

LIGA DE ENSINO DO RIO GRANDE DO NORTE
CENTRO UNIVERSITÁRIO DO RIO GRANDE DO NORTE
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

ANTIÓGENES TAVARES DA SILVA NETO

CENTRO DE OPERAÇÕES DE REDE (NOC) - UM ESTUDO DE CASO

NATAL / RN
2014

ANTIÓGENES TAVARES DA SILVA NETO

CENTRO DE OPERAÇÕES DE REDE (NOC) - UM ESTUDO DE CASO

Monografia apresentada ao curso de Especialização em Redes de Computadores do Centro Universitário do Rio Grande do Norte como requisito parcial para a obtenção do título de Especialista em Redes de Computadores.

Orientador: Prof. Me. Aluizio Ferreira da Rocha Neto.

NATAL / RN
2014

Catálogo na Publicação – Biblioteca da FARN
Setor de Processos Técnicos

Silva Neto, Antiógenes Tavares da.

Centro de operações de rede (NOC) – um estudo de caso. / Antiógenes
Tavares da Silva Neto. – Natal, 2014.
36 f.

Orientador: Prof. Me. Aluizio Ferreira da Rocha Neto.

Monografia (Especialização em Redes de Computadores) – Centro
Universitário do Rio Grande do Norte.

1. Redes de Computadores – Monografia. 2. Monitoramento de
Redes – Monografia. 3. Governança de TI – Monografia. I. Rocha Neto,
Aluizio Ferreira da. II. Título.

RN/UNI-RN/BC

CDU 004.72

LISTA DE FIGURAS

Figura 1: Interface de relatório do WhatsUp.....	15
Figura 2: Gráfico com informações da utilização de dispositivos com The Dude.....	15
Figura 3: Interface principal do WhatsUp.....	16
Figura 4: Interface principal do The Dude.....	17
Figura 5: Interface informativa do Nagios.....	20
Figura 6: Virtualização de um mapa de infraestrutura de rede pelo Nagvis.....	21
Figura 7: Instalação do OMD.....	23
Figura 8: Continuando a instalação do OMD.....	24
Figura 9: Definindo uma senha para o banco MySQL.....	25
Figura 10: Criação da instância.....	25
Figura 11: Iniciando a instância.....	26
Figura 12: Acessando a interface web.....	26
Figura 13: Interface web do Nagios.....	27
Figura 14: Interface web do Nagios.....	27
Figura 15: Hosts no Nagios.....	29
Figura 16: Serviços no Nagios.....	30
Figura 17: Diagrama da rede.....	30
Figura 18: Criação do mapa no Nagvis.....	31
Figura 19: Adicionado imagem de fundo ao mapa no Nagvis.....	31
Figura 20: Adicionando hosts no mapa.....	32
Figura 21: Detalhe de monitoramento do host.....	32

RESUMO

Esta monografia visa mostrar que o monitoramento de redes em conjunto com as boas práticas de TI vem se tornando indispensável na gestão da tecnologia da informação. Esta monografia mostra também uma análise sobre o monitoramento de redes de servidores e ativos de rede, comparando as ferramentas existentes no mercado. O mundo corporativo vem exigindo maior precisão nas tomadas de decisão do gestor no momento do planejamento, adequação e expansibilidade do parque tecnológico, no auxílio a isso o monitoramento de redes se encaixa muito bem e isso será demonstrado no decorrer desta monografia.

ABSTRACT

This monograph aims to show that the monitoring networks in conjunction with the best practices of IT has become essential in the management of information technology. This monograph also shows an analysis of the network monitoring server and network assets, comparing the existing tools on the market. The corporate world has been demanding greater accuracy in decisions making manager when planning, suitability and scalability of the technology park, in aid to that the monitoring network fits nicely and it will be demonstrated throughout this monograph.

SUMÁRIO

1	INTRODUÇÃO.....	6
1.1	OBJETIVOS	6
1.1.1	<i>Objetivos Específicos</i>	<i>6</i>
1.2	JUSTIFICATIVA.....	7
2	EVOLUÇÃO DA TECNOLOGIA DA INFORMAÇÃO	8
2.1	REDES DE COMPUTADORES.....	9
2.1.1	<i>Ativos e Serviços de Rede</i>	<i>9</i>
2.2	GOVERNANÇA CORPORATIVA, GOVERNANÇA DE TI E BOAS PRÁTICAS	11
2.2.1	ITIL®.....	12
2.2.1.1	Operação de Serviço	13
2.2.1.2	Gerenciamento de Incidentes.....	13
2.2.1.3	Gerenciamento de Problemas	13
2.3	MONITORAMENTO DE REDES.....	13
2.4	FERRAMENTAS DE MONITORAMENTO	14
2.5	NAGIOS	17
2.6	NAGVIS	21
2.7	OMD – THE OPEN MONITORING DISTRIBUTION	21
3	DESENVOLVIMENTO	22
3.1	IMPLANTAÇÃO DA FERRAMENTA	22
4	CONCLUSÃO	34
	REFERÊNCIAS	35

1 INTRODUÇÃO

Com o avanço da tecnologia, as redes de telecomunicações se tornaram uma necessidade para o momento atual de evolução no mundo dos negócios. O que antes era tratado como um luxo passou a ser um importante marco estratégico para o mundo corporativo, e necessário para a sociedade.

O crescimento acelerado e a aparição de novas tecnologias têm alterado as características das redes de computadores. Hoje, na gestão de tecnologia da informação, passou a ser indispensável o monitoramento em tempo real da infraestrutura de rede e seus ativos. Este monitoramento permite obter as informações necessárias sobre estes equipamentos de forma ágil, precisa e confiável, facilitando as tomadas de decisão do gestor no momento do gerenciamento de incidentes e problemas no parque tecnológico.

Este trabalho visa mostrar as vantagens de um centro de monitoramento de redes, fazendo uso de processos em conformidade com a Governança de TI para gerenciamento de incidentes e problemas utilizando ferramentas de código aberto, assim como o uso da infraestrutura na nuvem para hospedagem das ferramentas.

1.1 OBJETIVOS

O objetivo geral desta monografia é abordar um Centro de Operações de Rede (do inglês NOC – *Network Operation Center*), estudando os procedimentos e ferramentas que permitem o funcionamento do mesmo, dando ênfase no uso de melhores práticas nos processos e ferramentas de gerenciamento de redes e mostrando seu funcionamento e viabilidade.

1.1.1 Objetivos Específicos

Para atingir o objetivo geral, as seguintes etapas serão realizadas:

- Estudar a evolução da TI.
- Estudar as melhores práticas, dando ênfase na operação de serviço do ITIL.
- Estudar as ferramentas de monitoramento de redes demonstrando exemplos do seu funcionamento.
- Demonstrar as vantagens do NOC.

1.2 JUSTIFICATIVA

O estudo proposto servirá de fonte de conhecimento para empresas que necessitem de monitoramento em tempo real de sua infraestrutura de rede, com o propósito de obter informações para tomada de decisão.

2 EVOLUÇÃO DA TECNOLOGIA DA INFORMAÇÃO

A tecnologia da informação teve seu avanço na década de 50 quando surgiu o primeiro sistema de computador, baseado em sistemas de informação e equipamentos complexos para armazenamento de informações, operados por pessoas altamente especializadas. Como tudo que envolve a informática teve um avanço muito acelerado, com as redes de computadores não foi diferente. Depois da fusão dos computadores com as comunicações, houve uma profunda mudança na forma como os sistemas computacionais eram organizados.

O velho modelo de um computador atendendo a todas as necessidades computacionais de uma empresa foi substituído por um conjunto de computadores autônomos interconectados que podem trocar informações, conhecido como redes de computadores.

Na década de 80 as redes de computadores ganharam importância, especialmente com a diminuição dos custos dos computadores, tornando cada vez mais atraente a distribuição do poder computacional em módulos com processadores localizados em diversos pontos de uma organização. Assim, o uso de rede para compartilhamento de recursos passou a ser indispensável no cotidiano de uma empresa, e passaram a ser usadas também em ambientes domésticos. A rede de computadores não se limita a Internet, e está presente em várias atividades do cotidiano. São utilizadas em serviços bancários, no uso do cartão de crédito, em chamadas telefônicas, entre outros. Percebe-se que a cada dia há uma dependência maior na utilização destes serviços e, por consequência, na utilização das redes.

Nesse contexto, o uso de um computador sem que esteja conectado a uma rede está ficando sem utilidade. A facilidade e comodidade que é adquirida utilizando os serviços de rede fazem com que haja dependência desses serviços. Se o serviço de rede de uma empresa estiver inativo, todos os departamentos, diretamente ou indiretamente, são afetados.

É comum, inclusive, que os serviços de uma empresa fiquem ligados a um computador servidor, onde é provido acesso a um sistema ou responsável pela comunicação interna (DAIBERT, 2014).

2.1 REDES DE COMPUTADORES

O século XX foi um marco com o avanço no campo da informação. As pessoas buscam cada vez mais utilizar redes de computadores para se comunicar, armazenar e processar informações. Segundo Tanenbaum, “uma rede de computadores pode oferecer um meio de comunicação altamente eficaz para funcionários que trabalham em locais muito distantes um do outro”. As redes, hoje, são fortemente usadas em todas as áreas e por diversas classes de pessoas, seja para uso pessoal, para ler um e-mail ou acessar algum serviço de alguma rede social, até uso empresarial, para servir dados e aplicações para funcionários.

A tecnologia utilizada para a construção de uma rede pode ser:

- ponto a ponto, que consiste em conexão de pares individuais de máquinas que se comunicam direto sem passar por um intermediário onde tem um emissor e um receptor de dados;
- multiponto, que permite a conexão de várias máquinas compartilhando entre todos os dispositivos de rede um meio de transmissão único, através do qual toda a informação é transmitida.

Quanto à abrangência, uma rede pode ser definida em redes locais, as chamadas LANs (*Local Area Network*), que compartilham recursos e são redes privadas. As LANs abrangem em média 10 km e são utilizadas para conectar servidores, estações, periféricos ou qualquer outro recurso de rede que possuem dispositivos de processamento em um escritório, casa, ou edifícios. Quando uma rede é mais ampla são denominadas MANs (*Metropolitan Area Network* ou redes metropolitanas), que abrangem uma cidade. Já as redes WANs (*Wide Area Network*), conhecidas como redes geograficamente distribuídas, podem abranger um país ou continente, e temos como principal exemplo a Internet.

Uma outra estrutura de rede que vem ganhando uma importância relativa é a rede sem fio (*wireless*), sendo cada vez mais utilizada em dispositivos móveis, smartphones e celulares (DAIBERT, 2014).

2.1.1 Ativos e Serviços de Rede

Uma rede de computadores é formada por diversos tipos de equipamentos, como computadores, roteadores, switch e serviços de rede. Esses equipamentos e serviços podem ser monitorados dentro de uma rede, evitando assim falhas ou até mesmo que uma rede interrompa o seu funcionamento.

Um servidor na rede pode conter funcionalidades de diferentes naturezas. Alguns

tipos de servidores/serviços de rede são:

- O servidor FTP: que é o servidor onde os usuários têm acesso a arquivos em rede;
- O servidor *Web*: é responsável por aceitar pedidos HTTP (*Hypertext Transfer Protocol*) de clientes, servindo com páginas web e arquivos de site;
- O servidor DNS: que é responsável pela distribuição de nome de redes, convertendo nomes em IPs;
- O servidor de arquivos: que é responsável por armazenar arquivos de clientes;
- O servidor *Webmail*: que é responsável pelo envio/recebimento de contas eletrônicas e armazenamento de e-mails;
- O servidor de *Proxy*: que é o responsável pelo armazenamento dos endereços de sites acessados, funcionando como um cache.

Para interligar os computadores na rede é necessária a utilização de alguns dispositivos como o roteador e switch. Esse último responsável por criar um barramento de comunicação entre os diversos dispositivos de rede que podem estar presentes na estrutura.

O roteador é um dispositivo que tem como característica selecionar a rota mais apropriada para transferir e receber protocolos na rede. É utilizado para fazer a comunicação entre diferentes redes de computadores provendo a comunicação entre computadores distantes entre si.

Já o switch é um dispositivo utilizado em redes de computadores para reencaminhar quadros entre os diversos nós. Possuem diversas portas, assim como os hubs, e operam na camada acima dos hubs.

A diferença é que ele segmenta a rede internamente, sendo que cada porta corresponde a um segmento diferente, o que significa que não haverá colisões entre os computadores de segmentos diferentes.

Alguns switches podem ser gerenciados de forma a permitir administrar as portas separadamente. O switch gerenciável normalmente tem outras funcionalidades, como a capacidade de criar VLANs (Virtual LAN), QoS (Quality of Service), firewall, entre outros. Assim é possível habilitar e desabilitar as portas, definir a velocidade da conexão, definir VLANs, configurar o spanningtree, e utilizar software de monitoramento que acessa o switch através de protocolos como o SNMP (Simple Network Management Protocol) (DAIBERT, 2014).

2.2 GOVERNANÇA CORPORATIVA, GOVERNANÇA DE TI E BOAS PRÁTICAS

Muito tem-se falado nos últimos anos sobre o termo “Governança Corporativa”. A Governança Corporativa foi originada no mercado financeiro mundial com o intuito de priorizar a transparência na gestão empresarial em relação ao aumento da rentabilidade e redução de riscos para os investidores da empresa, garantindo o retorno de seus investimentos através da adoção de códigos de boas práticas de gestão. Boas práticas de gestão incluem esforços empresariais no sentido de minimizar o problema de conflito de interesses entre gestores e proprietários das empresas e definir papéis e responsabilidades para os atores no cenário de gestão corporativa (FREITAS, 2010).

Cada vez mais as empresas estão extraindo funcionalidades da Tecnologia da Informação para suportar os seus objetivos de negócio. A retórica da Governança Corporativa não pode ser eficiente se a empresa não dispuser de mecanismos de gerenciamento dos recursos de TI que são responsáveis pela geração, pelo tratamento e pela disponibilização das informações empresariais (FREITAS, 2010).

Após o advento da Governança Corporativa, não demorou muito e o mercado mundial cunhou o termo “Governança de TI” para nomear as práticas de Gestão de TI realizadas para garantir o alinhamento de TI as iniciativas de Governança Corporativa.

A “Governança de TI” possui duas justificativas ou linhas de ação, a saber:

- O objetivo de propiciar insumos para o atendimento das especificações da Governança Corporativa.
- Melhorias dos processos de Gestão de TI.

No primeiro caso, a Governança de TI surge como um componente fundamental para a obtenção da Governança Corporativa. No segundo caso, a Governança de TI surge como instrumento de aprimoramento, aconselhamento e auditoria da qualidade de Serviços de TI. Tais melhorias aumentam o grau de confiança nos recursos tecnológicos e têm como objetivo integrar as atividades de gestão de TI com os objetivos estratégicos das empresas. (Livro Fundamentos do Gerenciamento de Serviços de TI – Marcos André dos Santos Freitas – pag 11)

Antes do advento da Governança já existiam iniciativas de recomendações ou padronizações em diversas áreas do mercado. Boas práticas de mercado orientam e aconselham os processos de gestão e operacionais das empresas. Geralmente são desenvolvidas por instituições sem fins lucrativos que agrupam profissionais de determinadas áreas de conhecimento para trocarem experiências sobre o que pode dar certo ou errado no

mundo corporativo. O resultado desse trabalho em grupo resulta na publicação de guias ou padronizações que podem servir como referencia para as empresas buscarem a excelência nos seus processos. A adoção das boas práticas de mercado, no início, serviu como recomendação de melhoria nos processos nas empresas e atualmente está alcançando um nível de maturidade, deixando de ser somente diferencial competitivo e tornando-se instrumento de regulação de mercado e pré-requisito de qualificação e concorrência. Podemos citar como boas práticas de mercado mais utilizadas por TI atualmente:

- ISO 9000.
- PMBOK.
- COBIT.
- ITIL.

(FREITAS, 2010).

2.2.1 ITIL®

ITIL® é a sigla de *Information Technology Infrastructure Library* e significa: Biblioteca de Infraestrutura de Tecnologia da Informação. Uma dúvida muito comum a respeito do ITIL® é sobre o gênero dos artigos que precedem a palavra ITIL®. O conceito de “biblioteca” para denominar um conjunto de livros é mais utilizados quando queremos nos referir ao local onde são armazenados os livros. Não costumamos chamar de biblioteca um conjunto simplesmente. Eu, particularmente, classifico ITIL® como “o” ITIL® por estar me referindo a um “conjunto de livros”. Do contrário, chamaremos de “a” ITIL® por causa do termo “biblioteca”, mas quando nos referirmos a um livro específico chamaremos de “o” livro Estratégia de Serviço, por exemplo. Qualquer outra justificativa para o uso de “o” ou “a” deriva de anglicismos utilizados para denominar ITIL® como, por exemplo o framework ITIL®, a *best practice ITIL®*, o mais importante são as recomendações e práticas contidas no interior dos livros. Se a sua empresa está utilizando essas práticas e elas estão trazendo resultados ao negócio, não importa muito se é “o” ou “a” ITIL®. Somente deve-se atentar para o fato de que o ITIL® não é de maneira nenhuma uma metodologia. Uma metodologia é um conjunto de regras utilizadas em uma determinada disciplina. As palavras “regras” e “disciplina” denotam uma rigidez de aplicação e soam como obrigação de conformidade. ITIL® não é uma regra obrigatória a ser seguida, é um conjunto de recomendações baseadas em boas práticas de Gerenciamento de Serviços de TI (FREITAS, 2010).

O ITIL® atualmente está na versão 3 (ITIL® V3) e é composto por 5 ciclos de vida:

- *Service Strategy* (Estratégia de Serviço).
- *Service Design* (Desenho de Serviço).
- *Service Transition* (Transição de Serviço).
- *Service Operations* (Operação de Serviço).
- *Continual Service Improvement* (Melhoria Continuada de Serviço).
-

2.2.1.1 Operação de Serviço

O ciclo de Operação de Serviço coordena e conduz as atividades e os processos necessários para entregar e gerenciar os serviços, de acordo com os níveis requeridos pelos clientes e pelo negócio (FREITAS, 2010).

Os processos do ciclo Operação de Serviço são:

- Gerenciamento de Eventos.
- Gerenciamento de Incidentes.
- Gerenciamento de Problemas.
- Cumprimento de Requisições.
- Gerenciamento de Acesso.
-

2.2.1.2 Gerenciamento de Incidentes

O objetivo do Gerenciamento de Incidentes é restaurar a operação de normal dos serviços o mais rápido possível, para minimizar o impacto no negócio (FREITAS, 2010).

2.2.1.3 Gerenciamento de Problemas

O objetivo do Gerenciamento de Problemas é prevenir a ocorrência de Problemas e Incidentes associados através da eliminação de Incidentes recorrentes e da minimização do impacto de Incidentes que não puderam ser prevenidos (FREITAS, 2010).

2.3 MONITORAMENTO DE REDES

Ter um ambiente mapeado e monitorado é fundamental para o processo de crescimento de uma empresa. Já está mais do que comprovado que com um ambiente de TI bem planejado seu negócio tem mais chances de dar certo, mesmo para as empresas em que o principal foco não seja TI, pois todos dependem hoje da Internet e dos serviços que ela

disponibiliza.

Assim, em um ambiente de rede é necessário considerar a eficácia no funcionamento dos equipamentos e serviços existentes. Com o aumento no uso das redes de computadores, aumentam também os problemas na rede, onde os usuários reclamam de acesso lento em horários de pico, indisponibilidade no sistema, problemas em downloads e em acessos em geral. É importante detectar qualquer problema na rede antes que o usuário possa notar a falha. Como é impossível evitar os problemas na rede, a melhor forma de resolver o impacto causado é através do monitoramento.

Monitorar rede é verificar o funcionamento de cada serviço e equipamento disponível. Para isso é necessário utilizar ferramentas que verificam o funcionamento adequado dos equipamentos e serviços, enviando relatórios e alertas aos administradores, prevenindo falhas, e fazendo com que sejam corrigidas antes que sejam notadas pelo usuário (DAIBERT, 2014).

2.4 FERRAMENTAS DE MONITORAMENTO

As ferramentas de monitoramento de redes são utilizadas para que se possa ter um controle efetivo sobre todos os ativos nela disponíveis, verificando serviços e processos.

Existem diversas ferramentas para fazer esse serviço e, para fazer sua implantação, é necessário verificar qual melhor atende às necessidades de cada estrutura de rede.

Algumas opções conhecidas são The Dude, WhatsUP e Nagios, entre outras.

The Dude é uma ferramenta que faz a verificação automática de todos os dispositivos dentro de redes especificadas, desenha e faz o layout de mapas de rede, monitora serviços dos seus dispositivos e alerta em caso de problemas. É uma ferramenta gratuita e cumpre os objetivos simples de sistemas de gerenciamento de redes.

Já a ferramenta WhatsUP é um gerenciador e monitor de rede fácil de utilizar, permitindo a gerentes de TI transformar dados coletados da rede em informações estratégicas para seu negócio, como análise de tendência de planejamento de recursos estratégicos.

As ferramentas de gerenciamento The Dude e WhatsUP são similares nas suas funcionalidades. Destaca-se a ferramenta WhatsUP por possuir mais recursos e opções do que os disponíveis no The Dude, principalmente na forma de apresentar as informações que são disponibilizadas em vários tipos de relatórios e gráficos. A Figura 1 apresenta a interface de menu para acesso aos relatórios disponibilizados pelo WhatsUp, que são os relatórios do sistema, dos dispositivos, das áreas com problemas, dos grupos e de performance.

Na Figura 2 são apresentados gráficos disponibilizados pela ferramenta The Dude mostrando informações da utilização de dispositivos (DAIBERT, 2014).

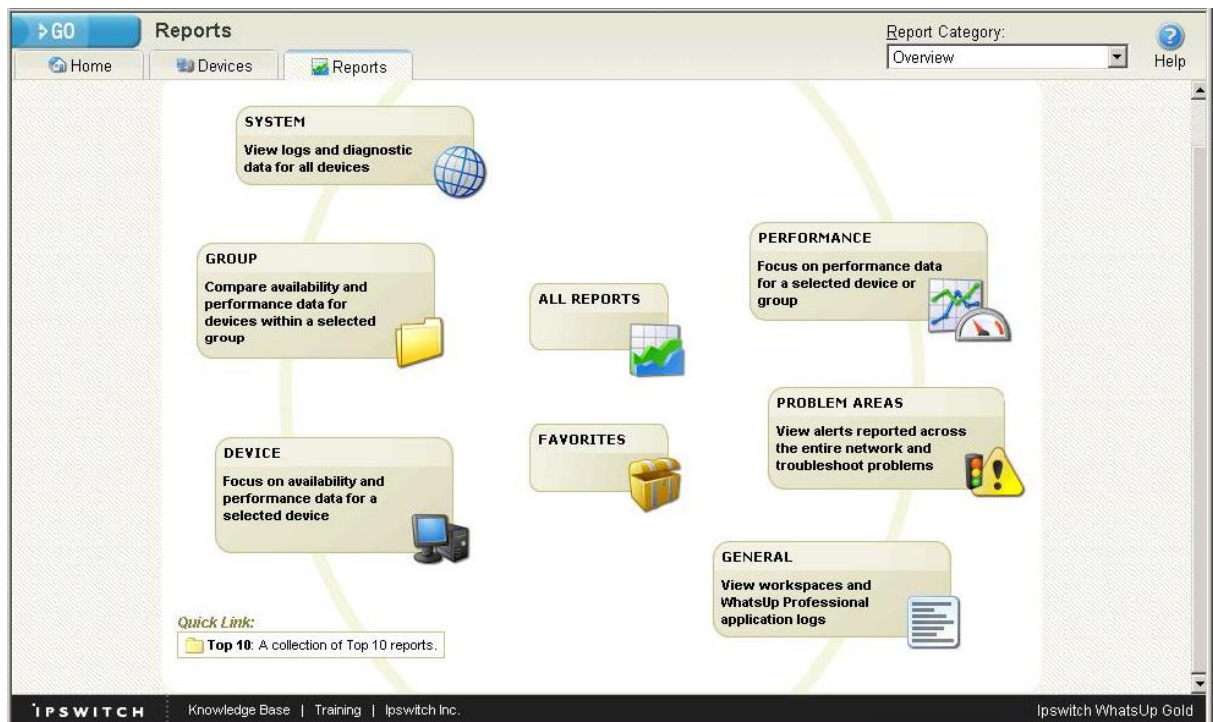


Figura 1: Interface de relatório do WhatsUp
Fonte: DAIBERT (2014).

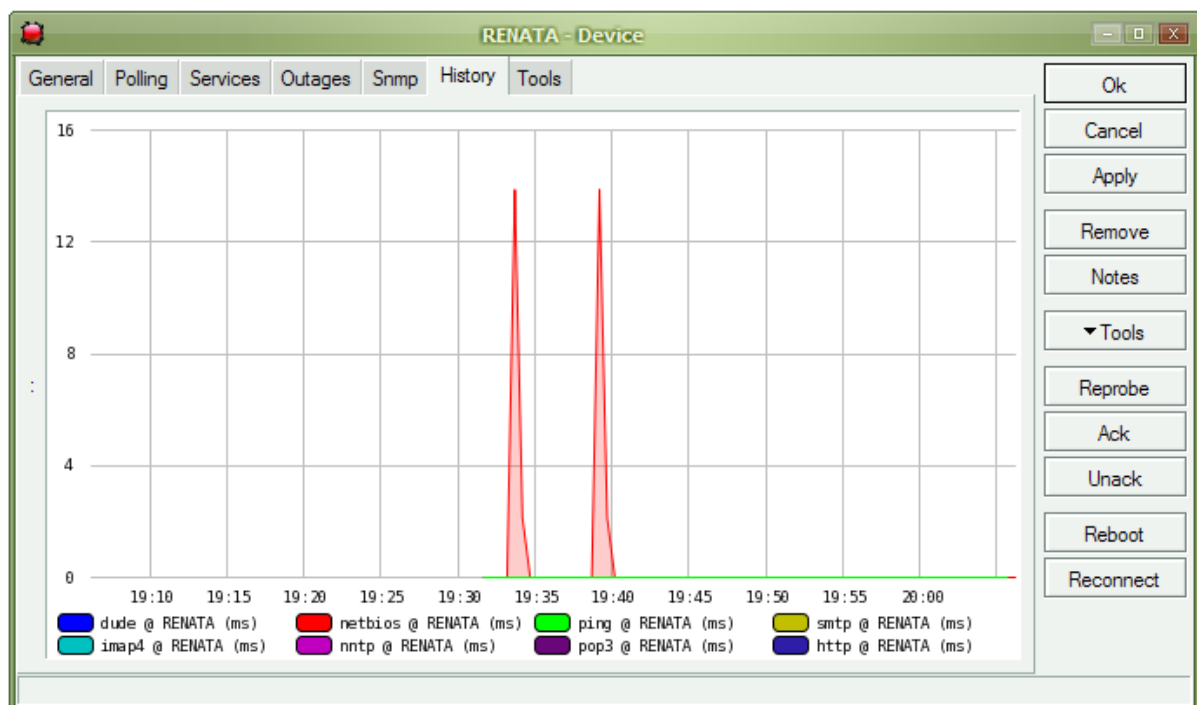


Figura 2: Gráfico com informações da utilização de dispositivos com The Dude.
Fonte: DAIBERT (2014).

Em uma análise comparativa, ambas as ferramentas possuem uma interface simples que permitem acesso web, e são fáceis e intuitivas de operar para usuários acostumados com o ambiente de janelas, ícones e mouse. Além disso, possuem características diferentes quanto à organização dos menus, botões, além dos dispositivos gerenciados. O WhatsUP possui uma interface mais tradicional como pode ser visto na Figura 3. Já o The Dude possui características diferentes quanto à organização das janelas e menus, o que não prejudica tanto a usabilidade conforme pode ser visto na Figura 4. A interface padrão web do WhatsUP apresenta-se mais rica em opções do que o The Dude. Outra diferença entre essas ferramentas é que a WhatsUP é paga, enquanto a ferramenta The Dude é gratuita (DAIBERT, 2014).

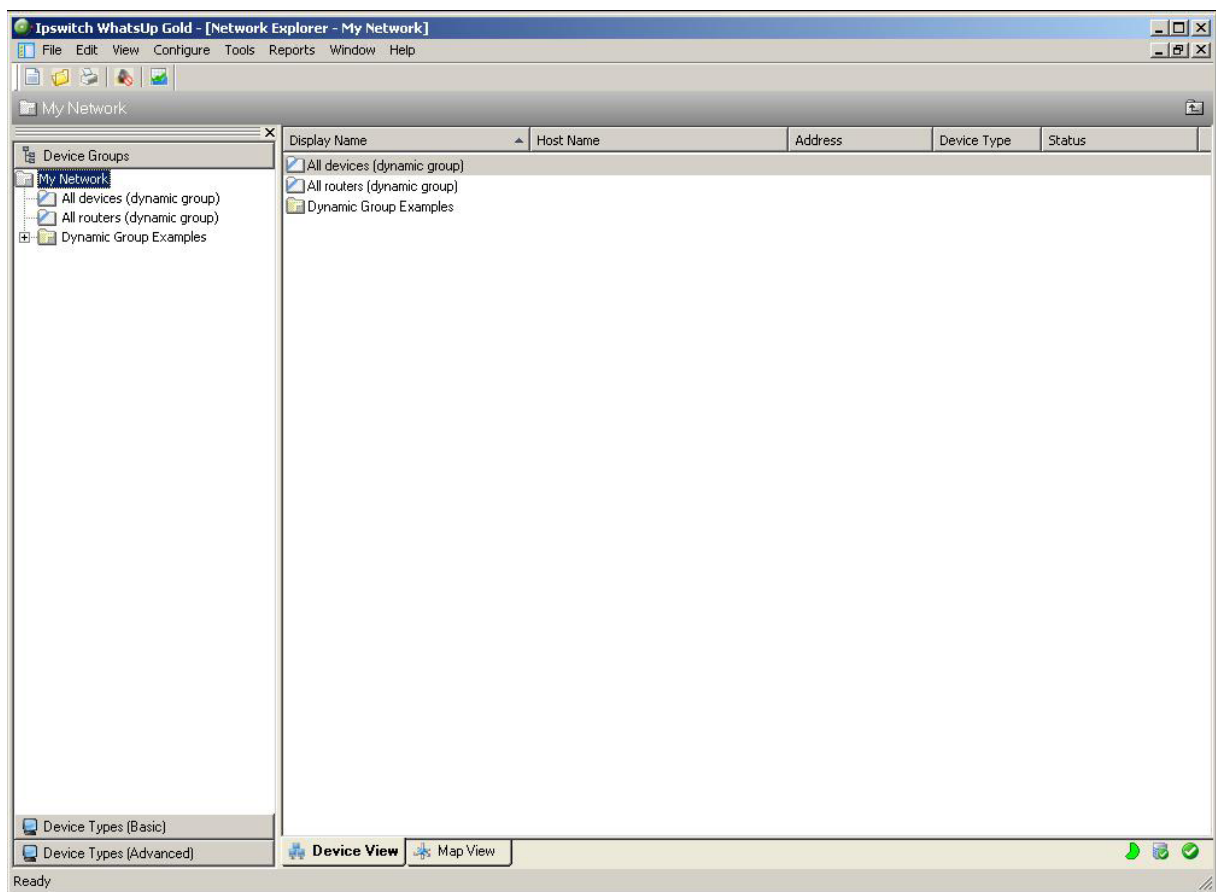


Figura 3: Interface principal do WhatsUp.
Fonte: DAIBERT (2014).

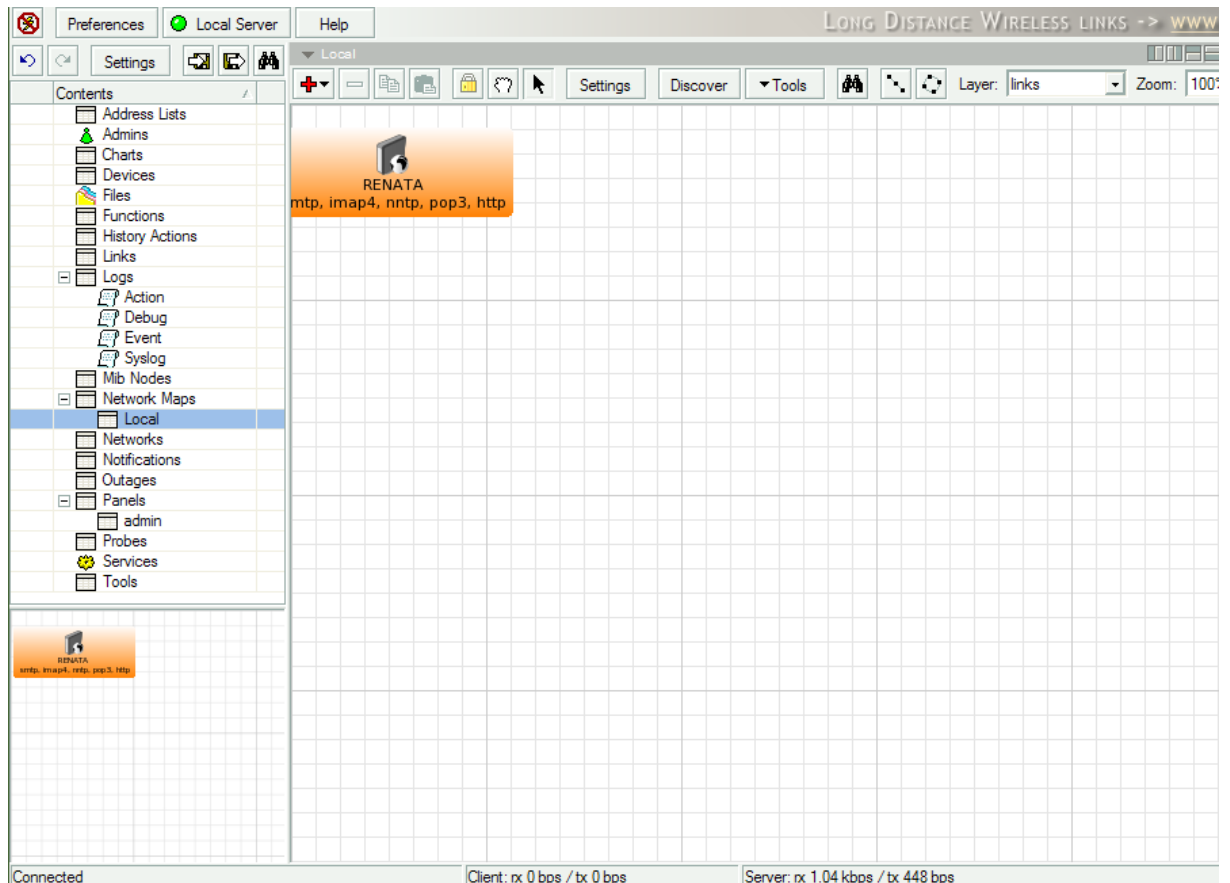


Figura 4: Interface principal do The Dude.
Fonte: DAIBERT (2014).

2.5 NAGIOS

O Nagios é uma aplicação de monitoramento de redes de código aberto e licenciado pelo sistema GPL (General PublicLicense) bastante popular.

Ela permite monitorar tanto hosts quanto serviços, alertando-o quando ocorrerem problemas na rede. Ela é utilizada por administradores de redes para que possam ter um controle sobre os serviços e equipamentos de sua rede. Foi desenvolvida inicialmente para ser utilizada em sistemas operacionais Linux e, a partir da versão 3.0.4, já está sendo compatível com outros sistemas Unix.

O Nagios foi criado primeiramente com o nome de Netsaint, foi escrito e é atualmente mantido pela Ethan Galstad, e sua equipe de desenvolvedores é responsável por manter os plugins oficiais e não-oficiais. Ethan Galstad é o criador do projeto e um dos maiores mantenedores.

O Nagios busca uma forma prática de auxiliar os administradores de redes no processo de monitoração. As características principais do Nagios são: o monitoramento de serviços de rede como tráfego de dados de host e serviços que podem ser definidos pelo

administrador da rede, além de monitorar serviços como SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol), HTTP (HyperText Transfer Protocol), NNTP (Network News Transfer Protocol), ICMP (Internet Control Message Protocol) e SNMP (Simple Network Management Protocol). O Nagios monitora também os recursos de servidores como logs do sistema, carga do processador, uso de memória e uso de disco.

Há uma infinidade de serviços que são monitorados por essa ferramenta, especialmente pela sua arquitetura baseada em plugins, onde qualquer administrador de rede pode desenvolver seu próprio plugin para monitorar qualquer particularidade de sua rede. Os plugins podem ser desenvolvidos em qualquer linguagem. Mas a grande maioria que existe é desenvolvido em perl e python.

A notificação dos possíveis problemas de rede é feita através de alertas enviados por e-mail, pager, SMS (Short Message Service), e outros meios definidos pelo administrador do sistema.

O serviço do Nagios é dado por algoritmos de verificação, podendo ser verificações simples como, por exemplo, o monitoramento via ping, ou monitoramento avançado podendo ser, neste caso, o monitoramento via o protocolo SNMP (Simple Network Management Protocol). Este protocolo permite que a máquina que está monitorando o host envie um OID (Object Identifier) para a máquina monitorada solicitando informações sobre o seu funcionamento. O protocolo então retorna a informação solicitada. O SNMP é o protocolo simples de gerência de rede que disponibiliza ao administrador da rede o acesso a diversas informações da máquina monitorada, entre elas: utilização de CPU, utilização de memória, configurações de rede, atividade de rede - download e upload -, usuários conectados, serviços ativos, entre outros. É possível ainda, na categoria de verificações avançadas, a utilização de plug-ins específicos que são disponibilizados em diversos sites especializados no assunto. Um exemplo é o site Nagios Exchange (<http://exchange.nagios.org/>), mantido pela empresa desenvolvedora do Nagios, que agrupa diversos plug-ins de seus usuários com diversas responsabilidades de monitoramento.

Os serviços de monitoração são feitos através de arquivos onde é definido o que será monitorado. A ferramenta já possui seus arquivos definidos, porém permite que o usuário crie modos próprios de monitoração. O principal arquivo da ferramenta é o `nagios.cfg`, que é onde está a configuração principal responsável pela operação do Nagios. Esse arquivo, por padrão, é criado automaticamente quando o Nagios é configurado. Outros arquivos também são necessários para o funcionamento da ferramenta, como o arquivo `resource.cfg`, que é utilizado para armazenar as variáveis que podem ser personalizadas com o objetivo de facilitar o acesso

às chamadas aos plug-ins pela ferramenta. Já o arquivo `services.cfg` é utilizado para identificar os serviços que serão verificados e as métricas associadas a cada cliente monitorado.

A definição dos clientes que serão monitorados é feita no arquivo de cliente `host.cfg`, e esses clientes podem ser agrupados com o propósito de simplificar as notificações. O arquivo `contacts.cfg` define quem receberá a notificação caso a rede apresente algum problema ou restabeleça um serviço. Um ou mais contatos podem ser agrupados para receber as notificações dos clientes através do arquivo `contactgroups.cfg`.

Outros arquivos de configurações são o `timeperiods.cfg`, responsável pelo período de tempo em que será válido fazer as notificações e checagem dos serviços; e o `commands.cfg`, responsável pelas definições dos comandos a serem executados para monitoramento. Cada comando usado no parâmetro `check_command` dos hosts precisará estar configurado nesse arquivo.

Outro arquivo de configuração importante é o `CGI.cfg`, que é o arquivo de configuração das permissões de acesso dos usuários quando esta opção estiver ativa nas configurações principais.

O Nagios não possui interface para configuração na versão gratuita e nas versões CORE. A configuração é feita manualmente ao editar seus arquivos de configuração. Já na versão enterprise, a Nagios XI, toda e qualquer tipo de configuração pode ser feita pela sua interface.

Existem outras ferramentas que fazem isso nas versões gratuitas, mas não são suportadas oficialmente pela desenvolvedora do Nagios. Um exemplo é o NagiosSQL (<http://www.nagiosql.org/>), uma ferramenta de administração web que possui uma interface que é definida após a instalação do Nagios para fazer a configuração do mesmo.

Antes de instalar e fazer a configuração do Nagios, é necessário preparar o ambiente em que será instalado. Como a aplicação irá gerar os arquivos CGI (Common Gateway Interface) para que a aplicação funcione perfeitamente, é necessário que esteja instalado um servidor Web, como o Apache, e algumas dependências como o compilador gcc (GNU Compiler Collection), e as bibliotecas GD (<http://www.libgd.org/>).

Em todas as versões do Nagios há uma interface Web informativa onde é possível acompanhar todo o monitoramento conforme Figura 5. Somente na versão enterprise estas interfaces se estendem para a manipulação dos arquivos de configuração. A interface das versões gratuitas é dividida em quatro partes: geral, monitoramento, relatórios e configuração.

Na parte geral (General) da interface existem os campos home, que direciona para a página principal do Nagios, e o campo documentação (Documentation), que se refere à

documentação da versão do Nagios que está sendo utilizada.

Na parte monitoramento (Current Status) tem-se o resumo de serviços, de hosts, de configuração, de monitoramento e o status da rede. É possível também visualizar os serviços e os hosts monitorados, inclusive separados por grupos que foram definidos, além do estado de cada um. Ainda na parte de monitoração, é possível visualizar o mapa da rede, os serviços com problema, a evolução e andamento do Nagios, o relatório de cada cliente, e visualizar os problemas na rede em ordem de relevância e ver onde está a causa dos problemas.

Em relatórios (Reports) é possível visualizar o intervalo de duração de cada problema ocorrido, a porcentagem de tempo em que um host ou serviço esteve em funcionamento, o histograma de um host ou serviço, a lista de alertas e as notificações do dia, e o resumo de alertas, filtrando os alertas por horas, serviços e/ou grupos.

Por último, na parte de configuração (System), é possível visualizar as configurações, os clientes e grupos de clientes, as dependências, os serviços e grupos de serviços, os comandos, os períodos de tempo e o escalonamento de notificações.



Figura 5: Interface informativa do Nagios.
Fonte: DAIBERT (2014).

(DAIBERT, 2014).

2.6 NAGVIS

O NagVis é um add-on de visualização para o Nagios, sistema bastante conhecido para gerenciamento de rede.

O NagVis pode ser usado para visualizar, por exemplo, os dados do Nagios exibindo processos de TI como um sistema de e-mail ou uma infraestrutura de rede conforme Figura 6.

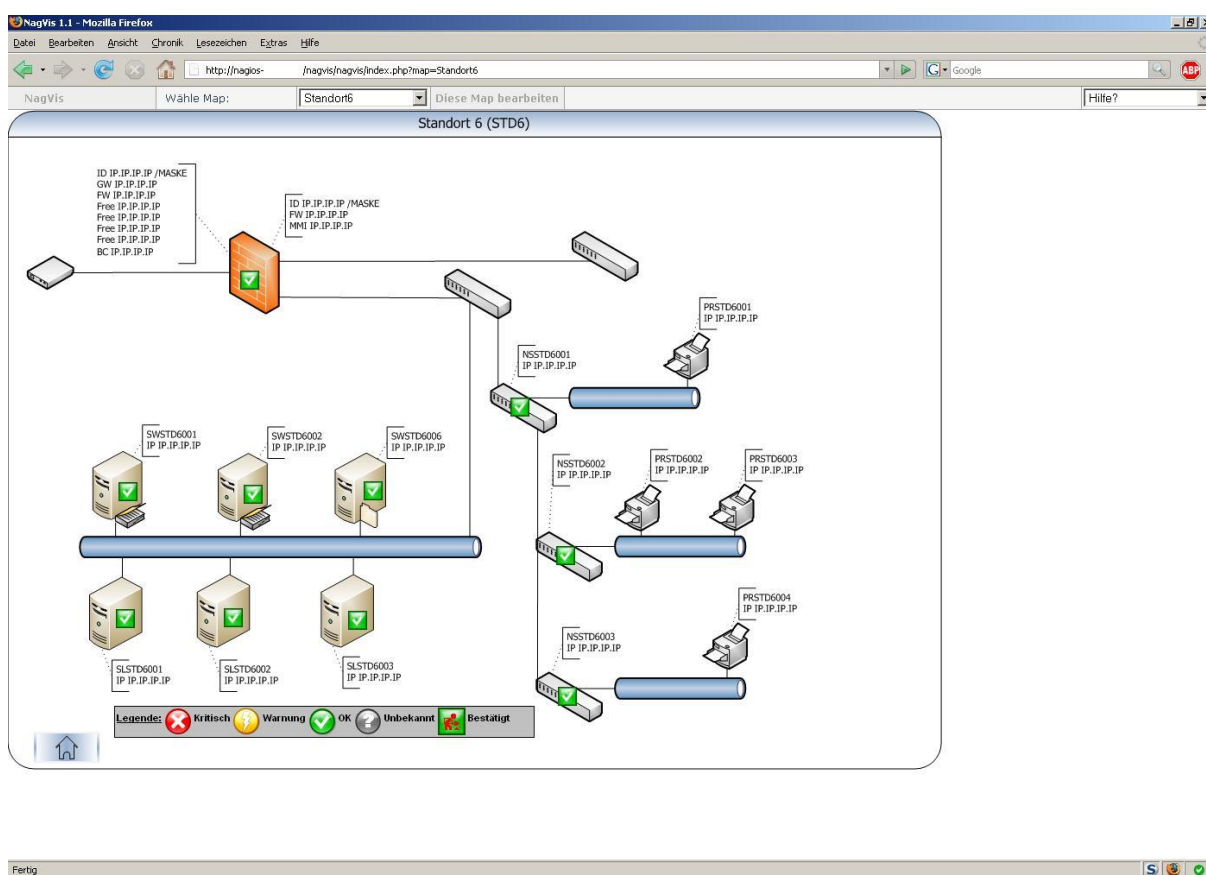


Figura 6: Virtualização de um mapa de infraestrutura de rede pelo Nagvis.
Fonte: NagVis Home (2014).

2.7 OMD – THE OPEN MONITORING DISTRIBUTION

O OMD implementa um conceito completamente novo de como instalar, manter e atualizar um sistema de monitoramento baseado no Nagios. O OMD evita o tedioso trabalho de compilação e integração manualmente de add-ons do Nagios e, ao mesmo tempo, evitando os problemas de pacotes pré-instalados que já vem com sua distribuição Linux, que são na maioria das vezes desatualizados e não fornecem atualizações regulares.

3 DESENVOLVIMENTO

O estudo de caso aqui apresentado é composto da implantação de um compilado das ferramentas Nagios/Nagvis para monitoramento dos serviços e disponibilidade dos servidores da rede da FIERN. Neste estudo de caso será considerado o monitoramento dos serviços HTTP, DNS, PROXY e disponibilidade pelo retorno do ping.

A Casa da Indústria possui atualmente 16 (Dezesseis) servidores principais para funcionamento do serviço de TI, sendo 3 (três) servidores físicos e 13 (treze) servidores virtualizados, que são:

- APPS01: Servidor de aplicações;
- APPS02: Servidor de aplicações;
- CACTI: Servidor de monitoramento do tráfego de rede;
- DC01: Servidor de controlador de domínio principal;
- DC02: Servidor de controlador de domínio secundário;
- FIREWALL: Servidor do Firewall;
- HYP01: Servidor de virtualização;
- HYP02: Servidor de virtualização;
- HYP03: Servidor de virtualização;
- KAS: Servidor com o console de administração da solução de antivírus;
- NAGIOS: Servidor do Nagios
- OCS: Servidor de inventário opensource;
- PROXY: Servidor do serviço de Proxy;
- WEB01: Servidor de hospedagem web;
- WEB02: Servidor de hospedagem web;
- WSUS: Servidor de controle de atualizações do Sistema Operacional das estações;

A casa também possui um roteador cisco que recebe um link da Oi, que também terá sua disponibilidade monitorada.

3.1 IMPLANTAÇÃO DA FERRAMENTA

O processo de instalação e configuração do Nagios e Nagvis pode ser bastante demorado, nesse estudo de caso essa instalação será simplificada, instalando o pacote OMD em um servidor com Sistema Operacional Linux usando a distribuição Debian 6, o servidor

possui a configuração abaixo:

- 2GB memória RAM;
- 100GB de HD;
- Processador Xeon;

A instalação será feita através dos repositórios fornecidos pelo desenvolvedor do OMD, antes da instalação é necessário adicionar o endereço do repositório na lista de fontes, que pode ser feito através do comando abaixo:

```
echo 'deb http://labs.consol.de/OMD/debian squeeze main' >> /etc/apt/sources.list
```

Após isso, deve-se atualizar a lista de repositórios com o comando:

```
apt-get update
```

Depois de atualizado, dar-se início à instalação usando o comando conforme Figura 7 e Figura 8.

```
root@xavier:~# aptitude install omd
Os NOVOS pacotes a seguir serão instalados:
apache2{a} apache2-mpm-prefork{ab} apache2-mpm-worker{ab} apache2-utils{a} apache2.2-bin{a}
apache2.2-common{a} curl{a} defoma{a} dialog{a} fancontrol{a} fontconfig{a} fontconfig-config{a}
fping{a} graphviz{a} libapache2-mod-fcgid{a} libapache2-mod-php5{a} libapache2-mod-proxy-html{a}
libapr1{a} libaprutil1{a} libaprutil1-dbd-sqlite3{a} libaprutil1-ldap{a}
libboost-program-options1.42.0{a} libcairo2{a} libcdt4{a} libcgraph5{a} libcurl3{a} libdat1{a}
libdbd-mysql-perl{a} libdbi-perl{a} libdbi0{a} libfile-copy-recursive-perl{a}
libfont-freetype-perl{a} libfontconfig1{a} libgd2-noxpm{ab} libgd2-xpm{ab} libgl2.0-0{a}
libgl2.0-data{a} libgraph4{a} libgvc5{a} libgvpr1{a} libhtml-template-perl{a} libjpeg62{a}
libltdl7{a} libmcrypt4{a} libmysqlclient16{a} libnet-daemon-perl{a} libnet-snmp-perl{a} libonig2{a}
libpango1.0-0{a} libpango1.0-common{a} libpathplan4{a} libperl5.10{a} libplrpc-perl{a}
libpng12-0{a} libpython2.6{a} libqdbm14{a} libsensors4{a} libsnmp-base{a} libsnmp-perl{a}
libsnmp15{a} libsqlite0{a} libssh2-1{a} libt1-5{a} libthai-data{a} libthai0{a}
libxcb-render-util0{a} libxcb-render0{a} libxdot4{a} libxft2{a} lm-sensors{a} mysql-client-5.1{a}
mysql-common{a} mysql-server{a} mysql-server-5.1{a} mysql-server-core-5.1{a} omd omd-0.54{a}
php-pear{a} php5{a} php5-cgi{a} php5-cli{a} php5-common{a} php5-gd{a} php5-mcrypt{a} php5-sqlite{a}
php5-suhosin{a} rsync{a} shared-mime-info{a} snmp{a} ssl-cert{a} ttf-dejavu-core{a}
ttf-liberation{a} unzip{a} update-inetd{a} x-ttcfidfont-conf{a} xinetd{a}
0 pacotes atualizados, 96 novos instalados, 0 a serem removidos e 0 não atualizados.
É preciso obter 139 MB de arquivos. Depois do desempacotamento, 423 MB serão usados.
Os pacotes a seguir possuem dependências não satisfeitas:
apache2-mpm-prefork: Conflita: apache2-mpm o qual é um pacote virtual.
libgd2-noxpm: Conflita: libgd2 o qual é um pacote virtual.
Conflita: libgd2-xpm mas 2.0.36~rc1~dfsg-5 será instalado.
libgd2-xpm: Conflita: libgd2 o qual é um pacote virtual.
Conflita: libgd2-noxpm mas 2.0.36~rc1~dfsg-5 será instalado.
apache2-mpm-worker: Conflita: apache2-mpm o qual é um pacote virtual.
As seguintes ações resolverão estas dependências:

Manter os pacotes a seguir em suas versões atuais:
1) apache2-mpm-prefork [Não Instalado]
2) libapache2-mod-php5 [Não Instalado]
3) libgd2-noxpm [Não Instalado]

Aceitar esta solução? [Y/n/q/?] █
```

Figura 7: Instalação do OMD.
Fonte: Elaboração própria.

apache2-mpm-worker: Conflita: apache2-mpm o qual é um pacote virtual.
As seguintes ações resolverão estas dependências:

Manter os pacotes a seguir em suas versões atuais:

- 1) apache2-mpm-prefork [Não Instalado]
- 2) libapache2-mod-php5 [Não Instalado]
- 3) libgd2-noxpm [Não Instalado]

Aceitar esta solução? [Y/n/q/?] Y

Os NOVOS pacotes a seguir serão instalados:

```
apache2{a} apache2-mpm-worker{a} apache2-utils{a} apache2.2-bin{a} apache2.2-common{a} curl{a}
defoma{a} dialog{a} fancontrol{a} fontconfig{a} fontconfig-config{a} fping{a} graphviz{a}
libapache2-mod-fcgid{a} libapache2-mod-proxy-html{a} libapr1{a} libaprutil1{a}
libaprutil1-dbd-sqlite3{a} libaprutil1-ldap{a} libboost-program-options1.42.0{a} libcairo2{a}
libcddt4{a} libcglib5{a} libcurl3{a} libdatatree1{a} libdbd-mysql-perl{a} libdbi-perl{a} libdbi0{a}
libfile-copy-recursive-perl{a} libfont-freetype-perl{a} libfontconfig1{a} libgd2-xpm{a}
libglb2.0-0{a} libglb2.0-data{a} libgraph4{a} libgvc5{a} libgvpr1{a} libhtml-template-perl{a}
libjpeg62{a} libltdl7{a} libmccrypt4{a} libmysqlclient16{a} libnet-daemon-perl{a}
libnet-snmp-perl{a} libonig2{a} libpango1.0-0{a} libpango1.0-common{a} libpathplan4{a}
libperl5.10{a} libplrpc-perl{a} libpng12-0{a} libpython2.6{a} libqdbm14{a} libsensors4{a}
libsnmp-base{a} libsnmp-perl{a} libsnmp15{a} libsqlite0{a} libssh2-1{a} libt1-5{a} libthai-data{a}
libthai0{a} libxcb-render-util0{a} libxcb-render0{a} libxdot4{a} libxft2{a} lm-sensors{a}
mysql-client-5.1{a} mysql-common{a} mysql-server{a} mysql-server-5.1{a} mysql-server-core-5.1{a}
omd omd-0.54{a} php-pear{a} php5{a} php5-cgi{a} php5-cli{a} php5-common{a} php5-gd{a}
php5-mcrypt{a} php5-sqlite{a} php5-suhosin{a} rsync{a} shared-mime-info{a} snmp{a} ssl-cert{a}
ttf-dejavu-core{a} ttf-liberation{a} unzip{a} update-inetd{a} x-ttcidfont-conf{a} xinetd{a}
```

0 pacotes atualizados, 93 novos instalados, 0 a serem removidos e 0 não atualizados.

É preciso obter 136 MB de arquivos. Depois do desempacotamento, 415 MB serão usados.

Você deseja continuar? [Y/n/?] Y

AVISO: versões não confiáveis dos seguintes pacotes serão instaladas!

Pacotes não confiáveis podem comprometer a segurança de seu sistema.
Você deveria prosseguir com a instalação somente se estiver certo de
que isso é realmente o que você deseja fazer.

omd omd-0.54

Você deseja ignorar este aviso e continuar mesmo assim?

Para continuar, digite "Sim"; para abortar, digite "Não":Sim

Figura 8: Continuando a instalação do OMD.

Fonte: Elaboração própria.

Durante a instalação será solicitada uma senha para o banco de dados MYSQL, conforme Figura 9.

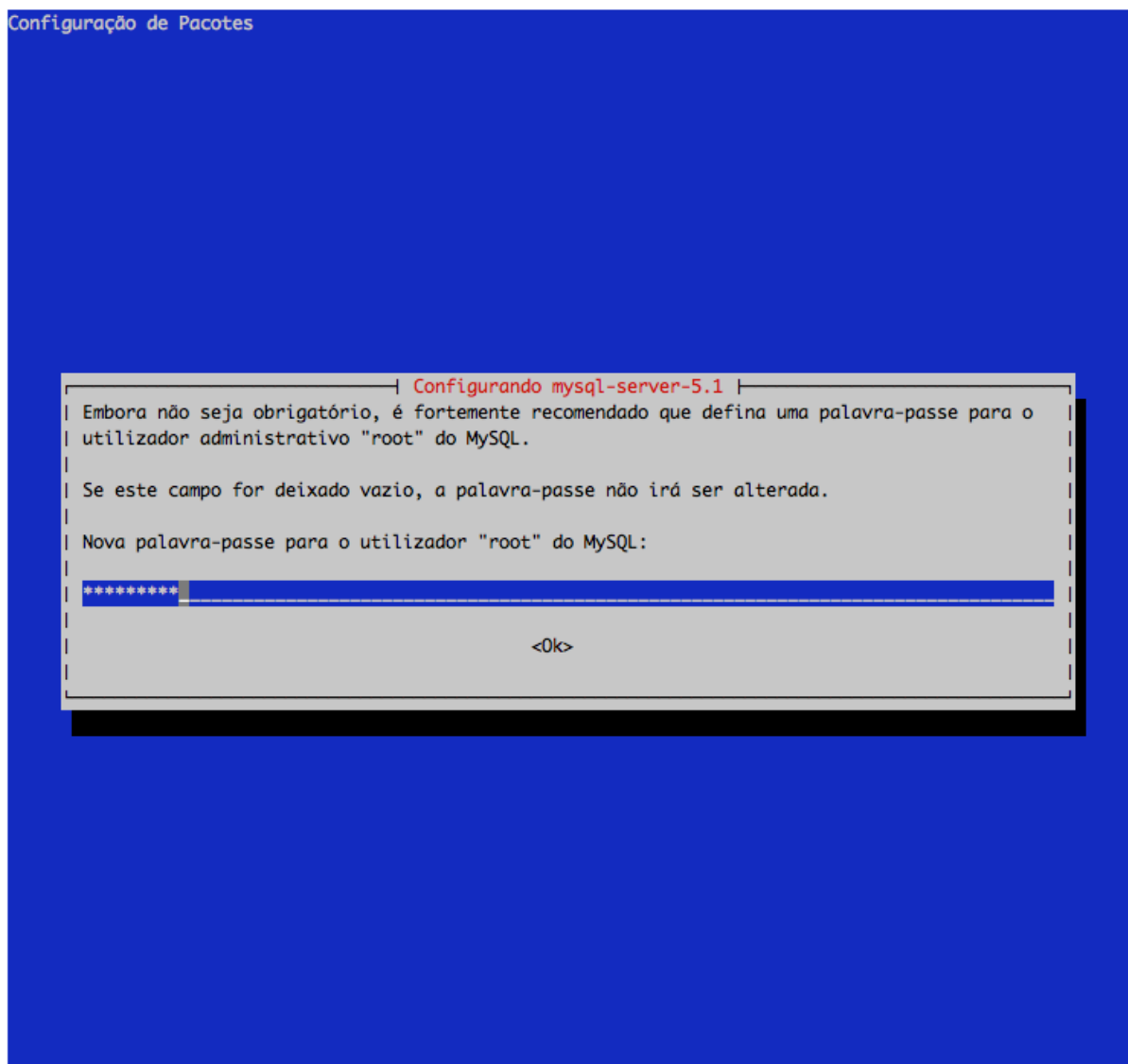


Figura 9: Definindo uma senha para o banco MySQL.

Fonte: Elaboração própria.

Após a instalação do pacote, será criada uma instância, chamada NOC, essa instância irá concentrar as ferramentas Nagios e NagVis, conforme Figura 10.

```
root@xavier:~# omd create noc
Adding /omd/sites/noc/tmp to /etc/fstab.
Restarting Apache...apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
OK
Creating temporary filesystem /omd/sites/noc/tmp...OK
Created new site noc with version 0.54.

The site can be started with omd start noc.
The default web UI is available at http://xavier/noc/
The admin user for the web applications is omdadmin with password omd.
Please do a su - noc for administration of this site.

root@xavier:~#
```

Figura 10: Criação da instância.

Fonte: Elaboração própria.

Após a criação da instancia é necessário inicia-la conforme Figura 11.

```
root@xavier:~# omd start noc
Starting dedicated Apache for site noc...OK
Starting rrdcached...OK
Starting npcd...OK
Starting nagios...OK
Initializing Crontab...OK
root@xavier:~# █
```

Figura 11: Iniciando a instância.

Fonte: Elaboração própria.

Agora já é possível acessar o Nagios criado pela instância NOC via interface web pelo endereço IP, conforme Figura 12:

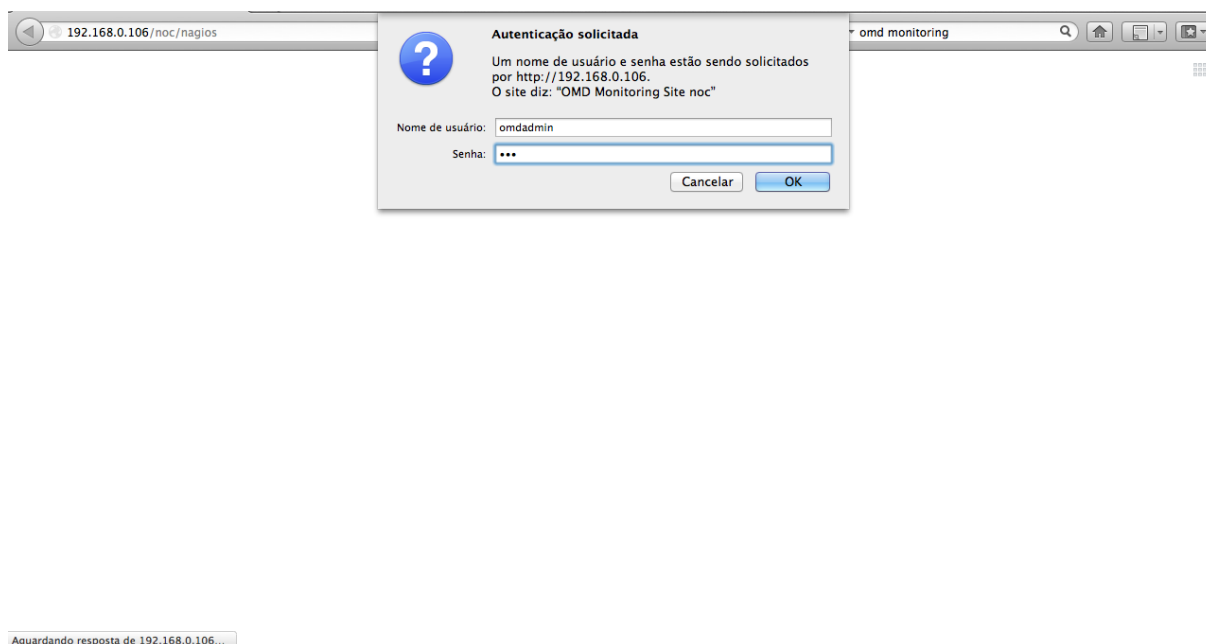


Figura 12: Acessando a interface web.

Fonte: Elaboração própria.

A princípio não existirá nenhum host sendo monitorado, pois o sistema acaba de ser instalado conforme Figura 13 e Figura 14:



Figura 13: Interface web do Nagios.
Fonte: Elaboração própria.

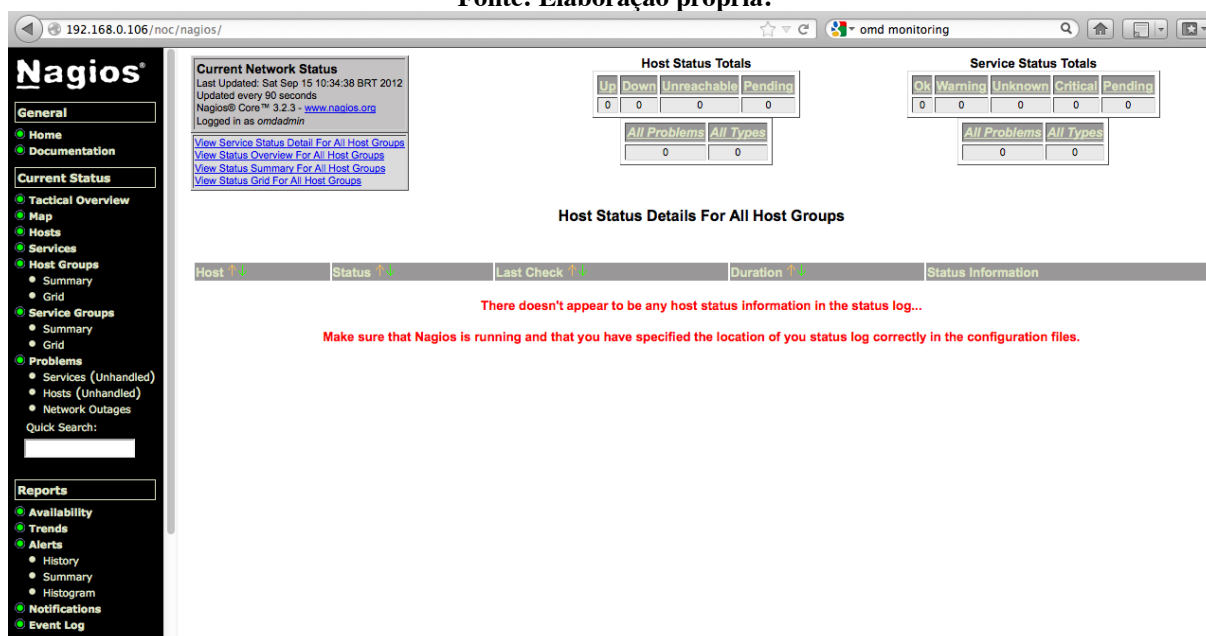


Figura 14: Interface web do Nagios.
Fonte: Elaboração própria.

Agora deve-se adicionar o template de monitoramento para depois criar os hosts. O seguinte template será adicionado ao arquivo “check_mk_templates.cfg”:

```
# Template de hosts Fiern
define host{
    name                check_fiern;
    use                  generic-host;
    check_period         24x7;
    check_interval       1;
    retry_interval       1;
    max_check_attempts   3;
    check_command         check-host-alive;
    notification_period   24x7;
```

```

notification_interval      120;
notification_options       d,u,r,f;
contact_groups             fiern;
register                   0;
}

```

Os itens configurados neste template são:

- use - define o template padrão do host, no exemplo é utilizado o generic-host;
- name - define o nome do template;
- Check_command - é o nome abreviado do comando que deverá ser usado para verificar se o cliente está funcionando ou não;
- Max_check_attempts - é a diretiva usada para definir o número máximo de vezes que o programa irá checar pelo serviço até reportar um erro;
- Notification_interval - é definido o tempo de espera para renotificar o contato sobre a situação do estado do cliente;
- Notification_period - define o período de tempo no qual as notificações de eventos de um cliente podem ser envidas aos contatos;
- Notification_options - utilizada para determinar quando a ferramenta poderá enviar notificações para o usuário administrador, onde d = enviar notificação em estados DOWN (inativo), u = enviar notificações em estados UNREACHABLE (inacessível), e r = enviar notificações nas recuperações, ou seja, quando o host volta a ficar ativo.
- Contact_groups - define o grupo de contatos que receberão as notificações dos clientes.

Após as configurações do template, deve-se adicionar a configuração de cada host e os seus respectivos serviços, alguns hosts não terão serviços monitorados, apenas sua disponibilidade, o início será dado com a adição do host para monitoramento do roteador que fornece o link de internet, será criado um arquivo com extensão “.cfg” onde serão adicionadas as seguintes linhas de parâmetros:

```

define host {
    use                check_fiern
    host_name          router
    alias              Router - 200.164.229.145
    address             200.164.229.145
    display_name       Router
}

```

Nesse caso, será monitorado apenas o endereço IP do roteador, afim de obter informações sobre sua disponibilidade, essa configuração será semelhante em todos os hosts que não tem serviços a serem monitorados.

Na sequência, será criado o monitoramento de um host que possui o serviço de Servidor DNS, nesse caso o controlador de domínio, o mesmo irá receber os seguintes parâmetros, essa configuração será semelhante aos hosts que possuem serviços a serem monitorados, alterando o comando de checagem do serviço para seu respectivo serviço:

```
define host {
    parents                router
    use                    check_fiern
    host_name              dc01
    alias                 DC01 - 10.134.25.155
    address               10.134.25.155
    display_name           FIERN - DC01
}

define service {
    use                    generic-service
    host_name             dc01
    service_description    DNS
    display_name          DNS
    check_command          check_dns!www.google.com!10.134.25.155
    register              1
}
```

Após a criação dos hosts, o servidor do Nagios dará início a checagem dos hosts e seus serviços, conforme pode ser visto na Figura 15 e Figura 16.

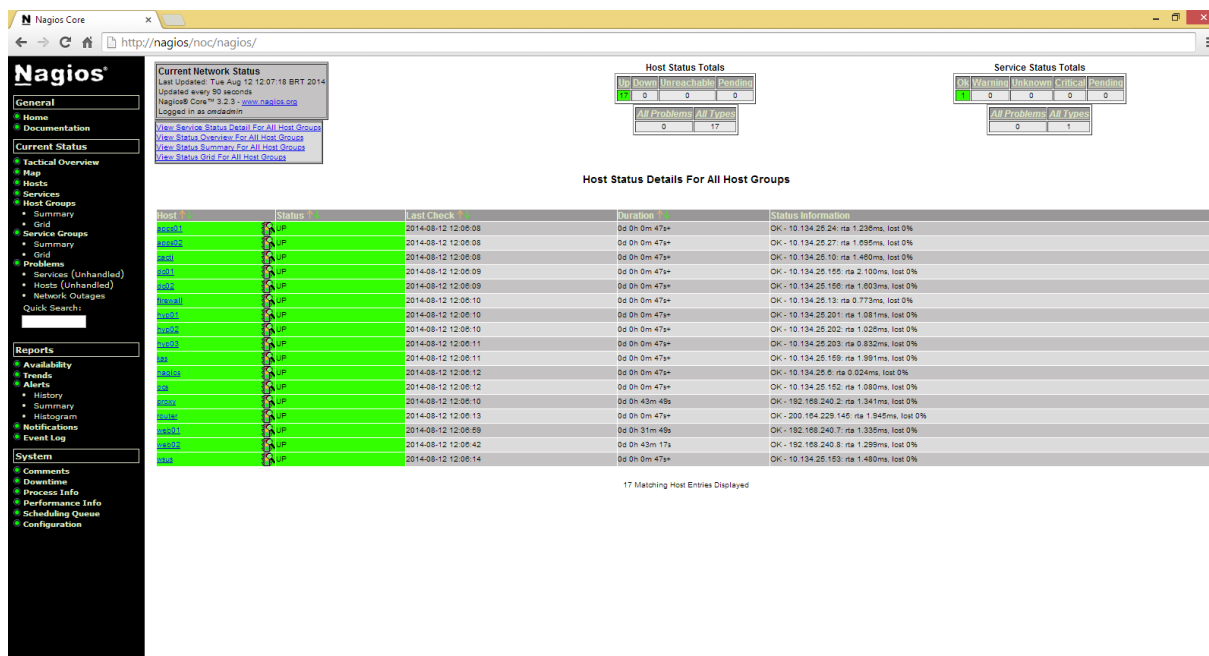


Figura 15: Hosts no Nagios.
Fonte: Elaboração própria.

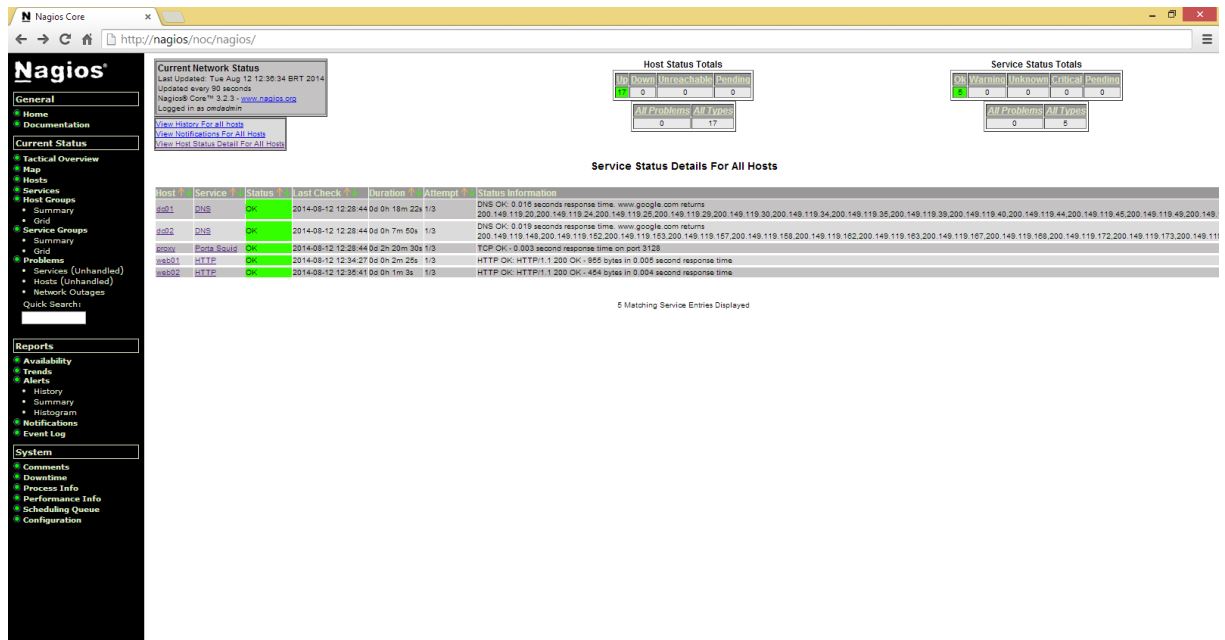


Figura 16: Serviços no Nagios.

Fonte: Elaboração própria.

Após a criação dos hosts e seus serviços é hora de colocar os mesmos para serem visualizados através do Nagvis, a princípio deve-se criar uma imagem com o diagrama da rede utilizando a ferramenta Visio da Microsoft, nele pode-se desenhar os hosts que serão monitorados para facilitar o entendimento visual, como pode ser visto na Figura 17.

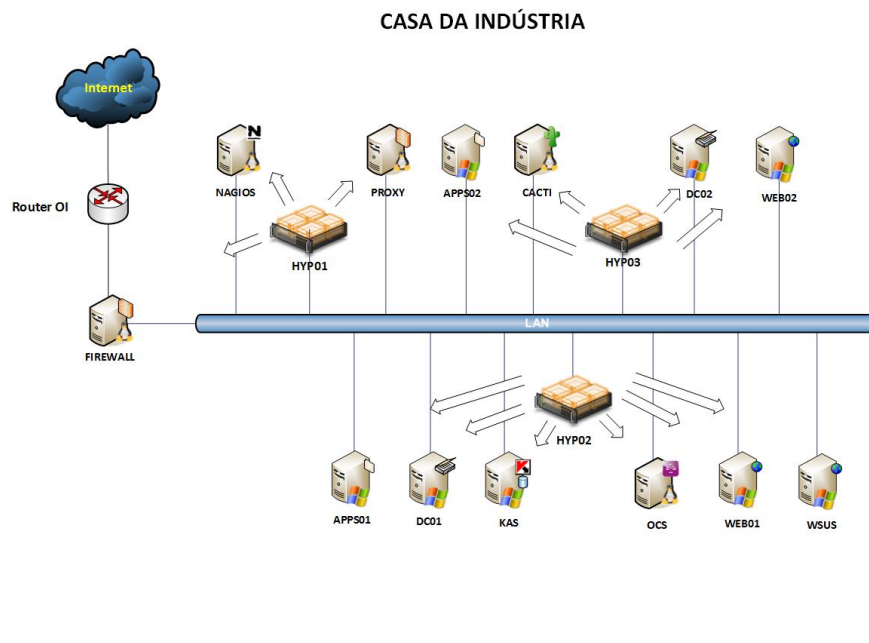


Figura 17: Diagrama da rede.

Fonte: Elaboração própria.

Após criado o diagrama da rede, deve-se criar o mapa de monitoramento no Nagvis, conforme pode ser visto na Figura 18.

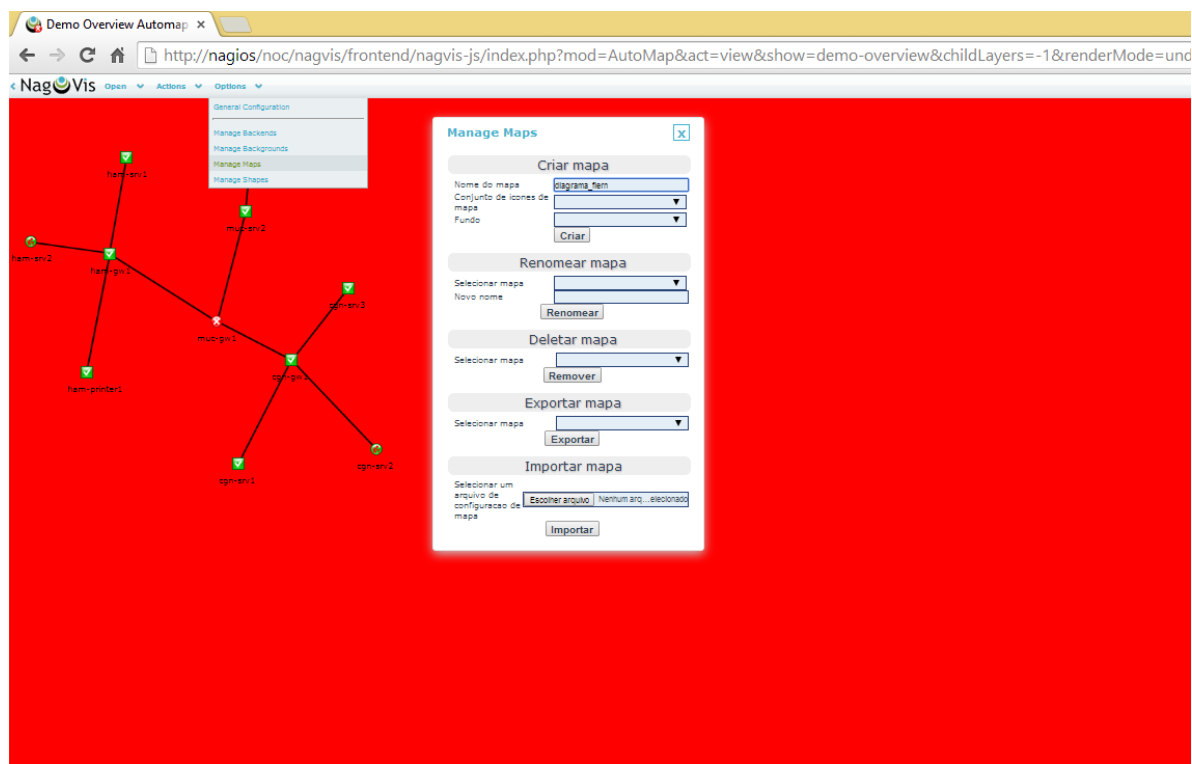


Figura 18: Criação do mapa no Nagvis.

Fonte: Elaboração própria.

Após a criação do mapa, deve-se fazer o upload da imagem do diagrama da rede que irá funcionar como imagem de fundo do mapa, como pode ser visto na Figura 19.

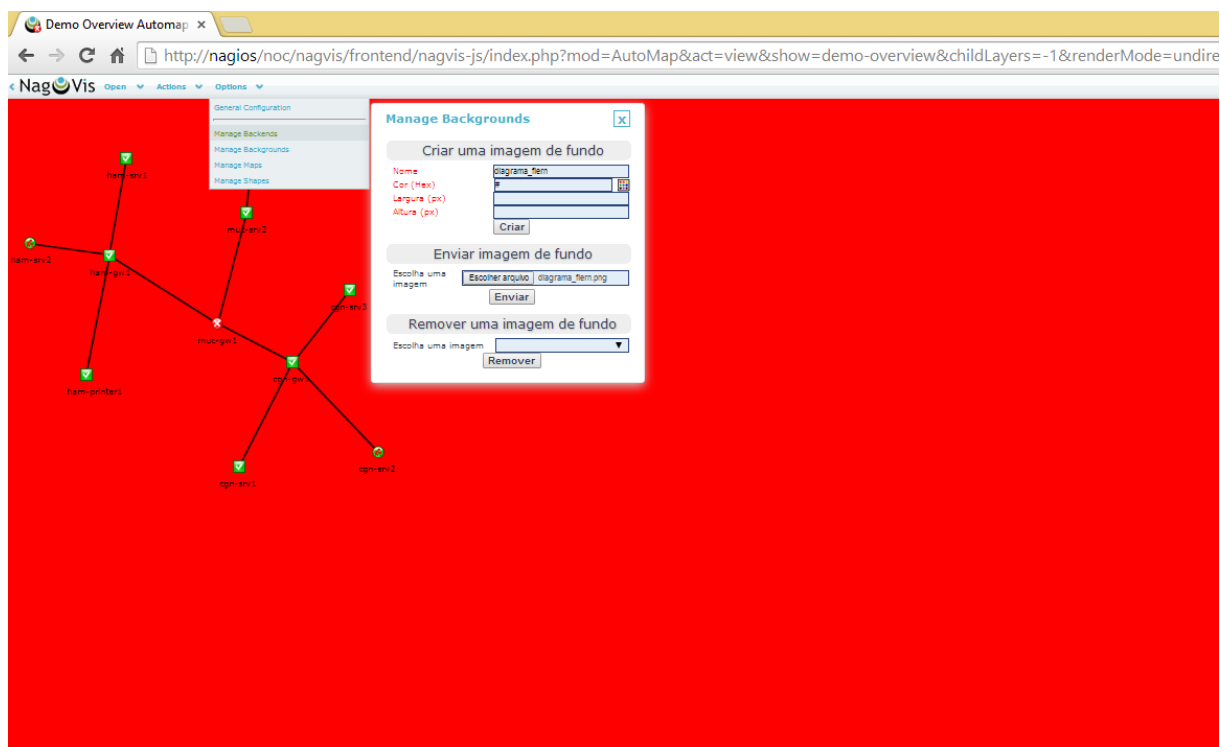


Figura 19: Adicionado imagem de fundo ao mapa no Nagvis.

Fonte: Elaboração própria.

Após a criação do mapa deve-se adicionar os hosts ao mesmo em suas respectivas localizações, como pode ser visto na Figura 20.

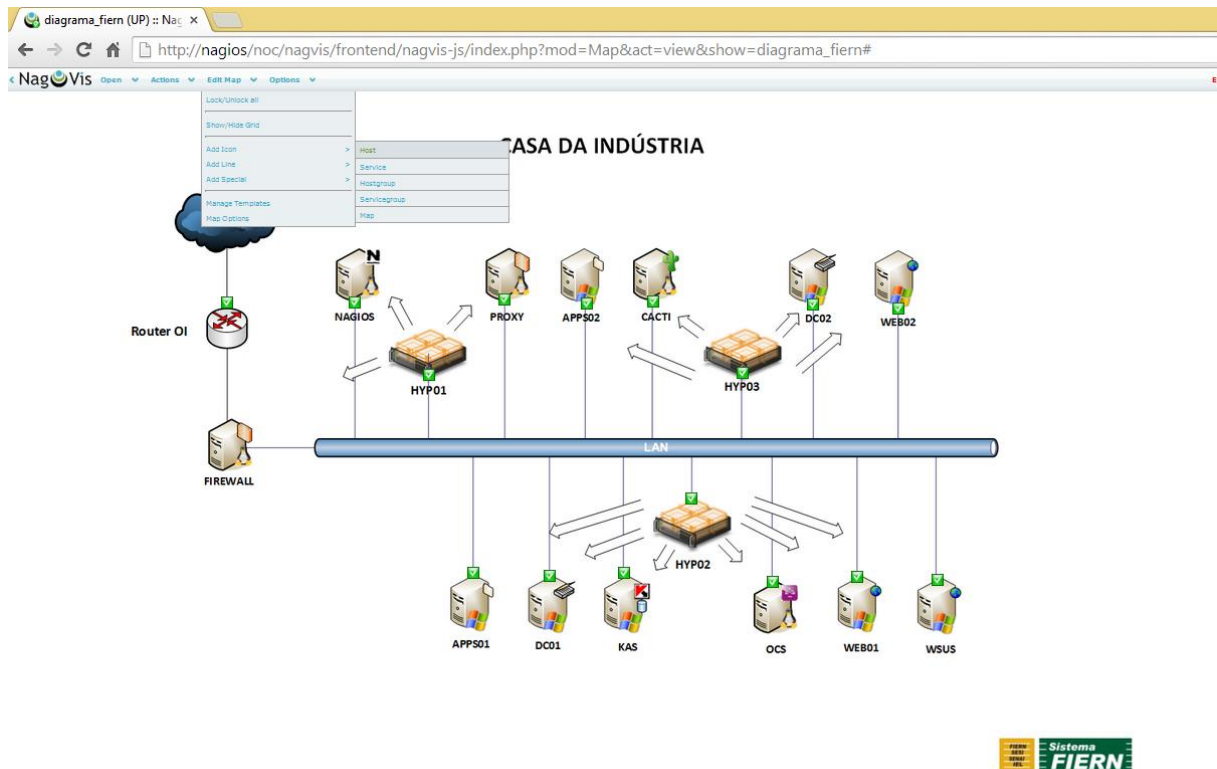


Figura 20: Adicionando hosts no mapa.

Fonte: Elaboração própria.

Após os hosts e seus serviços serem adicionados no mapa, pode-se exibir informações sobre o monitoramento de cada um deles descansando o mouse em cima do host, conforme pode ser visto na Figura 21.

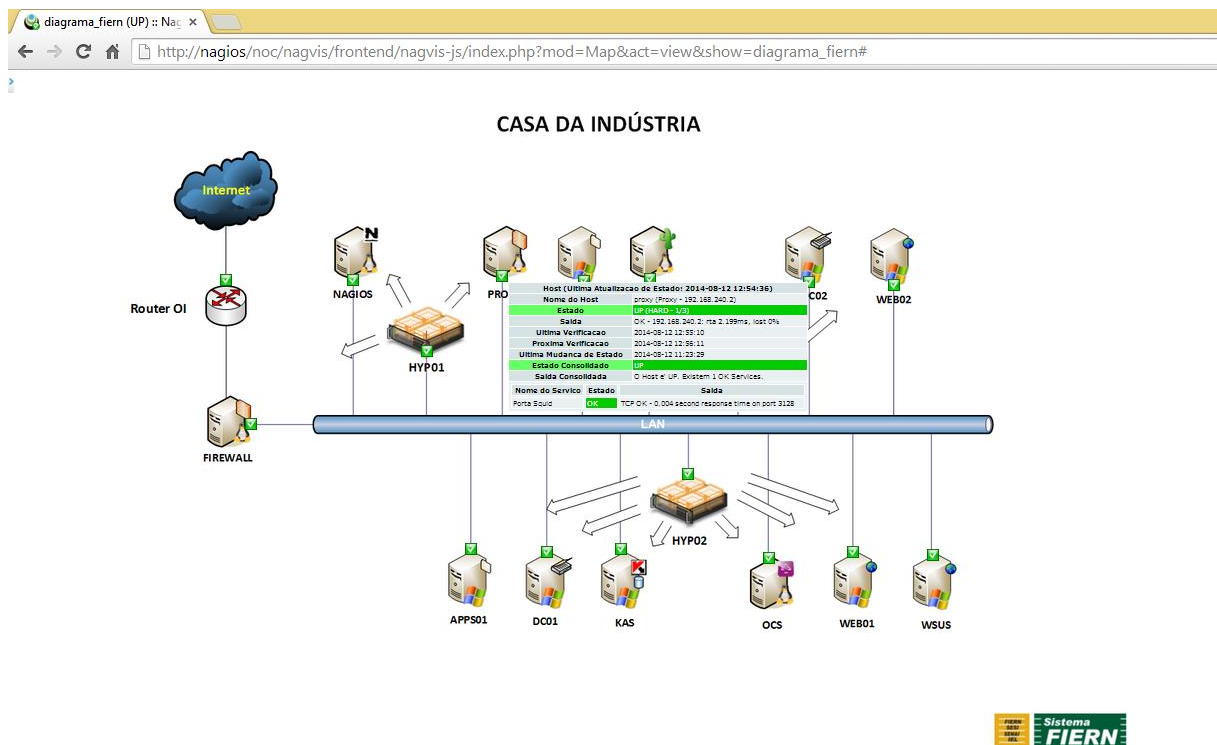


Figura 21: Detalhe de monitoramento do host.

Fonte: Elaboração própria.

4 CONCLUSÃO

Este trabalho procurou apresentar a importância de monitorar redes e ativos de rede através de um Centro de Operações de Rede. Muitos são os desafios para o gerenciamento de uma rede e seus ativos, tendo como premissa a manutenção de sua disponibilidade.

Assim, com a utilização de ferramentas de monitoramento, é possível acompanhar o comportamento dos serviços disponibilizados e manter o desempenho, disponibilidade e estabilidade num ambiente computacional, podendo evitar falhas e problemas na rede.

Vimos também que com o aumento na utilização das redes, um sistema de gerenciamento de redes torna-se cada vez mais indispensável. Entretanto, muitas vezes não se sabe qual seria a melhor solução que atenderia às suas necessidades devido às diferentes características de cada ferramenta. Todas elas tratam um único assunto que é ajudar a manter o bom funcionamento da rede, ou seja, melhorando a confiabilidade e segurança dos dados e recursos disponíveis aos usuários da mesma.

Por fim, vimos que o Nagios é uma ferramenta open source de monitoramento de redes que verifica constantemente a disponibilidade do serviço, seja local ou remoto, e avisa por meio de e-mail, celular e alerta sonoro sobre o problema ocorrido. Além disso, é possível obter relatórios de disponibilidade e configurar ações corretivas para os problemas ocorridos na rede. Com a utilização do Nagios foi possível detectar problemas com serviços de rede mais rapidamente, identificando o que poderia afetar a disponibilidade do sistema utilizado pela FIERN de forma confiável, e obtendo relatórios com informações precisas, possibilitando acompanhar o funcionamento dos serviços e da rede como um todo.

REFERÊNCIAS

DAIBERT, Marcelo Santos. **Monitoramento de Redes de Computadores**. Disponível em: <http://www.devmedia.com.br/websys.4/webreader.asp?cat=62&revista=inframagazine_1#a-3510>. Acesso em: 10 jun. 2014.

FREITAS, Marcos André dos Santos. **Fundamentos do Gerenciamento de Serviços de TI**. Rio de Janeiro: Brasport, 2010.

O PORTAL oficial do projeto NagVis. Disponível em: <<http://www.nagvis.org/about>>. Acesso em: 11 jun. 2014.

O PORTAL oficial do projeto OMD. Disponível em: <<http://www.omdistro.org>>. Acesso em: 09 jun. 2014.