSE!-w 80 -c 90
}
define service{
use generic-service
host_name Winxp
service_description C:\ Drive Space
check_command check_nt!USEDDISKSPACE!-l c -w 80 -c 90
```

}

onde:

* Define service - Indica que será aberta a sessão de configuração de um serviço (service).

* Use Template que sera utilizado (referenciado no arquivo templates.cfg).

* host_name - Nome da máquina cliente (hostname).

* service_description - Breve descrição do serviço (aparecerá na tela de monitoramento como o nome do serviço).

* check_command - Nome do Comando utilizado para realizar a checagem, localizado no arquivo commands.cfg.

Agora, é necessário referenciar o arquivo Windows.cfg ao Nagios:

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

Acrescente no arquivo a seguinte linha que especifica a origem do arquivo que criamos anteriormente:

cfg_file=/usr/local/nagios/etc/objects/Windows.cfg

Foi feito um teste com o Nagios, onde o host windows foi configurado para ser monitorado pele ferramenta. A Figura 3 mostra que o host windows está up, ou seja, esta sendo monitorado pelo Nagios.

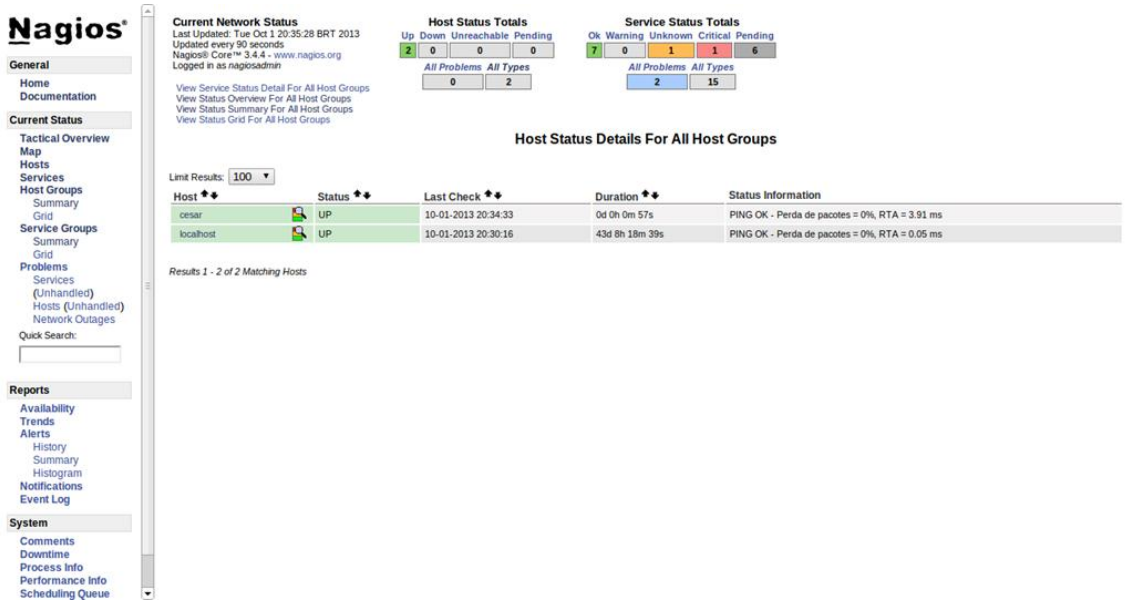

Figura 3: Teste de funcionamento do Nagios. Fonte:Nagios

6.2 Instalação do Cacti

Para a instalção do cacti, é necessários os seguintes passos:

1º passo. Instalar as dependências do Cacti

apt-get install mysql-server php5-mysql php5-gd snmp rrdtool

2º passo. É fazer a configuração do banco de dados,

Conecte ao banco de dados Mysql, use a opção -p caso tenha defenido uma senha para o usuário root:

sudo mysql -u root -p

Caso tenha definido uma senha para o usuário root, digite a senha: Enter password:****

Caso tenha definido uma senha para o usuário root, digite a senha: Enter password:****

Crie um banco de dados:

mysql> create database bancocacti;

Crie um usuário para o bancocacti:

mysql> grant all on bancocacti.*to usuariocacti;
Este comando diz que o usuário do bancocacti é o root:
mysql> grant all on bancocacti.*to usuariocacti@localhost;
Atribua uma senha ao usuariocacti:
mysql> set password for usuariocacti@localhost=password('1234');
Atribuia privilégios:
mysql> flush privileges;
Saia do banco:
mysql> exit

3º passo. É fazer o download do Cacti em:
http://www.cacti.net/downloads/cacti-0.8.7d.tar.gz
Execute o comando para descompactar o arquivo:
sudo tar -zxvf /home/usuario/Área\ de\ Trabalho/cacti-0.8.7d.tar.gz
Entre na pasta /var/www/ com o comando:
cd /var/www/
Crie uma pasta com o nome cacti:
sudo mkdir cacti

Copie o conteúdo da pasta descompactada para a pasta /var/www/cacti/:
sudo cp -r /home/usuario/Área\ de\ Trabalho/cacti-0.8.7d/* /var/www/cacti/
Execute o seguinte comando, importando a estrutura do banco de dados cacti, a senha é a mesma do usuariocacti:
sudo mysql --user=usuariocacti --password="1234" bancocacti < cacti.sql

Entre na pasta cacti com o comando:
cd cacti/
Mude o dono do arquivo:
sudo chown -R usuario rra/ log/

4º passo. É configurar o Cacti editando o arquivo config.php:
sudo editor /www/cacti/include/config.php
Configure conforme os parâmetros definidos:
$database_default = "bancocacti";

$database_hostname = "localhost";
$database_username = "usuariocacti";
$database_password = "1234";

Pressione Ctrl+o para salvar e Ctrl+x para sair:
Digite o seguinte comando:
sudo crontab –e
Adicione a seguinte linha, acrescentando o nome do usuário e caminho até o arquivo poller.php:
*/5 * * * * usuariocacti php /var/www/cacti/poller.php > /dev/null 2>&1

Reinicie o apache e o mysql:
sudo /etc/init.d/apache2 restart
sudo /etc/init.d/mysql restart

Acesse a página do Cacti:http://127.0.0.1/cacti

Na 1º página serão exibidas algumas informações sobre o Cacti, conforme a Figura 4.

Clique em Next.

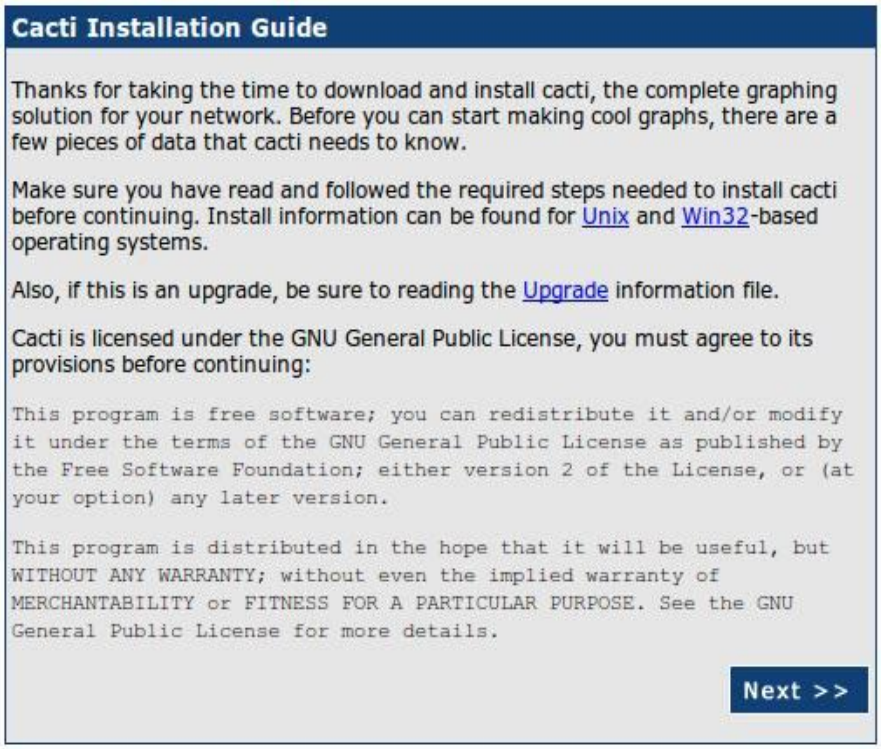

Figura 4 Tela de instalação do Cacti. Fonte:Cacti

Na 2º página pede se é para realizar uma nova instalação ou um upgrade, também mostra algumas informações de acordo com a figura 5, caso essas informações estejam erradas, pode-se corrigi-las editando o "config.php":

Default (New Install) ->

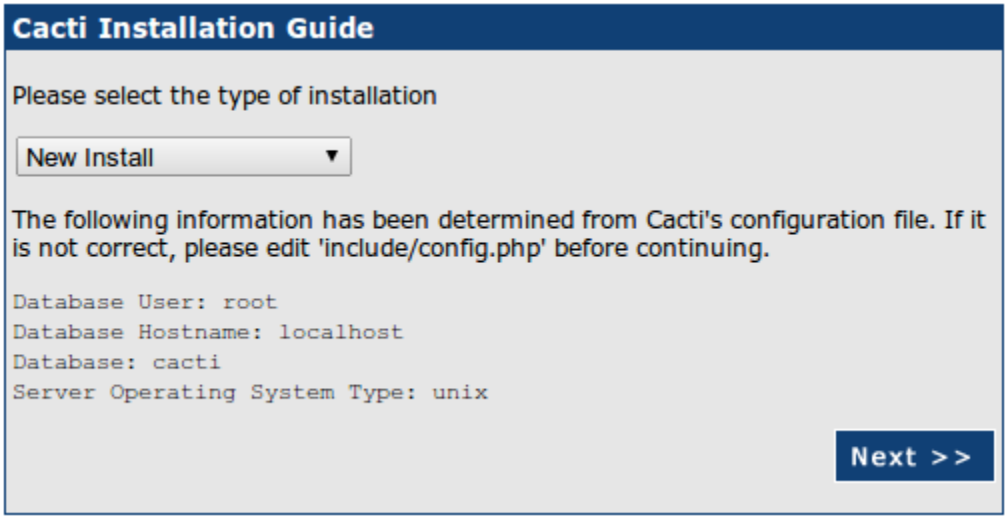

Figura 5: Tela de instalação do Cacti. Fonte: Cacti

A terceira página mostra algumas informações de acordo com a Figura 6, caso essas informações estejam erradas, pode-se corrigi-las

Clique em Finish.

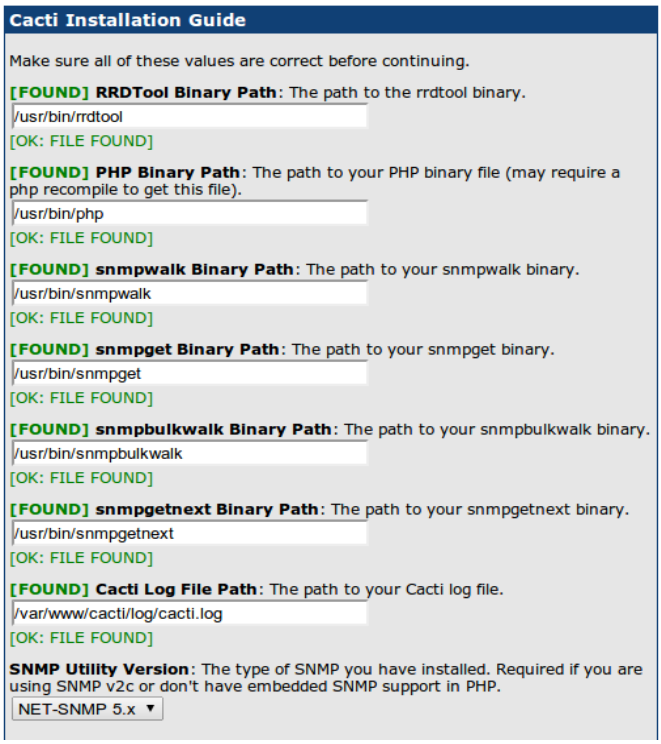

Figura 6: Tela de instalação do Cacti. Fonte: Cacti

Entre com o usuário e senha padrão de acordo com a Figura 7.

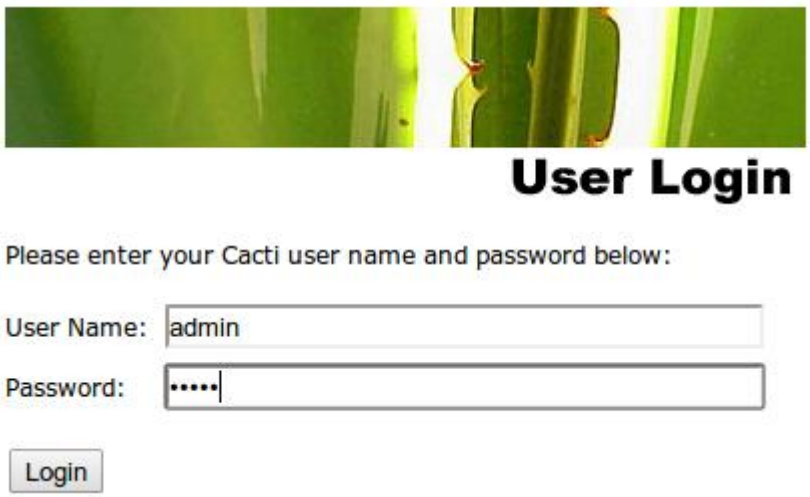

Figura 7 Tela de login do Cacti. Fonte: Autor.

6.2.1 Adicionar um *Host Windows* para ser monitorado pelo Cacti

Para adicionar um host com sistema operacional windows é necessário ter instalado o cliente SNMP, que em todas as versões do windows esse cliente vem desentalado.

Um detalhe importante é liberar as portas usadas pelo protocolo SNMP no firewall do Windows ou qualquer outro que esteja utilizando, caso contrário o Cacti não vai obter comunicação com o host.

Depois que esses procedimentos acima concluídos, na aba *Devices*, clique em Add que se encontra no canto superior direito e teremos esta configuração de acordo com a Figura 8.

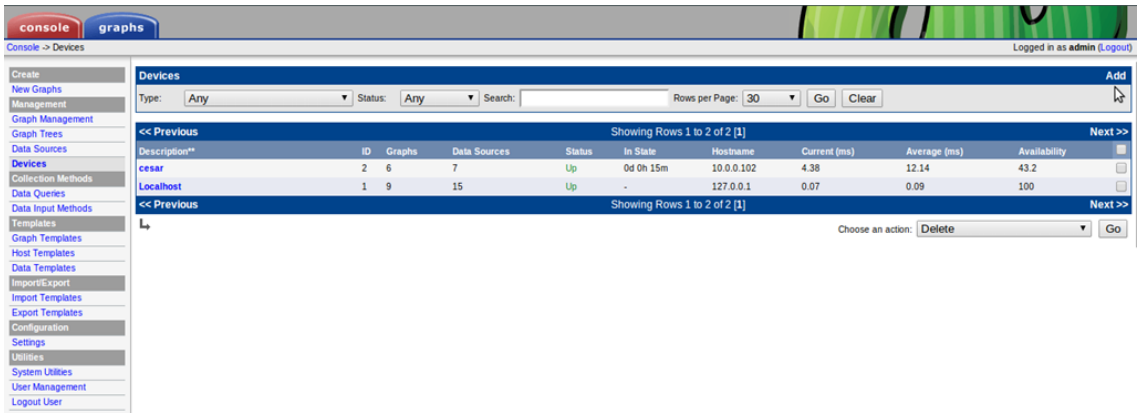

Figura 8. Host em funcionamento no Cacti. Fonte: Autor

Nos campos *descripition* e *hostname* , é de acordo com o host ou ativo de rede que é adicionado.

No campo SNMP Version escolha Version 1.

No campo *SNMP Community* digite o nome da comunidade configurada no nsclient++ do Windows, por default esta como Public. O nome que colocar no cliente será o mesmo nome que colocará neste campo.

Os campos restantes já virão com os valores padrão.

Após esta etapa clipe no botão *Save* que se encontra no campo inferior direito. De acordo com a figura 9.

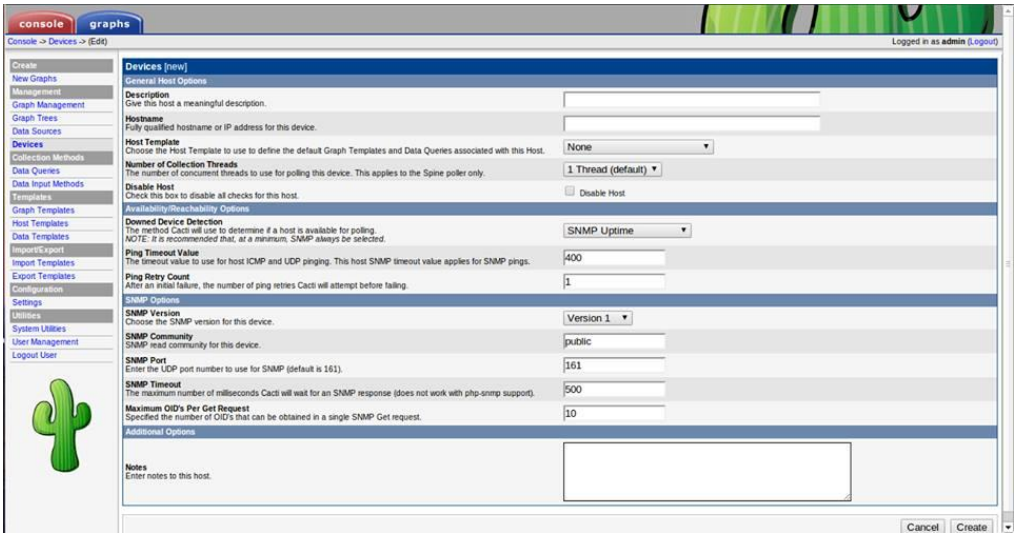

Figura 9 Tela de criação de devices. Fonte: Autor.

Após adicionar o host *Windows* para monitoramento, foi feito um teste para saber se o host foi adicionado corretamente. A Figura 10 mostra que o host *Windows* foi configurado com o nome Cesar.

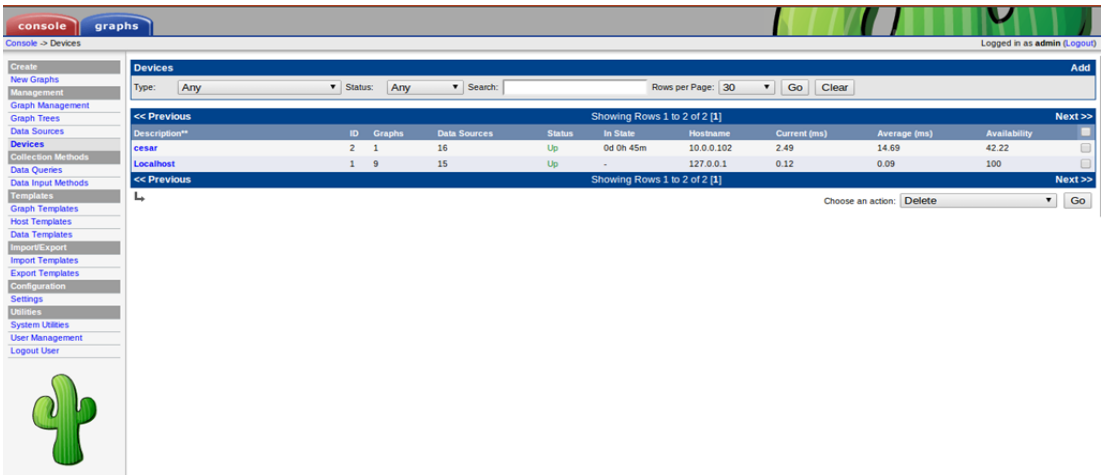

Figura 10 Apresentação dos *devices*. Fonte: Autor

6.3 Integração das ferramentas

Para a integração em si, os dados gerados pelo Nagios, tem que ser convertidos em outro formato, pois no formato original o Cacti não consegue realizar a leitura. O Cacti gera seus dados em formato .rrd, um script do fórum oficial do Nagios foi utilizado para a conversão dos dados, inicialmente o script converte os dados do Nagios em formato rrd, e não era relacionado diretamente com o Cacti, porém é o formato necessário para a leitura dos dados.

O script é encontrado no endereço http://support.nagios.com/forum , é necessário ser membro do fórum para ter acesso aos dados. Os dados de monitoramento são extraídos dos equipamentos da rede através dos plugins do Nagios que utilizam o script para abastecer o banco de dados RRD, que, por sua vez, é utilizado pelo Cacti para a criação dos gráficos. A imagem 11 exemplifica o funcionamento do script.

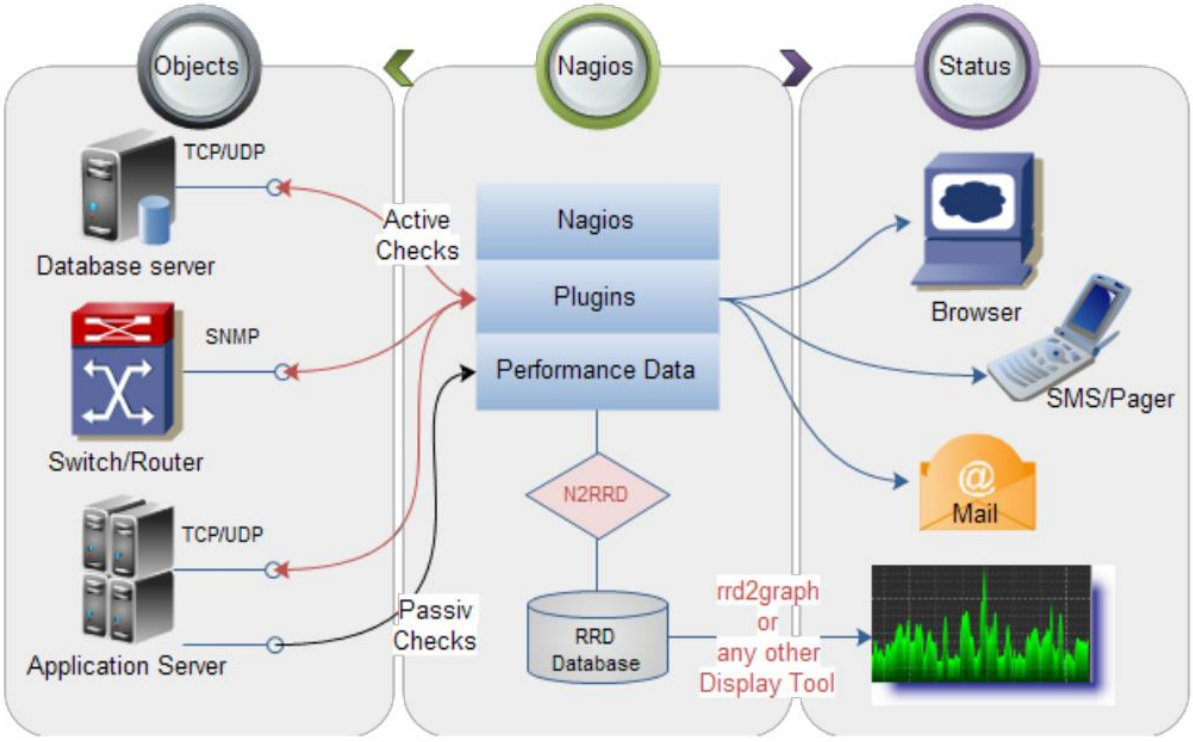

Figura 11 Funcionamento do script. Fonte: Fórum do Nagios.

São duas as formas oferecidas para a comunicação entre o Nagios e o script:Pipe: Este método utiliza menos recursos. O Nagios passa os dados através de um túnel e o serviço perd2rrd os recebe em tempo real. Caso o serviço perf2rrd trave, os dados naquele período serão perdidos.

UDP: Este método é o mais seguro, visto que os dados do Nagios são armazenados em um arquivo. Este é excluído, caso a transferência seja comprovada, caso contrário, os dados são mantidos até que a transferência seja efetuada. As variáveis que devem ser obrigatoriamente configuradas no script são:

CACTI_DIR : Caminho para o diretório do Cacti.

NAGIOS_CONF_DIR : Caminho para os arquivos de configuração do Nagios /etc/nagios/ por padrão.

ROTATION : Rotation mode : d for diária, h para horária, n para nenhuma. SERVICE_PERFDATA_PIPE : Caminho para o pipe (perf2rrd).

PERFDB_USER : usuário.

PERFDB_PASSWORD : senha.

PERFDB_HOST : nome do servidor. TEMPLATE_SEPARATOR_FIELD : "@" por padrão, separador para diferenciar nome de serviço de nome de template, exemplo: cpu_pload@CPULOAD O diretório /etc/n2rrd/templates/rra contém os modelos necessários para monitoramento de espaço em disco, uso do processador etc.

O método de comunicação utilizado é o Pipe, a configuração deve ser feita no arquivo /etc/nagios/nagios.cfg, onde o seguinte código deve ser adicionado: process_performance_data=1 service_perfdata_file=/var/log/nagios/perfdata.pipe service_perfdata_file_template=[SERVICEPERFDATA]|$SERVICEDESC$|$HOSTNAME$|$HOSTADDRESS$|$TIMET$|$SERVICEEXECUTIONTIME$|$SERVICELATENCY$|$SERVICESTATE$|$SERVICEOUTPUT$|$SERVICEPERFDATA$ service_perfdata_file_mode=w

Nesse caso, são estipulados os campos escritos no arquivo temporário perfdate.pipe. Configuração do cacti para a integração É necessário criar um novo modelo de entrada de dados, um *template*, de acordo com a Figura 12 que vai ser

vinculado ao arquivo em que os dados do nagios são gravados, primeiramente cria-se um novo data input, como na figura Na criação o nome do *Data Input* para melhor organização, deve se relacionar com a entrada a ser criada, como exemplo: ping dos host, espaço livre em disco,etc. E e no campo *Input string* é o caminho do arquivo convertido do *Nagios.*

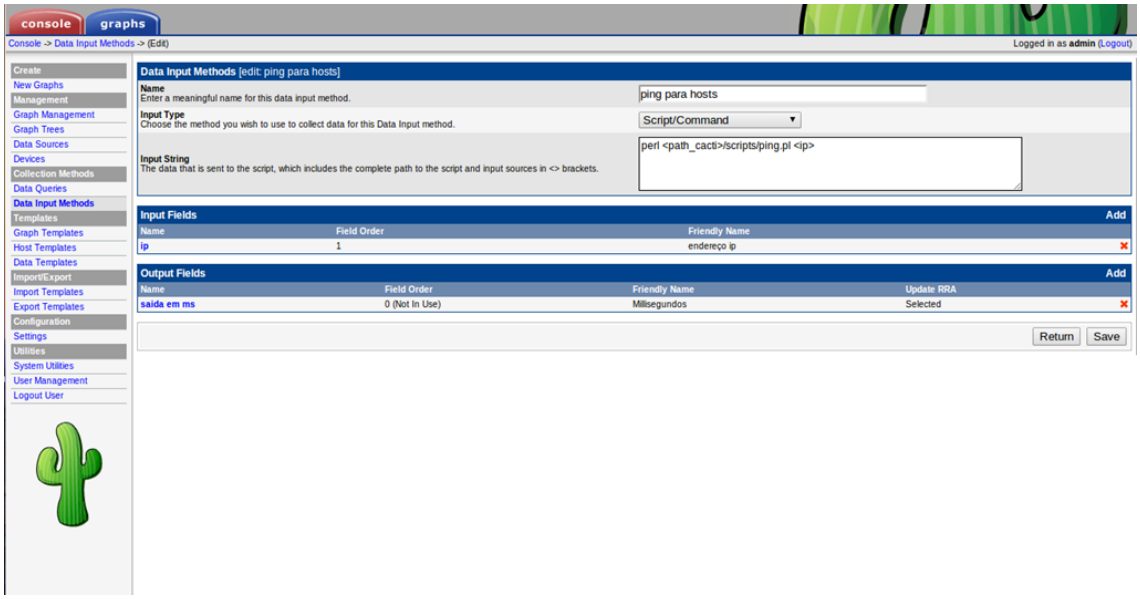

Figura 12 Tela de criação do Data Input. Fonte: Autor

Depois do novo *Data Input criado*, é necessário criar um novo *Data Source*, que pode ser vinculado a um host, na aba *Templates*, clicar em *Data Templates*, de acordo com a figura 13.

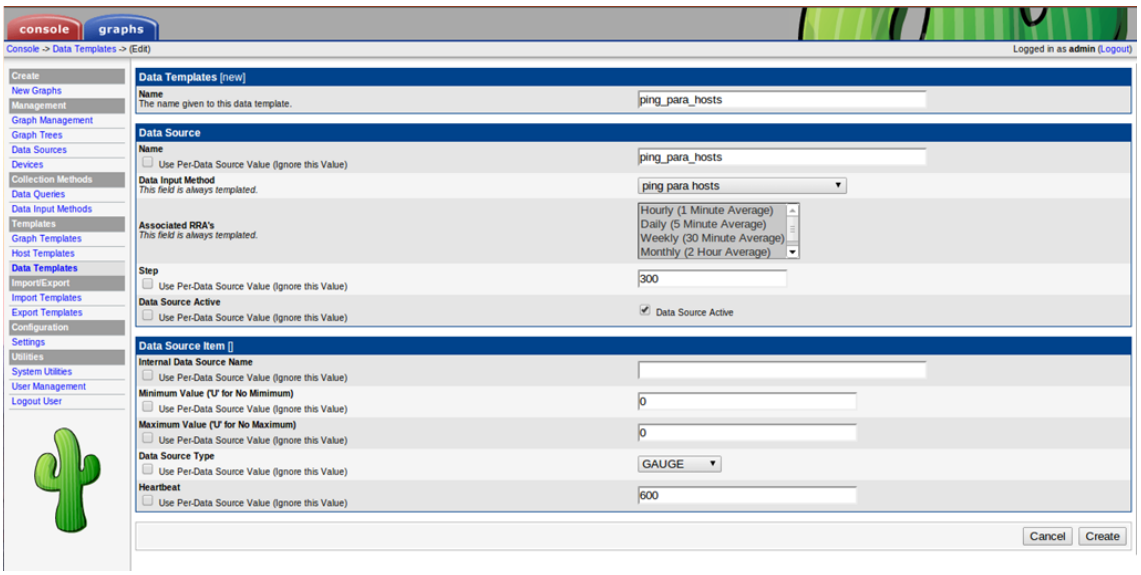

Figura 13 Criação do novo Data Source. Fonte: Autor

Se a criação do *Data Input Methods* foi correta, a opção deve aparecer no campo “ *Data Input Methods”,* e então é necessário escolher o *data input* criado, o nome do novo Data *template* é livre, mas por organização é melhor relacionar o nome com o serviço monitorado.

Logo depois, clicar na aba *Graph Management*, e então localizar o nome do gráfico que foi cadastrado, e então o gráfico é gerado, de acordo com o gráfico 1. Durante os testes, foi observado que a gráfico não é criado instantaneamente, demora aproximadamente 1 ou 2 minutos. Para os testes, cadastramos apenas um dos hosts, para que não houvesse nenhuma dúvida da construção do gráfico, apenas com os dados fornecidos pelo Nagios.

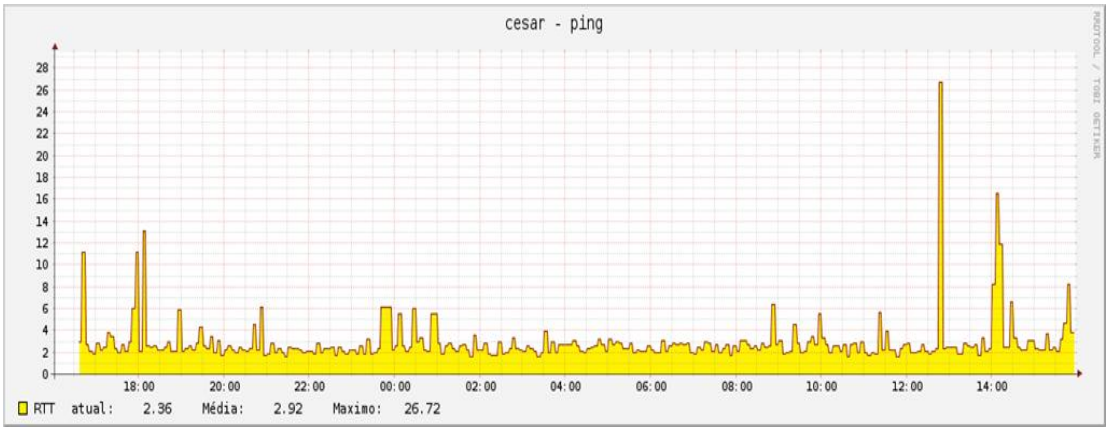

Grafico 1. Gráfico de ping. Fonte:Autor.

O gráfico gerado pode ser personalizado, editando o *Graph Template*, as cores podem ser alteradas, a forma de exibir o gráfico também pode ser alterado, e podem ser adicionado parâmetros, tomando como exemplo um gráfico de *ping*, podem ser criado parâmetros de máximo, mínimo, e a média.

7. DICAS DE PROCEDIMENTO

Caso seja necessário remover o Cacti ou o Nagios devido a problemas, recomenda-se que os remova completamente, com o comando apt-get purge cacti, ou apt-get purge nagios. Assim todas as configurações feitas também podem ser apagadas.

Tanto o Nagios quanto o Cacti, possuem seus fóruns específicos, lá é possível encontrar vários relatos de problemas, ou bugs, e na maioria dos casos há uma solução, é importante utilizar os fóruns como consulta para problemas.

Problemas e possíveis soluções:

O Cacti não exibe os gráficos:
possível solução – abra o terminal, e vá até a pasta /var/www/cacti , e execute o comando poller.php, depois e só atualizar a pagina do cacti.

Gráficos “picados” (problema quando os gráficos exibidos, aparecem falhados, como se a cada 2 amostragens, apenas uma delas aparecer): Possível solução – entrada do cron duplicada, o poller pode estar duplica no cron, verifique em /etc/cron.d, caso exista 2 entradas para o poller, comente uma linha e atualize o cacti.

Problemas com o Nagios Error: Could not read object configuration data! Possível solução - para esse problema existem varias soluções, isso vai depender de como foi configurado o Nagios, a distribuição do sistema operacional que e tá servindo de servidor para o Nagios e a forma como o apache e o Nagios são parados e reiniciados. É sempre recomendado que reinicie o apache e o Nagios antes de tentar qualquer uma das soluções. No caso desta configuração, o Nagios foi instalado em um sistema operacional Linux, então o comando para parar e depois ligar o Nagios é :

/etc/init.d/nagios stop

#/etc/init.d/nagios start

Depois de reiniciar o serviço do Apache e do Nagios, foi alterado a

permissão dos arquivos da pasta Nagios para nagios:nagios e depois adicionado o usuário nagios para o grupo Apache:

chown -R nagios:nagios /usr/local/nagios/

usermod -G nagios apache

Erro de instalação ou atualização do nagios. Durante a instalação ou atualização do nagios no sistema operacional Ubuntu, é necessario executar o comando abaixo para validar a ação:

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

No processo de validação aparece um erro com a seguinte mensagem: “Error in configuration file ‘/usr/local/nagios/etc/nagios.cfg’ – Line 465 (Check result path is not a valid directory) Error processing main config file! /usr/local/nagios/var/spool/checkresults”

Possível solução - existem duas possíveis soluções para o problema, verificar se existe o diretorio /usr/local/nagios/var/spool/checkresults/, caso não tenha, o usuário deve criar o mesmo. Depois de criado o diretório é necessário dar permissões nos dois diretórios a seguir : chmod 2775 /usr/local/nagios/var/ chmod 2775 /usr/local/nagios/var/spool/checkresults/

CAPÍTULO 8 - CONCLUSÃO

O administrador de rede pode confiar nos resultados oferecidos graficamente pelo Cacti, sendo que os dados do gráfico foram fornecidos pela ferramenta Nagios.

A integração das duas ferramentas, oferece uma solução de baixo custo para o monitoramento de redes e de recursos computacionais.

Alguns administradores utilizam as duas ferramentas, porém separadamente, sem nenhum tipo de interação. Os softwares são eficientes no monitoramento de recursos, cada um com suas particularidades, porém a interação cria uma forma mais completa para monitorar a rede.

Um ponto bem interessante é a utilização de ambos os softwares para manter a segurança da rede, visto que é possível monitorar vários elementos, fazendo com que o inicio de um ataque seja facilmente detectado, ou caso aconteça um ataque, há possibilidade de ter conhecimento sobre a origem.

8.1 Trabalhos futuros

Em relação ao protocolo SNMP, ambos os programas abordados neste trabalho fazem o uso do mesmo protocolo o SNMP. Sugere-se a a criação de um mecanismo que utiliza-se apenas uma mensagem SNMP para ambos os programas, e que evitaria trafego desnecessário na rede.

Outro trabalho sugerido é a criação de uma interface, ou alguma ferramenta que realize de forma automática a parte manual da intregação, fazendo com que o processo de definições dos gráficos como *Data Input* e *Data Source*, fosse automatizado.

BIBLIOGRAFIA

1. Apache. The Apache Software Foundation. acessado em 10/09/2013 (disponível em: http://www.apache.org)

2. Cacti. 2004-2013 The Cacti Group. acessado em: 11/05/2013, (disponível em: http://www.cacti.net)

3. DIAS, DAGOBERTO A. NETTO, DANIEL BARBOSA, SOUZA WEVERTON G. L. e ARRUDA EMILIO J. M. FILHO. **Redes Monitoradas com Cacti e Nagios,** 2010**.**

4. CAMPOS, PAULO SÉRGIO DE. **Implementação do software Nagios para gerência e monitoramento de redes corporativas com estrutura LAN, MAN E WAN,** 2007

5. DUARTE, OTTO M.B. **Gerenciamento de Redes.** (1996).

6. KOCH, MOISÉS. **Uma proposta de solução de gerenciamento de contabilização utilizando Nagios e Cacti,** 2008.

7. MACHADO, LEONARDO HENRIQUE. MACEDO, PEDRO FERNANDES**. Manual de instalação do nagios,** 2013.

8. MAJEWSKI, ROBERTO. **Sistemas de monitoração de rede**, 2006.

9. MOURA, MARCOS DANIEL. BECKER, PEDRO CRISTIANO. **Utilização da Ferramenta Nagios Para Monitoramento de Sinal de Antenas de Rede Wireless,** 2007

10. NETO, ARLINDO FOLLADOR. UCHOA, JOAQUIM QUINTEIRO. **Ferramentas livres para monitoração de servidores**, 2009.

11. PEREIRA, MATHEUS CASANOVA**. Dissertação Administração e Gerência de Redes de Computadores,** 2001.

12. PEREIRA, EDUARDO PEREZ. MOURA, RODRIGO COSTA DE. **Estudo da Ferramenta Cacti, para análise de desempenho de rede**, 2008.

13. PHP. 2001-2013 The PHP Group. acessado em 10/09/2013 disponível em: http://www.apache.org.

14. RODRIGUES, RÔMULO ALCEU. **Integração das Ferramentas Nagios e Cacti como solução de monitoramento de recursos computacionais em redes**, 2010.

15. RRDTOOL. Oetiker, T. (2009). OETIKER+PARTNER AG. Acessado em: 10/09/2013 disponível em: http://oss.oetiker.ch/rrdtool.

16. SANCHEZ, ÁLVARO PEREZ. CAMPOMORI, CLEBER LOPES. ROCCA, JOSÉ MARCOS. LEMES, PEDRO AURÉLIO. **Sistema Operacional Linux**, 2011.

17. SANTOS, CINTHIA CARDOSO DOS. **Gerenciamento de redes com a Autilização de Software Livre,** 2010.

18. SILVA, RODRIGO FERREIRA DA. **Virtualização de Sistemas Operacionais**, 2007.

19. SOUZA, ROGÉRIO ARCANJO. **Gerenciamento de Redes usando Nagios,** 2009.

20. TORRES, GABRIEL. **Redes de computadores Curso completo. 1a ed.São Paulo: Editora Axcel Books**, 2001.

21. VAZ, TIAGO BOROTLETTO. **Monitoramento e Segurança de Redes com Software Livre**, 2010.

22. www.cacti.net Acessado em 23/08/2013.

23. www.cacti.net/documentation.php Acessado em 20/08/2013.

24. www.cisco.com Acessado em 03/09/2013.

25. www.nagios.org Acessado em 15/10/2013