UNIVERSIDADE FEDERAL FLUMINENSE

SEAN STEWART FAULSTICH CRAMMOND

UMA INFRAESTRUTURA DE MONITORAMENTO PARA A REDE DO INSTITUTO DE COMPUTAÇÃO DA UFF

NITERÓI

2012

UNIVERSIDADE FEDERAL FLUMINENSE

SEAN STEWART FAULSTICH CRAMMOND

UMA INFRAESTRUTURA DE MONITORAMENTO PARA A REDE DO INSTITUTO DE COMPUTAÇÃO DA UFF

Trabalho submetido ao Curso de Bacharelado em Ciência da Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação. Área de concentração: Processamento paralelo e distribuído.

Orientador:
Prof. PhD. EUGENE FRANCIS VINOD REBELLO

NITERÓI

2012

Uma Infraestrutura de Monitoramento Para a Rede do Instituto de Computação da UFF

Sean Stewart Faulstich Crammond

Trabalho submetido ao Curso de Bacharelado em Ciência da Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação.

Aprovada por:

Prof. PhD. Eugene Francis Vinod Rebello / IC-UFF
(Presidente)

Profa. D.Sc. Aline de Paula Nascimento / IC-UF

Profa. PhD. Maria Cristina Silva Boeres / IC-UFF

Niterói, 26 de outubro de 2012.

Dedico este trabalho a minha querida mãe,
minha rocha.

Agradecimentos

Agradeço a equipe do suporte do IC, sem eles este trabalho não seria possível. Agradeço aos meus amigos, que fizeram dessa jornada acadêmica a mais divertida possível. Agradeço ao professor Vinod por ter visto potencial em mim e por fim a minha família por ter me ajudado nessa minha importante jornada.

Resumo

Redes de computadores crescem e se proliferam, em resposta a necessidade de se compartilhar recursos lógicos e físicos para processamento das informações criadas em empresas e ambientes de pesquisa e ensino em todo mundo. Estas redes são sujeitas a acessos não autorizados bem como falhas no fluxo de informação entre os nós, além de falhas nos próprios nós. Monitorar essas redes é de extrema importância, para saber de problemas assim que estes aconteçam, bem como poder prever possíveis problemas, sendo assim vital para que a informação que nelas trafegam não sofram interferências. Muitas redes consistem de milhares de computadores e servidores, separados geograficamente uns dos outros e com serviços diferentes que requerem atenção, tornando muito complexo a sua administração. Para que os administradores possam ter o domínio delas, os administradores dispõem de ferramentas de monitoramento para tornar o trabalho de administração da rede mais fácil. Neste projeto discutiremos o uso de algumas destas ferramentas e proporemos um modelo de monitoramento para a rede do Instituto de Computação da Universidade Federal Fluminense.

Palavras-chave: Redes Computacionais, Monitoramento, Ferramentas de Monitoramento

Abstract

Computer networks grow and proliferate in response to the need to share resources for physical and logical processing of information created in companies and research and teaching environments worldwide. These networks are subject to unauthorized access, flaws in the flow of information between nodes as well as failures in the nodes themselves. Monitoring these networks is very important in order to be aware of problems as soon as they happen, as well as to be able to anticipate potential problems, so that communication of information and access to services being provide by IT systems suffer from the minimum of interference. Many networks consist of thousands of computers and servers, often geographically separated from each other, with different services that require different degrees of attention, thus making computing infrastructures very complex to administer. Network administrators have turned to the adoption of monitoring tools to make their work easier. In this project, we will discuss the use of some of these tools and propose a model for monitoring the network of the Institute of Computing from Federal Fluminense University.

Keywords: Computer Networking, Monitoring, Monitoring Tools

Palavras-chave

1. Redes de Computadores
2. Monitoramento
3. Ferramentas de Monitoramento

Glossário

IC	:	Instituto de Computação da UFF;
NAGIOS	:	Nagios Core;
TI	:	Tecnologia da Informação;

Sumário

Lista de Figuras

Capítulo 1

Introdução

Vivemos em um mundo onde acesso a informação é vital. No ponto de vista financeiro, empresas podem perder muito dinheiro se acontecer uma interrupção no tráfego da rede pelo qual passam suas informações, caso um banco sofrer um problema em sua rede, seus correntistas não teriam acesso a suas contas, podendo criar sérios problemas. Discutiremos isso mais profundamente no capítulo 2. No ponto de vista científico, resultados de pesquisas podem ser perdidas caso aconteça algum problema aonde ela é mantida. As redes as quais essas informações trafegam devem estar funcionando, bem como as informações que ali trafegam devem estar íntegras. Para tal, são necessárias ferramentas de acompanhamento que reportem qualquer problema e de forma rápida, para minimização dos prejuízos.

Grandes empresas e instituições de ensino e pesquisa têm centros espalhados em todos os cantos da Terra, conectados em rede entre eles, tornando difícil o acompanhamento pleno de suas funções.

Para tal monitoramento, os administradores de rede têm a possibilidade de verificar vários protocolos de redes para checar irregularidades. Alguns amplamente usados para isso são: SNMP, telnet, ICMP, entre outros.

Aos administradores de rede cria-se um problema: como monitorar suas redes, de forma a prevenir possíveis problemas ou solucioná-los, caso por ventura venham a acontecer? A resposta foi o surgimento de ferramentas de monitoramento capazes de observar os vários tipos de redes, que se adaptam a estas. Além disso, essas ferramentas avisam a equipe de apoio qual nó da rede é o problemático, fornecendo os dados importantes para que seja possível a equipe solucionar o problema.

Há, neste universo, várias ferramentas para os mais diversos tipos de monitoramento, por exemplo, ferramentas que monitoram intrusões numa rede (Snort) [1], outras que monitoram o desempenho das aplicações que rodam nas máquinas da rede (CA introscope) [2]. Existem também as ferramentas que monitoram a saúde (estado) das máquinas na rede, além de alguns serviços que elas provêm.

Neste trabalho, o foco será sobre o último grupo de ferramentas de monitoramento apresentadas no parágrafo anterior e em como usá-las para auxiliar os mantenedores da rede na solução de problemas que venham a surgir e em sua prevenção futura.

Como um estudo de caso neste trabalho, estudamos a topologia de rede do Instituto de Computação da Universidade Federal Fluminense, mais especificamente os servidores e firewalls dela, que em conjunto formam a espinha dorsal do funcionamento da rede deste instituto. Entrevistamos os funcionários e alunos que cuidam destes servidores para sabermos quais serviços de quais máquinas são importantes e que deveriam ser priorizados, bem como os níveis e frequências dos alarmes de avisos que deveriam ser definidos. Por fim, um modelo de monitoramento foi implementado e avaliado.

No capítulo 2 abordaremos os conceitos básicos das ferramentas de monitoramento, falando um pouco das ferramentas mais famosas, e quais são os diferenciais delas.

No capítulo 3 falaremos da ferramenta escolhida para o trabalho, a ferramenta nagios, dando um breve histórico dela, suas funcionalidades e explicando o motivo de ser a escolhida.

No capítulo 4 será onde mostraremos a solução adotada. Descreveremos a topologia de rede do Instituto de Computação e explicaremos a solução criada.

No capítulo 5 analisaremos a ferramenta em questão através de relatórios de disponibilidade para mostrar que o comportamento dos servidores. Mostraremos que com a ajuda dela podemos observar problemas em máquinas e assim corrigi - los.Por fim, no capítulo 6, será mostrado a conclusão do trabalho e possíveis trabalhos futuros.

Capítulo 2

Conceitos Básicos de Ferramentas de Monitoração

O objetivo deste capítulo é apresentar alguns conceitos de monitoramento e sua importância nas redes de computadores atuais. Apresentaremos 5 ferramentas de monitoramento usadas atualmente no mercado, mostrando suas principais características e explicitando seus funcionamentos.

2.1 Conceitos

O que significa monitoramento? Monitorar, é observar, atentar aos desvios e perceber os sinais de alerta. Podemos expandir esta definição e dizer que a monitoração é um processo de controle que serve para que se tenha completa ciência do ambiente que se observa. Podemos através da observação, solucionar problemas que apareçam com mais agilidade, bem como prever problemas vindouros, através de análise do histórico das observações feitas em um dado ambiente, por essa análise, podemos ver se as ações tomadas para solução de problemas surtiram o efeito esperado ou se outras ações são necessárias. Para tornar mais fácil o trabalho de observação desses ambientes, são usadas ferramentas de monitoramento, desenvolvidas para os mais específicos fins. Temos diversas ferramentas de monitoramento, como os sistemas de suporte a vida que verificam a pressão do sangue do paciente, bem como a pressão intracraniana e o funcionamento do coração, fornecendo dados e auxiliando os médicos em manter pacientes vivos. Ferramentas de monitoramento que monitoram sistemas aeroviários, que auxiliam aos controladores de tráfego mostrando a posição dos aviões no céu e impedindo acidentes. Minas extratoras também precisam de

monitoramento. Para proteger a vida dos trabalhadores sensores monitoram a qualidade do ar em seu interior bem como deslocamentos de terra e a menor alteração, é possível evacuar a mina com o máximo de segurança. Para atestar a validade de uma transação financeira, tal com um pagamento, por exemplo, é necessário monitorar todo o fluxo da transação e ser capaz de responder a um erro, caso ele aparecer. Em nosso estudo, abordaremos as ferramentas de monitoramento utilizadas em redes computacionais.

A wikipedia[3] define que uma ferramenta de monitoramento de sistemas de computadores é um sistema que constantemente monitora uma rede de computadores para buscar em seus componentes formadores aqueles que estejam se comportando de forma lenta (desempenho lento) ou que estejam apresentando algum tipo de falha, notificando o administrador desta rede (por email, SMS ou outra forma de aviso) no caso da falha. Já Kim S. Nash e Alyson Behr[4] definem como uma função critica de TI que economiza dinheiro, melhorando a produtividade de empregados e previne excesso de custos de infraestrutura, ajudando também na melhoria da performance da rede observada. Através da monitoração podemos indentificar equipamentos que estejam sobrecarregados, gargalos de rede, bem como identificar o motivo pelo qual uma sessão de email foi perdida. A definição também diz que o monitoramento pode ajudar a resolver lentidão de sites, utilização "questionável" de recursos da rede por parte de usuários, além do estado de "offline" dos servidores. Esses autores traçam um paralelo de monitoramento como uma ida ao cardiologista, enquanto o médico procura sinais de perigo ao analisar o fluxo de sangue que passa pelo coração do paciente através das artérias e veias, o administrador de rede vai procurar sinais de perigo no fluxo de dados que passam pelos cabos e fibras-óticas e chegam nos servidores de uma rede computacional. Há vários sistemas de monitoramento, otimizados e adaptados para as mais diversas funções, para as mais variadas estruturas.

Por que devemos monitorar essas redes? De acordo com Stuart J. Johnston[5], que escreveu o artigo "*Cloud outage report of 13 providers reveals downtime costs*", diz que downtimes de serviços de computação em nuvem que durem mais de 10 horas por ano podem gerar prejuízos de 70 Milhões de dólares.

Na sessão 2.2, será mostrado algumas ferramentas utilizadas largamente pelos administradores de rede e para qual finalidade foram desenvolvidas

2.2 Ferramentas

Nessa seção, falaremos sobre algumas ferramentas de monitoramento, para o que foram feitas e suas qualidades e defeitos[6]. Algumas dessas ferramentas foram implementadas para o estudo para podermos entender seu funcionamento profundamente (Cacti e Ganglia).

2.2.1 Ganglia

Ganglia[7] é um sistema de monitoramento distribuído e escalável feito para sistemas de computadores de alto desempenho, tais como clusters e grades computacionais. Ele permite que o seu usuário possa, remotamente, observar estatísticas e atuais ou históricas de todas as maquinas que estão sendo monitoradas. Ganglia usa xml para representar seu dados, XDR (External Data Representation) como protocolo de transferência de dados e RRDtools para visualização desses dados. O ganglia é um projeto nascido da Universidade da California e inicialmente fazia parte do Projeto MILLENNIUM (Millenium project).

O Ganglia para funcionar utiliza 2 daemons e um frontend web para mostrar as métricas coletadas pela ferramenta, podendo se utilizar de vários outros programas utilitários. O gmond é um daemon multi-thread que deve rodar em todo nó do cluster que se quer monitorar, basicamente monitora mudanças no host, anuncia mudanças relevantes, escuta mudanças relevantes de outros nós via canal multicast ou unicast e responde requerimentos para um XML descritor de um estado do cluster. O gmetad é o daemon que organiza todos os dados coletados pelos daemons gmond dos nós do cluster, sendo este o único modo de monitoramento da ferramenta. O frontend prove a visão de todos os dados coletados para os administradores e usuários. A ferramenta Ganglia requer observação constante por parte dos administradores da rede que ela monitora, visto que ela não tem a opção de configuração de alertas em caso de problema na rede. Sua função é mostrar o funcionamento da rede. Vemos uma foto do front-end da ferramenta na figura 2.1.

2.2.2 Cacti

Cacti[8] é uma ferramenta de monitoramento e de geração de gráficos com código aberto, desenvolvida para ser um frontend para a ferramenta de data-logging RRDTools (programa que lê dados e cria gráficos com esses gráficos) e ser acessado via internet(web-based). Cacti permite a um usuário executar um poll de serviços em determinados in-

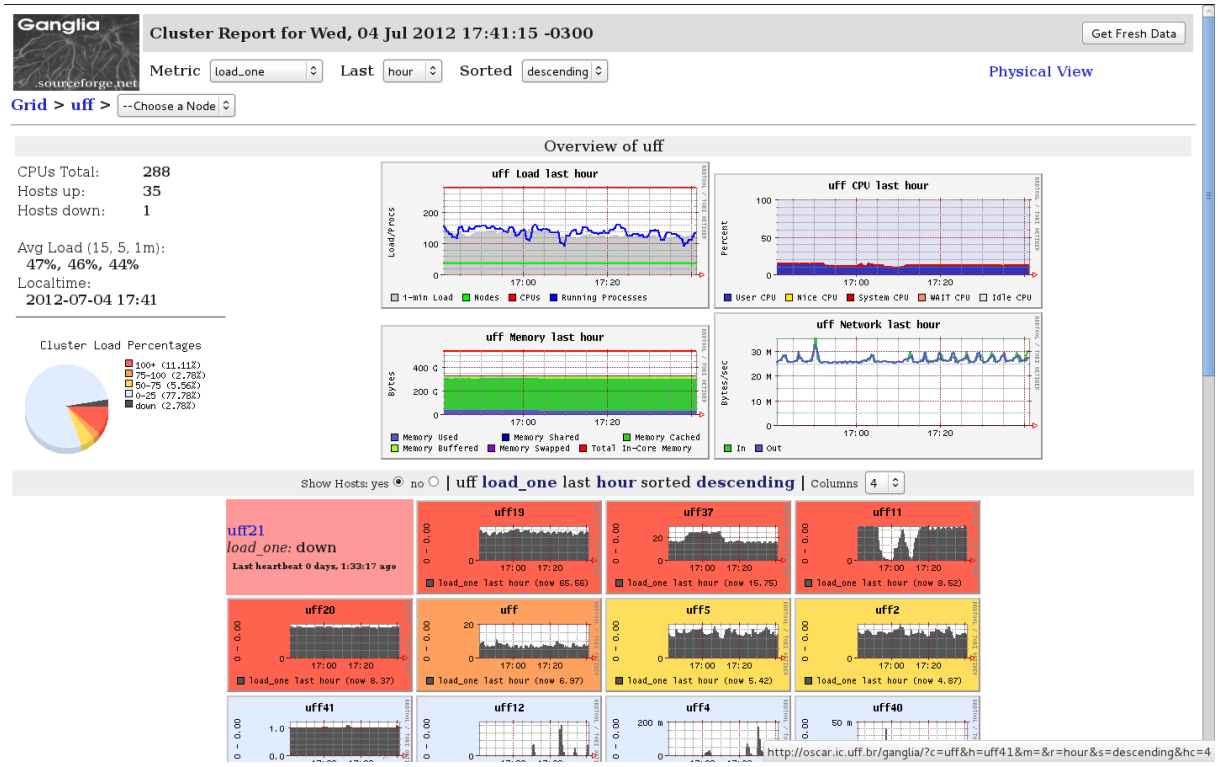

Figura 2.1: Foto da tela de monitoramento do Cluster Bull do Laboratório de Pós-Graduação em Ciência da Computação da UFF

tervalos de tempo e gerar gráficos com a informação resultante. A ferramenta é usada comumente para fazer polling de um switch ou roteador através do protocolo SNMP (Simple Network Management Protocol). A ferramenta não tem opção de configuração de alertas em caso de problema na rede como o ganglia, com um agravante, a ferramenta é dependente do protocolo SNMP, isso implica que, se na rede a se monitorar as máquinas que as compõem não poderem usar o SNMP, a ferramenta é inútil. O SNMP pode ser ruim também para servidores expostos a internet. O SNMP tem 3 versões atualmente, sendo as versões 1 e 2c as mais usadas. Somente a versão 3 (mais atual) tem preocupações com segurança, como encriptação de senhas (nas versões 1 e 2c a senha é transmitida via texto puro). O SNMP pode ser uma escolha ruim se for usado em redes de alta latência e de banda computacional baixa, pois com o tráfego usado pelo SNMP é possível que se use porções significativas da banda desta rede. Vemos uma tela da ferramenta instalada, mas não usada pelo grupo de monitoramento do laboratório SGCLab na figura 2.2.

2.2.3 GroundWork Monitor

GroundWork Monitor[9] é um a suíte de monitoramento que agrega várias ferramentas de monitoramento opensource em um único produto. Ela é capaz de monitorar não

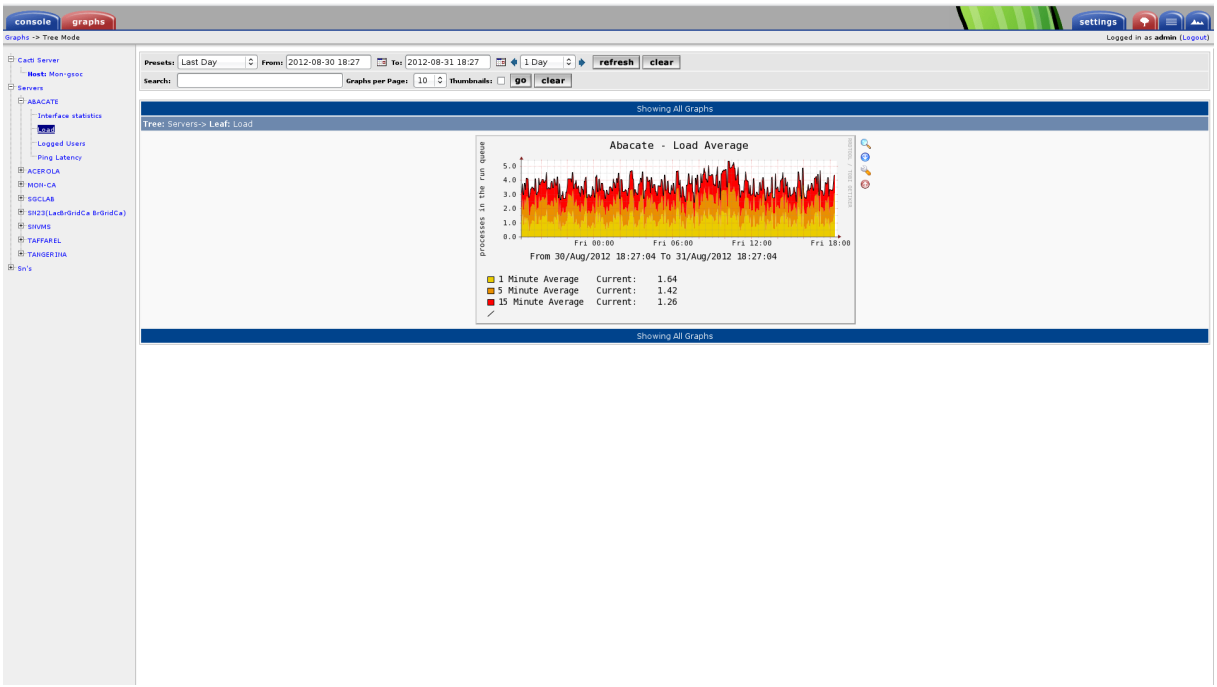

Figura 2.2: Foto da tela de monitoramento da ferramenta instalada no SGCLab

somente nós de rede, bem como a disponibilidade da aplicação e desempenho da rede. O groundwork é pago, podendo não ser uma boa opção para pequenas empresas que necessitam desse tipo de serviço. O groundwork tem uma versão gratuita, porém esta versão não recebe atualizações pela empresa e não é considerada segura por esse motivo. Vemos um exemplo de uma tela da ferramenta retirada do site da desenvolvedora na figura 2.3. Alguns componentes de código aberto que formam o GroundWork Monitor estão listados a seguir.

- NAGIOS
- Cacti
- JBoss Portal
- PostgreSQL
- Ntop
- Network Weathermap
- NeDi
- Apache HTTP Server
- RRDTool

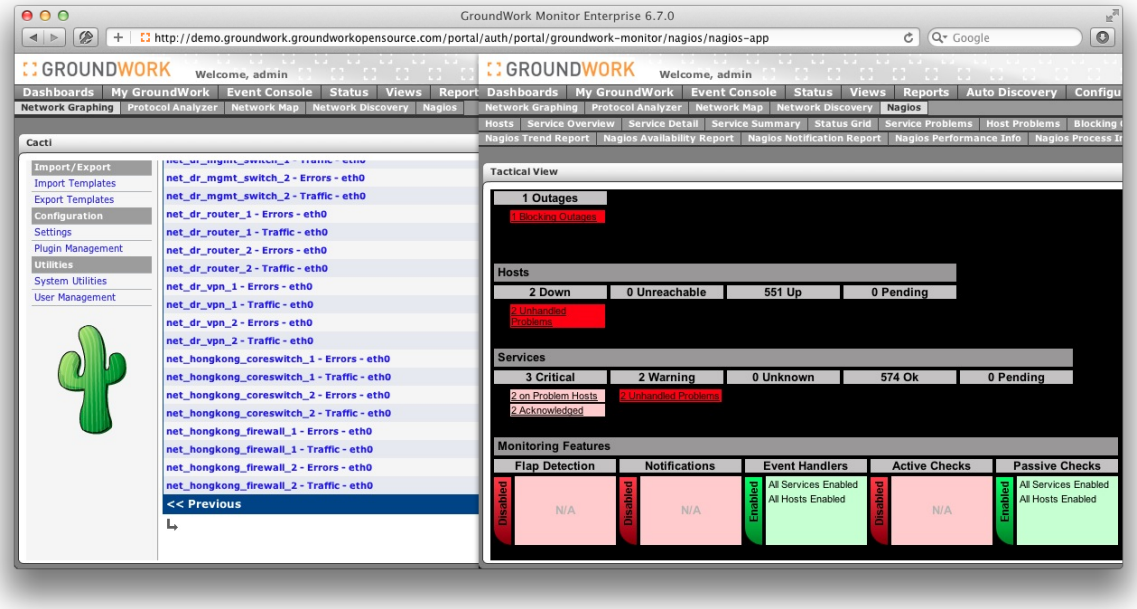

Figura 2.3: Foto retirada do site da ferramenta (http://www.gwos.com/)

2.2.4 Microsoft Network Monitor

A ferramenta[10] nada mais é que um analisador de pacotes, permitindo visualizar, analisar e decriptografar protocolos de rede. Pode ser usado para identificar problemas de rede e problemas da aplicação na rede. Atualmente a ferramenta está em sua versão 3.4 e tem com características:

1. Controle de processos;
2. Agrupamento por conversação de rede;
3. Suporte a mais de 300 protocolos públicos e proprietários da Microsoft;
4. Sessões de captura simultâneas;
5. Modo de monitoramento wireless com suporte a NICs sem fio
6. Captura de pacotes em tempo real e visualização de quadros
7. Sniffing de modo de tráfico promiscuo
8. Pode ler arquivos de captura libpcap
9. API para acessar o motor de analise e captura

Por ser uma ferramenta de análise, sua utilidade é importante somente quando, ao verificar algo errado com alguma rede, o administrador dela a usa para buscar exatamente onde o erro se encontra. Essa ferramenta também só servirá para analisar a rede, se algum problema acontecer dentro de algum nó na rede, este não será detectado. Um tela da ferramenta é mostrada na figura 2.4.

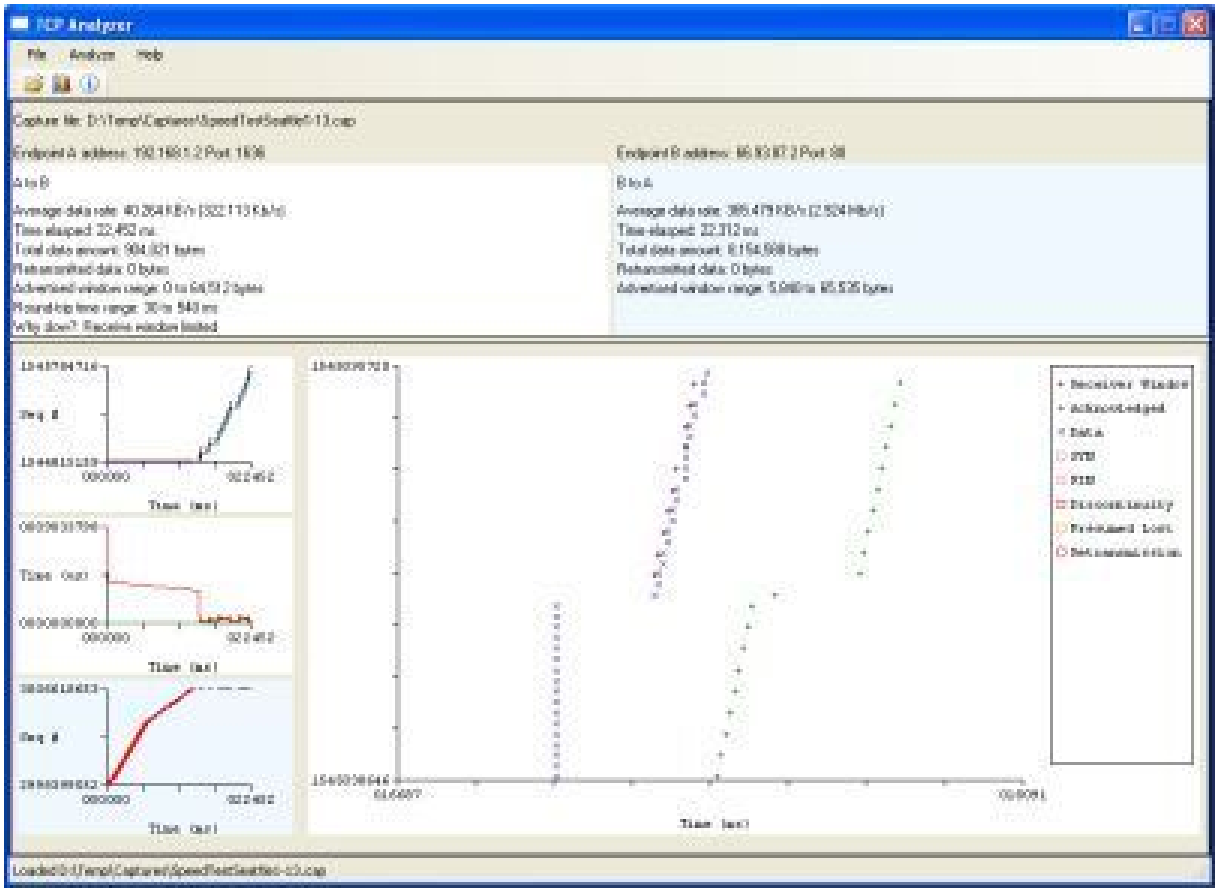

Figura 2.4: Imagem retirada do site http://research.microsoft.com/en-us/projects/tcpanalyzer/

2.2.5 WhatsUP Gold

Ferramenta proprietária, WhatsUP Gold[11] é uma ferramenta de monitoramento que existe desde 1991. Com ela é possível monitorar equipamentos e serviços, receber notificações, mapear a rede e gerar relatórios. Essa ferramenta tem interface grosseira, não intuitiva e sua instalação depende de console web e Windows, além de ser uma ferramenta paga. Devemos salientar também, que essa ferramenta utiliza o protocolo SNMP para obter seus dados, podendo ter problemas com redes de latência alta. Um tela da ferramenta é mostrada na figura 2.5.

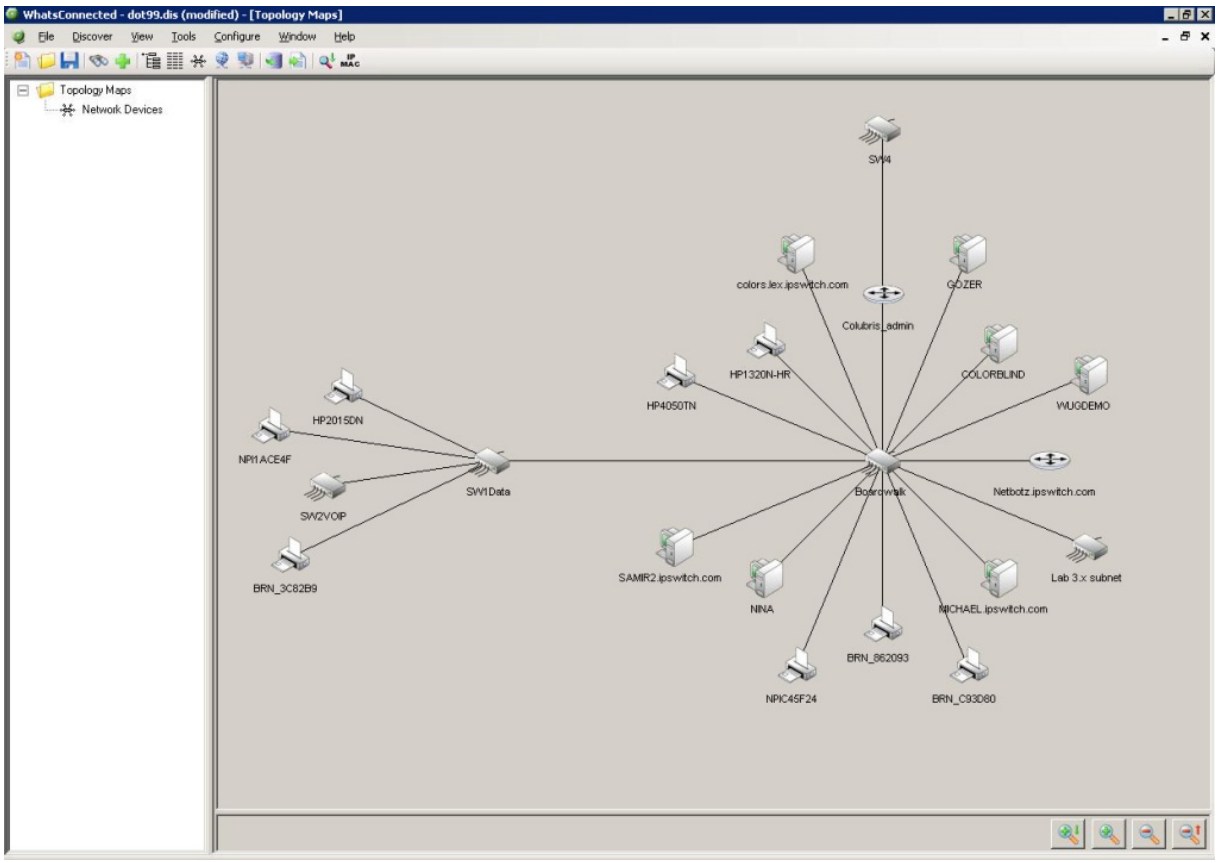

Figura 2.5: Imagem retirada do site http://www.whatsupgold.com/

2.3 Resumo

A integridade de uma rede de dados é de suma importância nos dias de hoje. Uma rede onde não se tem ciência do que acontece nela pode ser catastrófica e uma receita de desastre. Sistemas de monitoramento são essenciais para permitir um bom funcionamento da rede, porém cada rede tem sua característica única. Cabe ao administrador de rede analisar as demandas de sua rede e utilizar a ferramenta que atenda a estas demandas. Discutimos algumas ferramentas usadas hoje em dia e falamos um pouco de suas atribuições. No próximo capítulo, falaremos sobre a ferramenta escolhida para a monitoração, o NAGIOS.

Capítulo 3

NAGIOS

Neste capítulo o objetivo é apresentar a ferramenta de monitoramento NAGIOS. Será dado um breve histórico da ferramenta, além de uma explicação sobre seu funcionamento. Diremos também os motivos da escolha dela para o trabalho.

3.1 Histórico

NAGIOS[12] começou no ano de 1999, com o nome de NetSaint[13], devido a problemas de marca com esse nome, o criador do nagios, Ethan Galstad, decide trocar o nome para NAGIOS, anacronismo recursivo de "Nagios Ain't Gonna Insist On Sainthood" (Nagios não vai insistir em santidade, em inglês).

NAGIOS[14] começou com um pequeno projeto para atacar um nicho de mercado: o monitoramento de redes. Na época do nascimento do NAGIOS, ferramentas de monitoramento comerciais eram caras. Pequenas empresas precisavam de um sistema bom e eficiente, tendo uma grande característica, poder se implementado a baixo custo por uma empresa.

NAGIOS em 2002 competia com varias ferramentas pagas, tal como: What's up Gold. NAGIOS atualmente está na versão 3.x e foi rebatizado de novo, agora NAGIOS é NAGIOS core[14], tendo seus arquivos de instalação baixados da página onde é hospedado, a SourceForge.net, mais de 600,000 vezes. Neste trabalho, NAGIOS core será referenciado apenas por NAGIOS, seu nome inicial.

Figura 3.1: Foto do sítio da ferramenta (nagios.org)

3.2 Funcionamento

NAGIOS tem como objetivo chave informar ao administrador da rede sobre condições questionáveis ou críticas, sendo essas condições configuráveis pelo próprio administrador da rede. A ferramenta disponibiliza também uma página web, onde o administrador e outros usuários podem ver um sumário da situação dos nós da rede monitorados. Nesse sumário, a situações são representadas em: verde, para situação normal, amarelo, para situação questionável, e finalmente, vermelha, para situação crítica.

NAGIOS[14] se diferencia das outras ferramentas de monitoramento, pois foca no monitoramento de estados, usando o modelo de semáforo de estados, tendo como objetivo informar rapidamente sobre os estados "questionáveis" dos servidores da rede com problemas. Outras ferramentas têm como estratégia somente exibir em tempo real os estados da rede e de seus servidores de forma gráfica (na forma de gráficos) e há aquelas que têm como estratégia medir somente o tráfego de rede, esses tipos de ferramentas são muito usadas para análise, visto que só serão acionadas quando um problema for constatado. A ferramenta NAGIOS simplesmente avisa o administrador de rede se um de seus serviços ou nós de redes mudou do estado ok (verde), que mostra que está tudo bem para um dos outros estados (amarelo ou vermelho) que mostra que algo está errado. Nesse quesito, ela cumpre bem o que promete.

O núcleo[15] do NAGIOS em si, não executa nenhum teste, tendo ele uma estrutura modular, para isso ele usa plugins. Esses plugins são scripts externos, que executam os testes nos nós e serviços da rede. O NAGIOS oferece um pacote de plugins básicos, que testam os serviços mais conhecidos, o NAGIOS plugins. Os plugins do NAGIOS podem ser em qualquer linguagem, e além dos três estados já falados anteriormente (ok, warning e critical), temos mais um que pode ser representado por esses plug-ins, o estado unknown. Com isso, qualquer coisa que seja mensurável é passível de monitoração por parte do NAGIOS, deixando a ferramenta praticamente sem limites no quesito monitoramento. Se for possível coletar dados sobre o que se quer medir, é possível monitorar.

O NAGIOS possui na notificação um de seus pontos fortes. Pode-se configurar qual pessoa ou grupos de pessoas (contact groups, grupos de contato em inglês) devem receber avisos de problemas, além de poder especificar para qual grupo deve ser mandado o aviso do problema.

NAGIOS não exibe gráficos dos servidores e serviços que monitora, bem como não tem uma otimização para monitoramento de clusters, para isso a ferramenta permite integração com outras que façam isso. Ao se integrar com a ferramenta cacti, por exemplo, NAGIOS pode ter seus dados exibidos em gráficos, ajudando o administrador a analisar o comportamento de um servidor com problema, bem como unificar em uma ferramenta o monitoramento da rede. No trabalho devido ao tempo, não foi possivel fazer essa integração.

A notificação do NAGIOS pode ser feita a partir de programas externos também, permitindo notificações de status de serviços e nós de qualquer modo, podendo ser via email, SMS, pager. A interface web[14] exibe informações detalhadas de todos os nós e serviços da rede que estão monitorados por ela. Na interface podemos verificar o histórico de tudo que é monitorado, a ferramenta permite que o usuário possa ativar e desativar algumas configurações do monitoramento de serviços e dos nós da rede.

O NAGIOS suporta monitoramento redundante, bem como monitoramento distribuído, com vários servidores NAGIOS descentralizados, mandando dados a um servidor central. A ferramenta possibilita a monitoração de cluster de serviços e de máquinas.

A ferramenta tem dois tipos de monitoração, a ativa e a passiva. Na ativa, o servidor NAGIOS toma a iniciativa e busca os dados no nó da rede de tempos em tempos, sendo isso configurável pelo administrador do servidor NAGIOS. Já na passiva o resultado da checagem é feita adquirida por uma aplicação ou processo externo, que submetem ao NAGIOS esse resultado para ser processado. A monitoração passiva é bastante útil quando

se deseja monitorar serviços assíncronos que não teriam monitoração eficaz se seu estado fosse analisado com frequência regular ou quando um servidor está atrás de um firewall que não permite que o servidor NAGIOS faça a checagem dos serviços diretamente[16].

Porque escolher o NAGIOS? Enumeramos alguns motivos:

1. **Altamente customizável.** NAGIOS pode ser adaptado a praticamente qualquer topologia de rede e monitorar qualquer coisa que se possa medir.
2. **Código aberto.** Por ser uma ferramenta de código aberto, está em constante atualização, através de uma comunidade ativa.
3. **Integra-se com a maioria das ferramentas de monitoramento existentes atualmente.** NAGIOS, como discutido anteriormente, pode se integrar com ganglia, cacti, splunk e muitas outras mais.
4. **Diferentes modos de monitoramento.** Monitoramentos passivo e ativo. Na figura 3.2 [15] mostraremos os modos de monitoramento do NAGIOS.

3.2.1 Modos de Monitoramento do NAGIOS

Como dito anteriormente, para monitorar, NAGIOS utiliza scripts chamados plugins. Nos casos mais simples, podemos testar serviços de internet, para isso basta chamar um plugin localmente no servidor nagios. Alguns testes podem ser feitos facilmente pela rede. Não existe protocolo de rede que cheque o espaço livre em disco, por exemplo. O administrador de rede terá que executar o plugin na máquina cliente via shell remoto ou outros métodos, tais como SNMP para fazer a verificação de espaço, por exemplo. O fato é que existem várias formas de se monitorar com o NAGIOS e a figura 3.2 ilustra alguns dos métodos usados para tal.

Para monitorar serviços de internet no primeiro cliente, como explicado antes, o servidor NAGIOS "roda" o plugin localmente, no exemplo da figura 3.2 "check_xyz". A partir do cliente 2 até o 5, são clientes que rodam o plugin localmente para obter os dados para o servidor NAGIOS.

No cliente 2, é utilizado monitoramento via Secure Shell, SSH. O NAGIOS executará check_by_ssh, um plugin no servidor NAGIOS que receberá um argumento para rodar o plugin desejado na maquina cliente. Esse monitoramento necessitará que o check_by_ssh possa "logar" na máquina cliente sem senha. No cliente 4, é utilizado um plugin que busca a informação do plugin instalado na máquina através do protocolo SNMP.

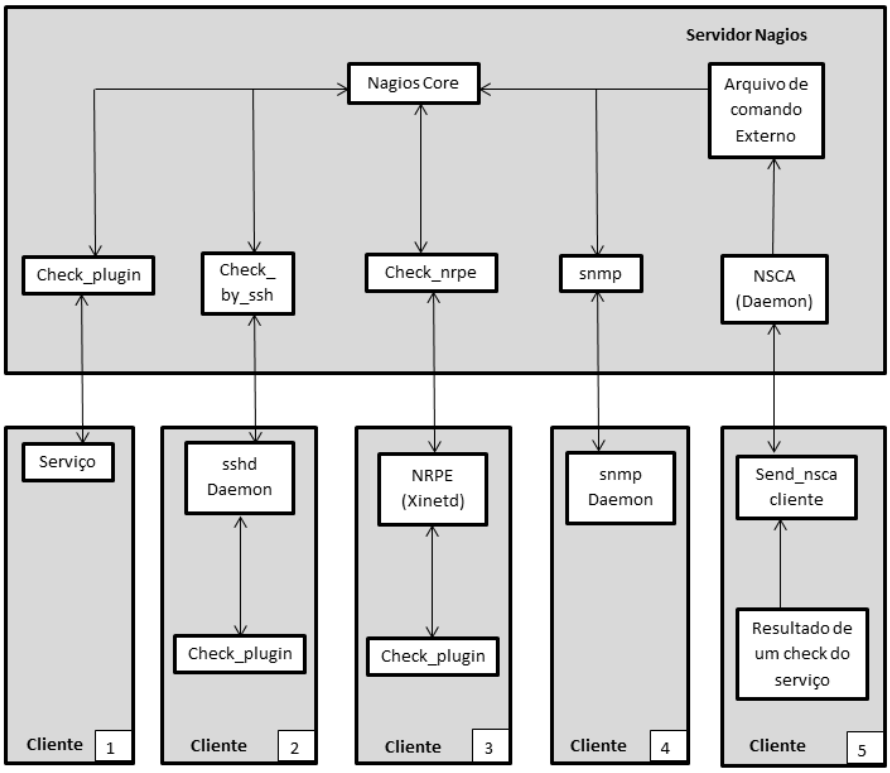

Figura 3.2: Desenho dos modos de monitoramento descritos no livro

No cliente 3, utilizamos o plugin NRPE, que é instalado no cliente e iniciado via daemon inet (que deve estar configurado de acordo). Se o NRPE receber uma consulta do servidor NAGIOS via porta TCP 5666 (selecionável), ele executará a consulta correspondente e obterá o resultado. Esse monitoramento foi escolhido para a implementação do projeto. Explicaremos como ele será utilizado no capítulo 4.

No cliente 5, o NAGIOS Service Check Acceptor, NSCA, roda como um daemon no servidor NAGIOS esperando por resultado de testes enviado pelos clientes. Esse método e tido como passivo, pois o NAGIOS não toma a iniciativa para buscar os resultados.

3.3 Resumo

NAGIOS é uma ferramenta robusta de monitoramento. Usada para monitoramento de elementos de rede, hoje em dia é usada nas mais variadas atividades que requerem algum tipo de controle, além de ser usada como base de várias aplicações de monitoramento, tais como o groundwork, Opsview, Icinga. Graças a sua arquitetura adaptativa e modular,

que permite o seu usuário moldar a ferramenta de acordo com sua necessidade, ela se torna uma das ferramentas de monitoramento mais usadas da atualidade.

Capítulo 4

Estudo de Caso

Com base para este trabalho, neste capítulo serão mostradas algumas topologias de monitoramento utilizando a ferramenta NAGIOS que podem ser aplicadas na rede do Instituto de Computação (IC), baseados nas necessidades de seus administradores e de acordo com a topologia das redes do IC. Com isso mostraremos a topologia de monitoramento escolhida e explicaremos a partir dai como foi feita a implementação da ferramenta.

4.1 Topologias NAGIOS

4.1.1 Estrela

Topologia básica onde existe somente um servidor NAGIOS que monitora todos os itens de uma rede de computadores. Ideal para redes com um pequeno número de computadores e redes. Não muito bom para redes com muitas sub redes ou quando se necessita monitorar computadores de redes distantes fisicamente, pois pode onerar muito o tráfego de rede, além de sobrecarregar a máquina com o servidor NAGIOS. Nas figuras 4.1 e 4.2 temos exemplos dessa topologia.

4.1.2 Distribuída

Esta topologia é composta de vários servidores NAGIOS onde cada um toma conta de uma pequena parte de uma rede ou no caso de redes separadas geograficamente entre si, cada servidor tomará conta de cada rede. Esses servidores enviam os dados do monitoramento para um servidor NAGIOS principal, que agrega todas as informações dos outros

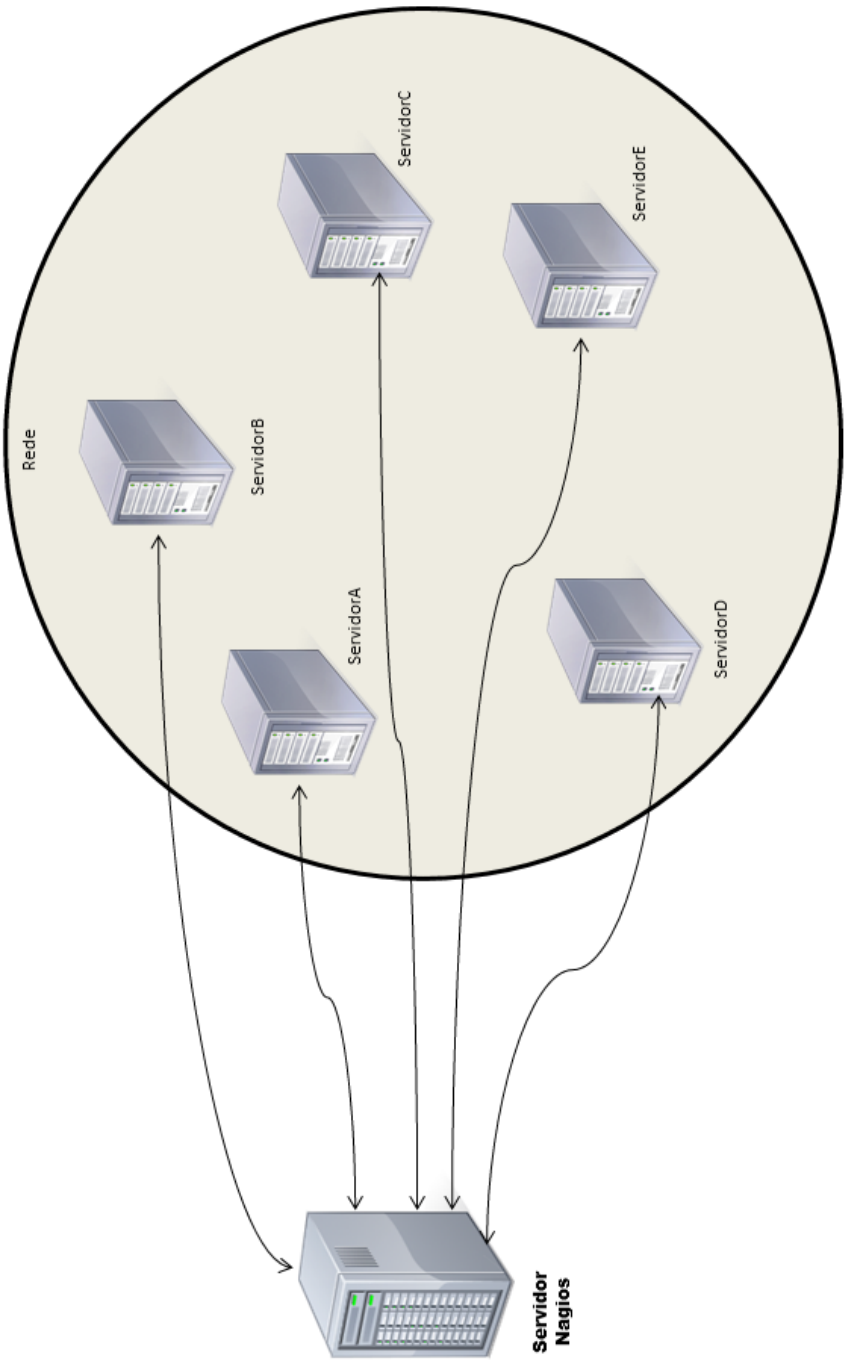

Figura 4.1: Modelo de topologia estrela simples.

servidores. Como dito anteriormente, esse tipo de topologia é ideal quando se faz necessária para monitoramento de redes compostas de redes que são separadas fisicamente, podemos usar essa topologia também para redes que tem firewalls controlando o acesso aos servidores que as constituem. Podemos configurar um servidor NAGIOS dentro dessa rede monitorando os servidores de dentro dessa rede e configurar o firewall para ele permi-

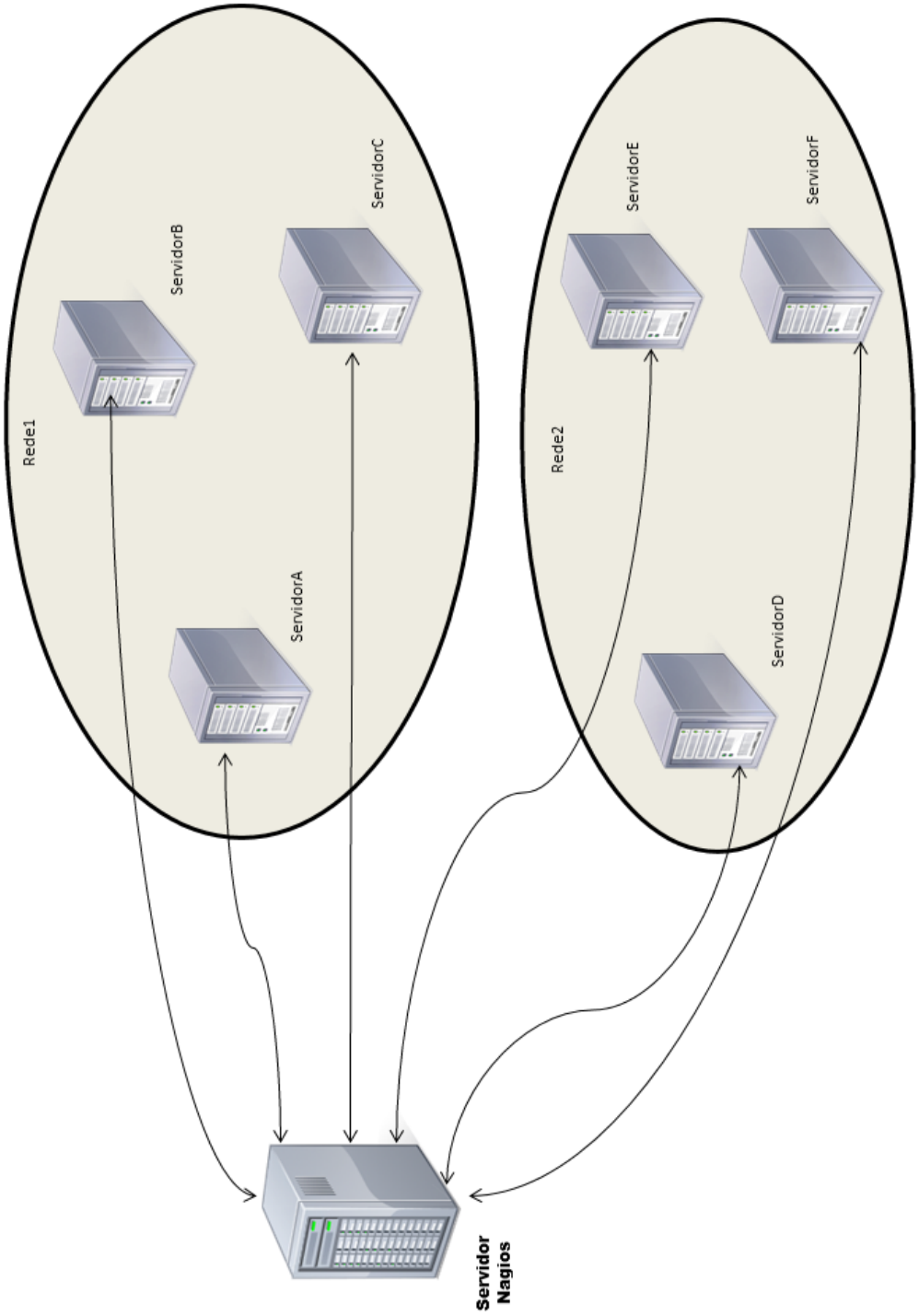

Figura 4.2: Modelo de topologia estrela monitorando 2 redes.

tir o acesso do servidor NAGIOS principal somente ao servidor NAGIOS de dentro dessa rede. Neste tipo de configuração, podemos ter apenas um executor de testes de serviços e status das máquinas no papel de um servidor NAGIOS completo (NRPE [17]), como demonstrado na figura 4.3.

Esse tipo de topologia ajuda o monitoramento quando o volume de dados é grande,

pois divide o trabalho de processamento da informação. Uma desvantagem dessa topologia é que caso um desses servidores nagios secundários ter problema, todos os dados dos servidores por ele monitorado poderão ser perdidos, um modo de contornar esse problema seria criar um monitoramento failover, onde outro servidor NAGIOS pode assumir a monitoração em caso de problema. Temos também um outro modo de monitoramento, por redundância, onde podemos ter mais de um servidor NAGIOS monitorando o mesmo servidor. Podemos ter a situação em que exista uma rede onde o firewall bloqueia acessos de fora desta. Podemos usar um servidor NAGIOS dentro dessa rede que envie os dados e o servidor "mestre" recebe os dados da rede de forma passiva (discutidas no capitulo 3) como exemplificado na figura 4.4. Nas figuras 4.5, 4.6, 4.7 temos alguns exemplos dessa topologia.

4.2 Análise da rede do IC

No desenho mostrado na figura 4.8, temos esquematizado alguns servidores e sub-redes que compõe a rede de computadores do IC. Temos a rede dos computadores das secretarias e os das dos professores que são separadas das outras por um firewall (Mangostin), temos também a rede de computadores que compreendem os computadores do laboratório do curso de graduação de ciência da computação (LCC), protegidos por um firewall (Lcc-fw). Temos outro firewall que protege do tráfego da rede wi-fi que o Instituto disponibiliza aos seus estudantes, funcionários e professores. Temos dentro da rede um cluster de computadores de alto desempenho da empresa BULL (CLUSTER OSCAR) e por fim, os servidores que serão uns dos objetos de nosso estudo de caso, servidores que são responsáveis pelo funcionamento dos serviços que são oferecidos pelo IC. Como inicio de implementação da monitoração, devido ao número pequeno de servidores e serviços planejados a ser monitorados inicialmente e que serão discutidos a frente, mesmo com os firewalls que compõem a rede, foi optado pela topologia de monitoração em estrela. Usamos elementos da topologia distribuída e também usando o servidor mon-gsoc para monitoração de forma distribuída, para monitoração da autoridade certificadora UFF Br-GridCA. Usamos redundância também para monitorar as estações de trabalho maquinas frutas. Nesses firewalls foram adicionadas exceções e aberto portas para que o servidor NAGIOS pudesse monitorar.

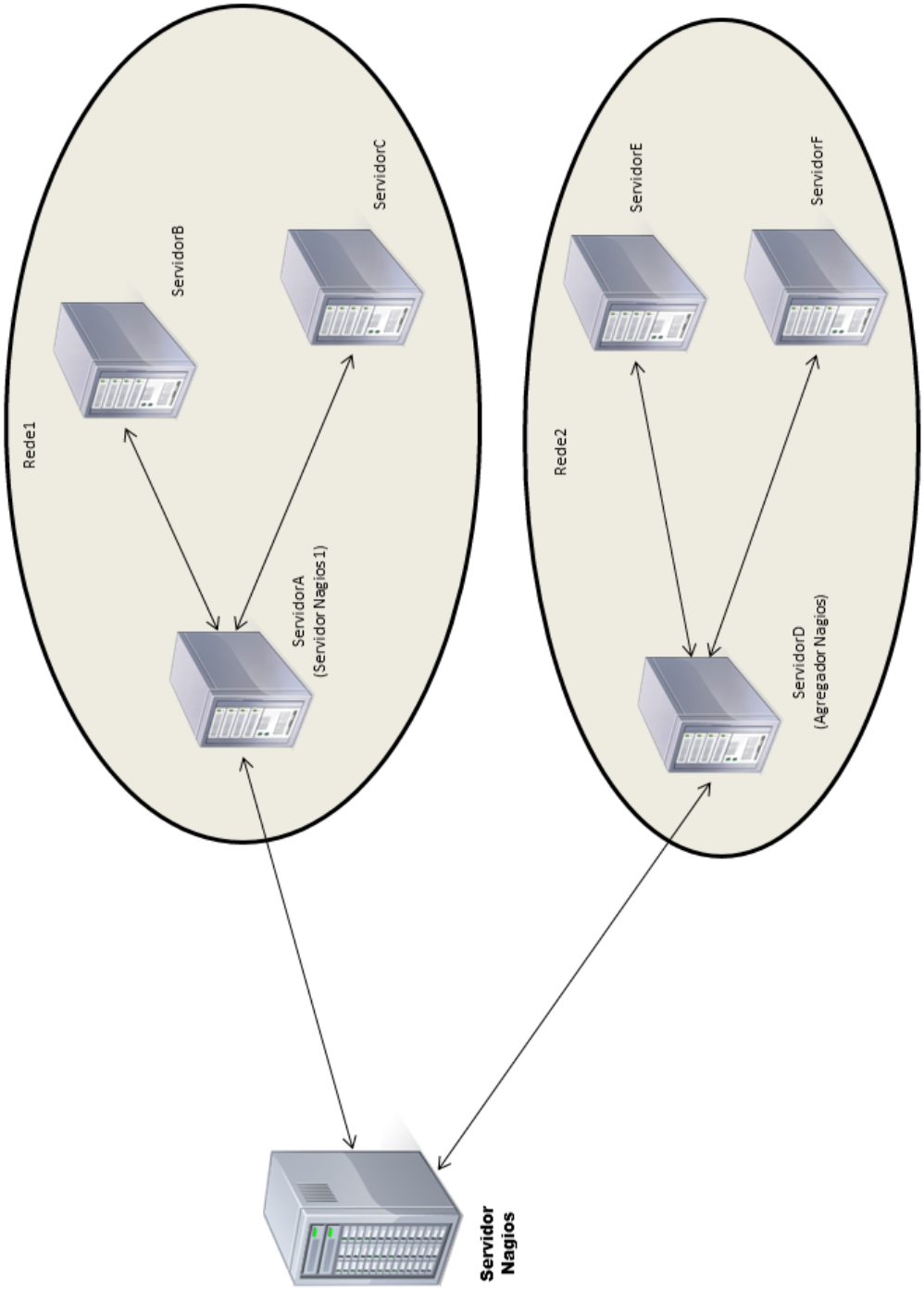

Figura 4.3: Modelo de topologia distribuida(árvore).

4.3 Definindo a Monitoração

Analisado as sub-redes que compõe a rede do IC, foi discutido com os administradores da rede quais servidores e serviços seriam importantes nesse primeiro momento para monitoração, os servidores mais importantes que foram listados por eles foram os seguintes

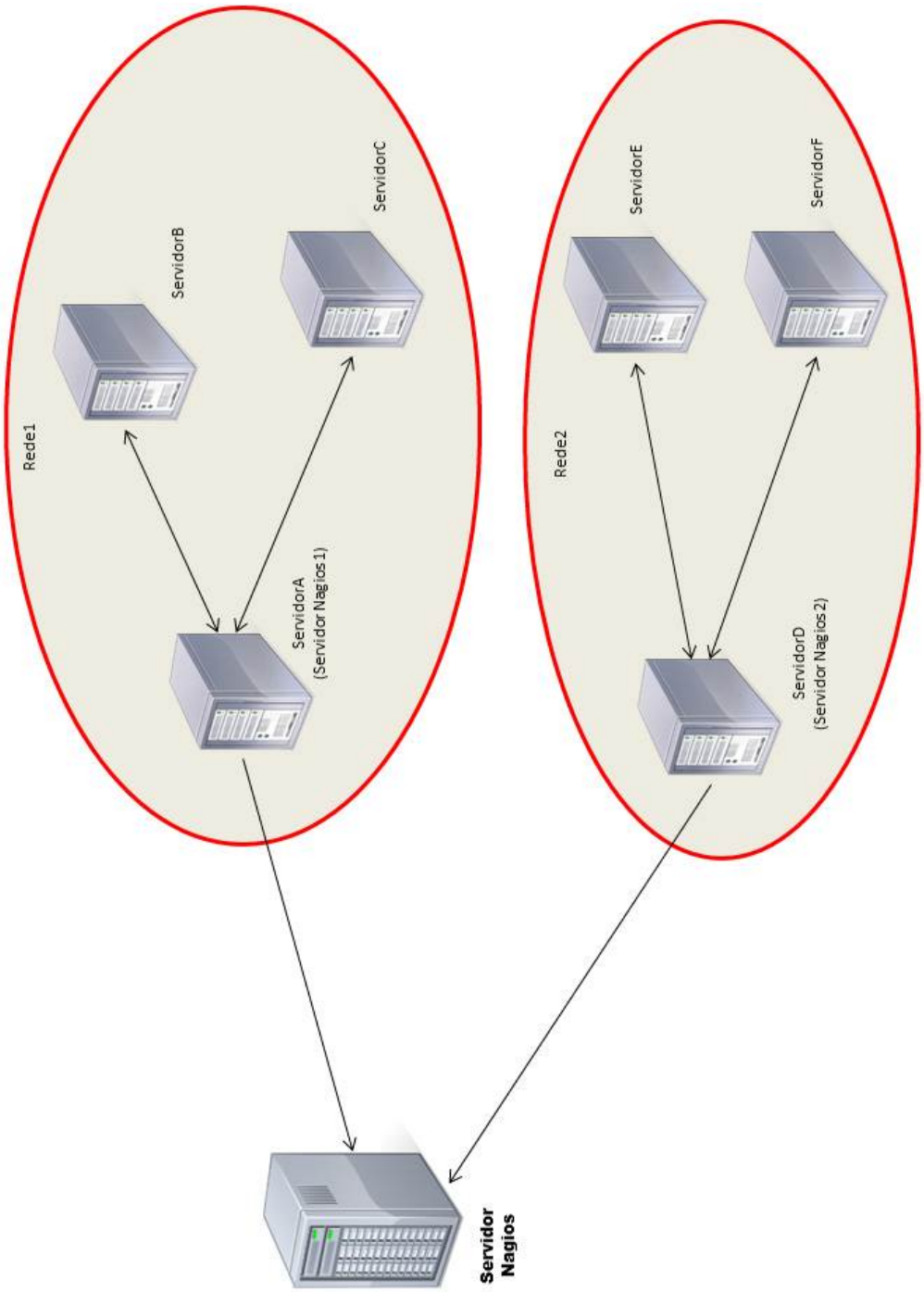

Figura 4.4: Modelo com duas redes separadas geograficamente com firewalls bloqueando.

- abacate (NIS, DNS, portal de entrada por SSH),
- acai (Servidor de máquinas vírtuais VMware(guarana, abacate)),
- dida-fw (Firewall),
- dmzhost1 (Servidor de máquinas vírtuais VMware(tangerina, mxsec)),

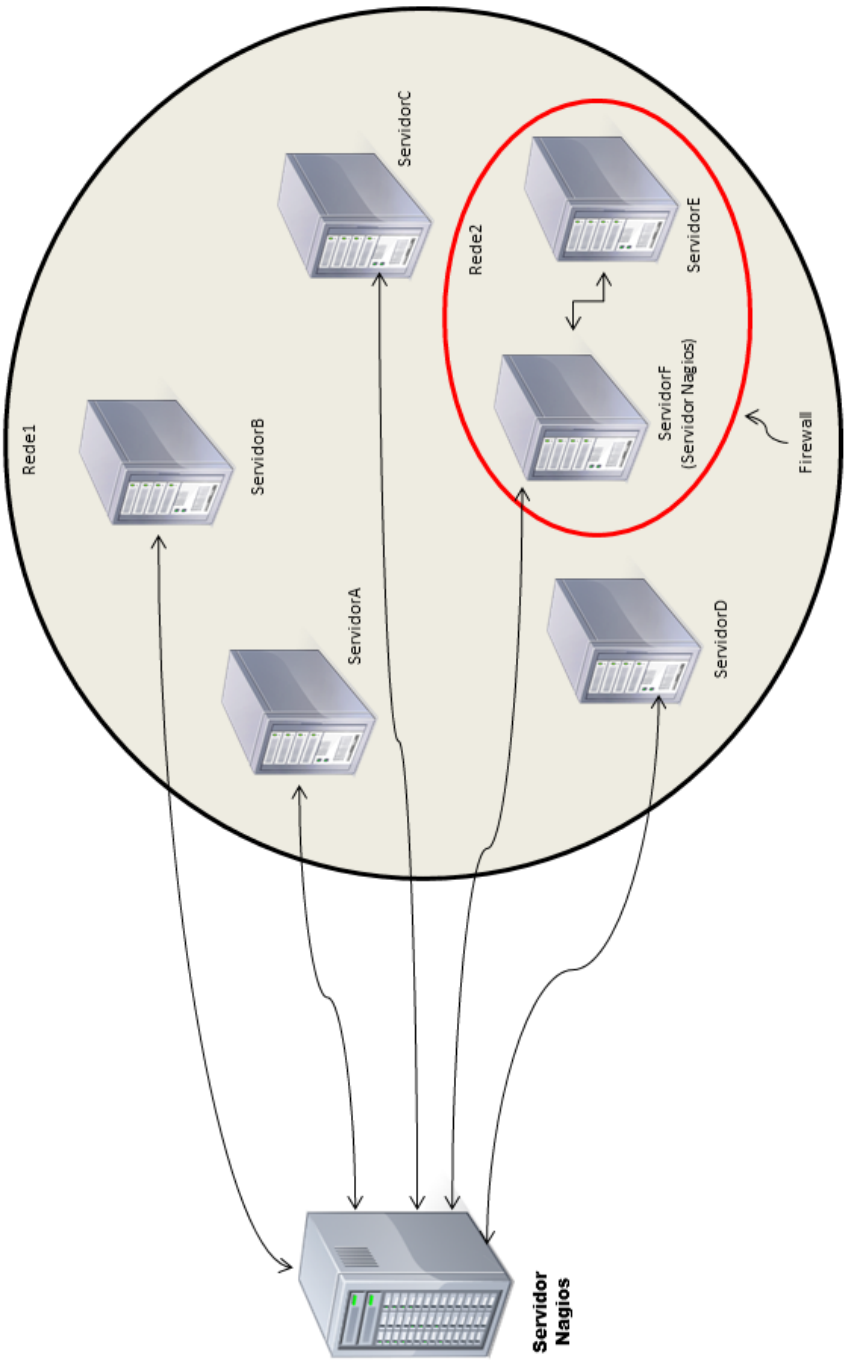

Figura 4.5: Modelo com uma rede que contém uma sub-rede que tem um servidor nagios monitorando esta sub-rede.

- dmzhost2 (Servidor de máquinas vírtuais VMware(mangamx)),
- drácula (Servidor de backups de serviços e configurações dos servidores do IC),
- fruteira (Servidor NFS),

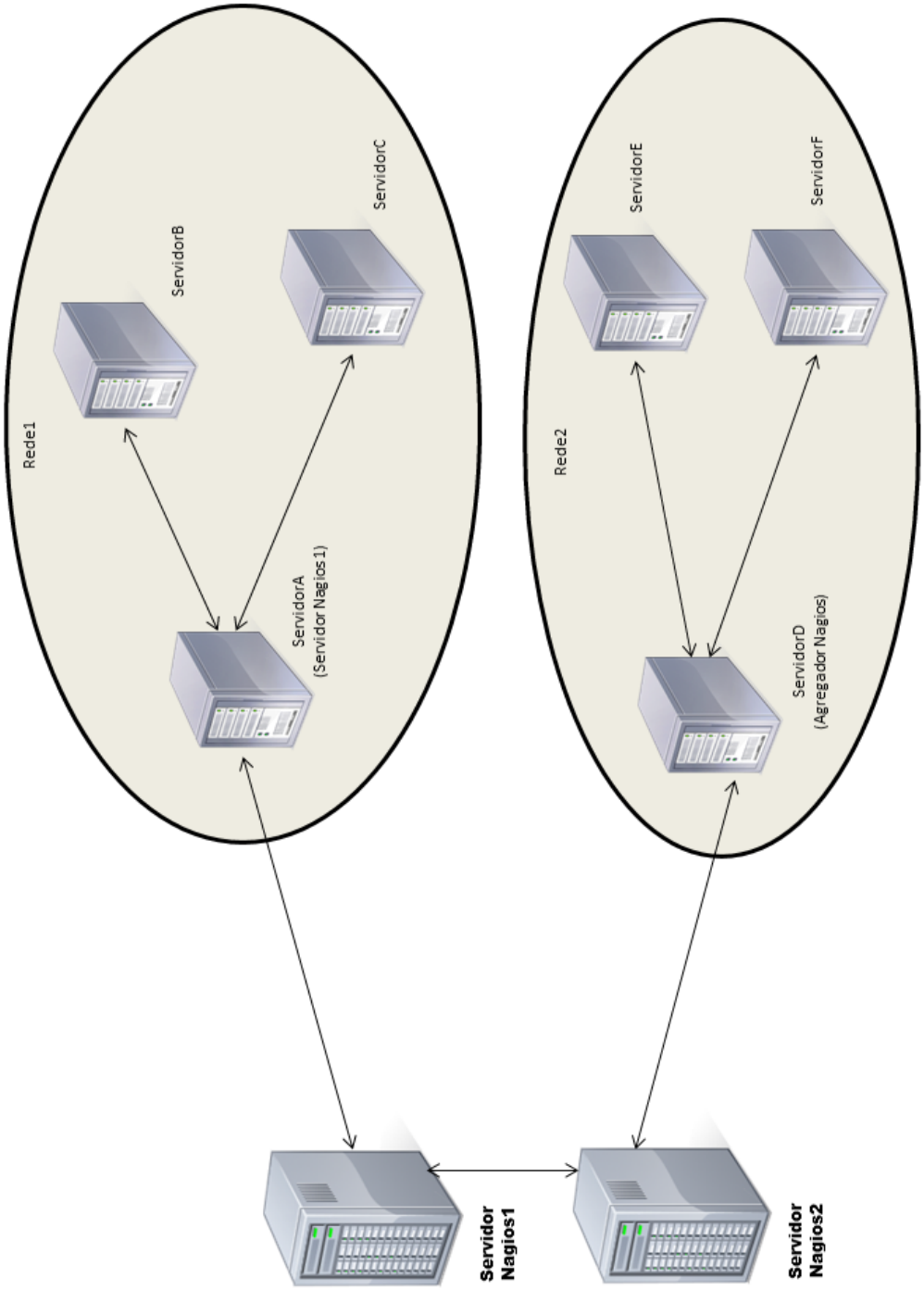

Figura 4.6: Modelo com monitoramento failover, onde um servidor NAGIOS assume as máquinas do outro em caso de falha.

- gsstore (Servidor centralizador de contas dos usuários do laboratório SGCLab),
- guaraná (Servidor SAMBA),
- lcc-fw (Firewall),

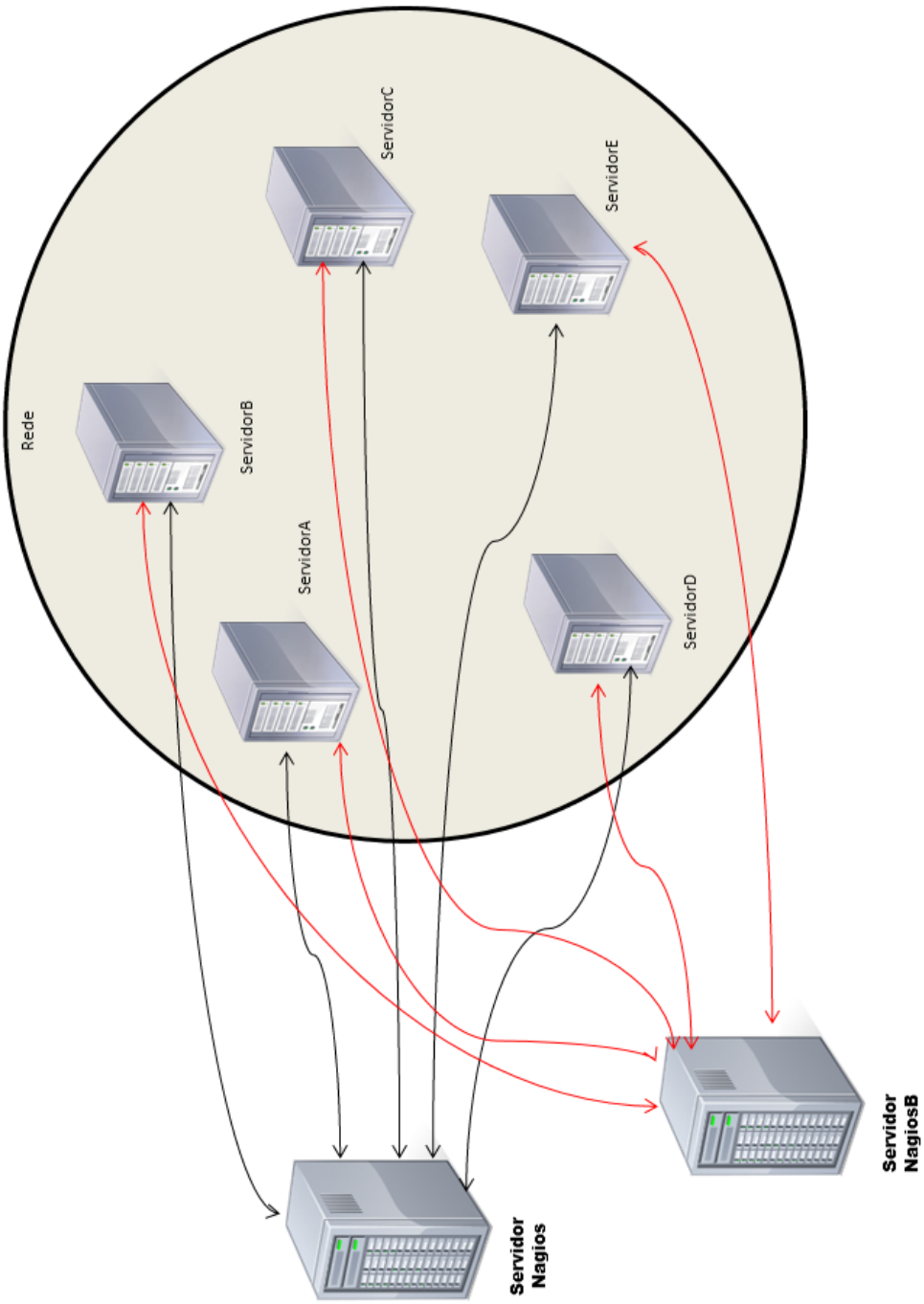

Figura 4.7: Modelo com monitoramento redundante, dois servidores NAGIOS monitoram uma única rede.

- mangamx (Servidor de e-mails),
- mangostin (Firewall),
- mxsec (Servidor de e-mails secundário),

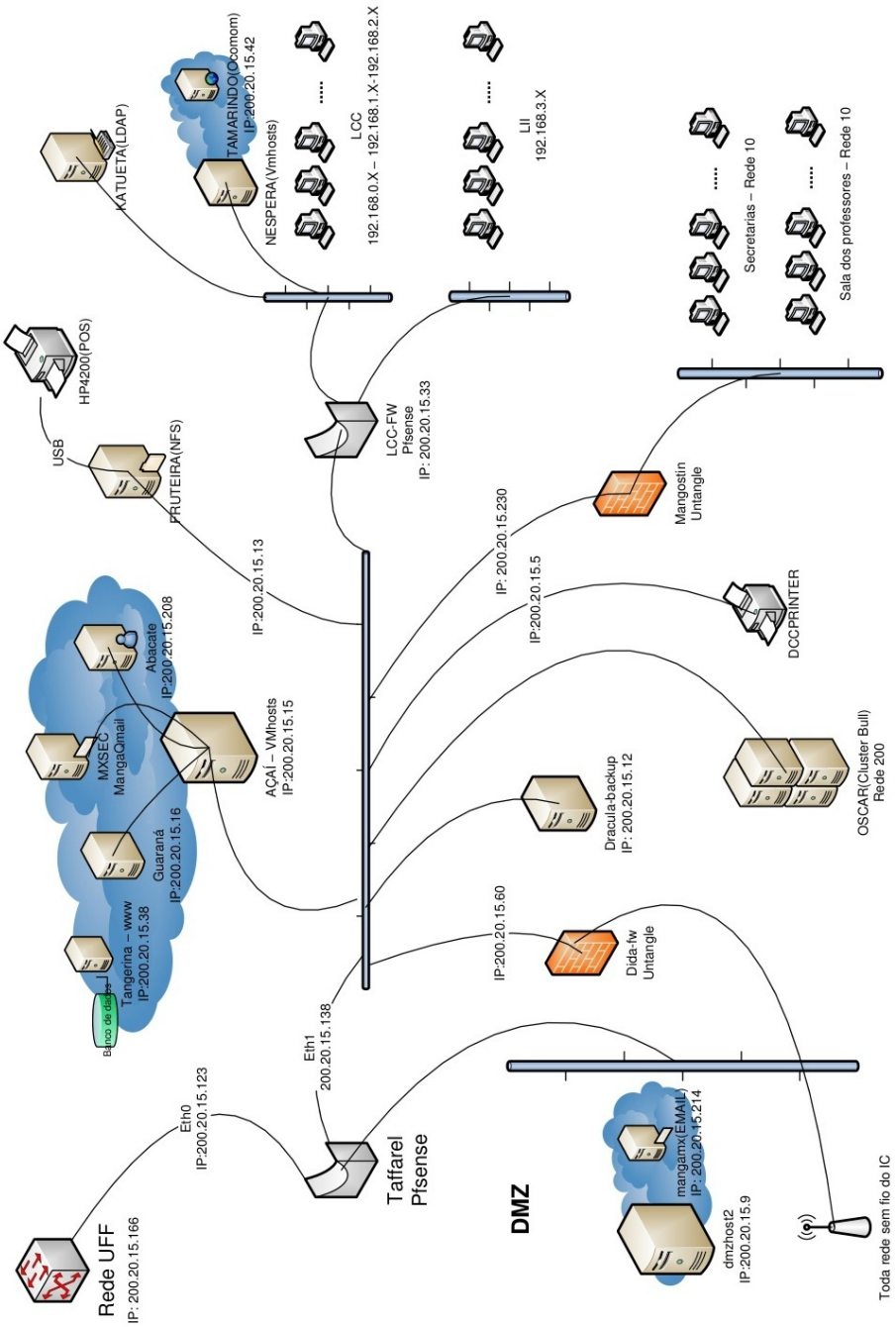

Figura 4.8: Topologia de rede do IC.

- Taffarel (Firewall),
- Tangerina (Servidor Web).

Esses servidores e firewalls são a espinha dorsal da rede do Instituto e sem eles funcionando corretamente, a rede pode sair do ar, os e-mails não serão enviados ou recebidos,

bem como backups não seriam feitos. Os administradores da rede também gostariam de verificar a conectividade da rede em relação à rede da UFF e ao mundo exterior, para isso, foi sugerido o monitoramento do link de rede do Instituto com a rede da UFF e o monitoramento do google, ambos feitos via ping, deste modo será possível, caso aconteça uma interrupção no tráfego entre a rede do IC e o resto da internet, identificar em qual link foi interrompido, se no link que o IC tem com a UFF (monitorando o site da UFF), ou se foi no link que a UFF tem para se comunicar com o rest da internet(monitorando o site da GOOGLE). Na imagem da rede não existe, mas nesse trabalho monitoraremos também os servidores SNs que pertencem a sub-rede do laboratório SGCLab. Estes servidores já estão preparados para monitoramento, pois já são monitorados por um servidor NAGIOS configurado anteriormente, que atualmente está sendo usado internamente pelo laboratório SGCLab (servidor mon-gsoc). Monitoraremos as varias máquinas com nomes de frutas, que servem de estações de trabalho para os alunos de pós-graduação do IC e também já estão preparadas para monitoramento. São servidores SNs os seguintes: sn00, sn01 a sn22 e sn24 a sn31. As máquinas frutas são: banana, caju, graviola, laranja, maracuja, oiti, pinha, postel, siriguela, cacau, goiaba, jenipapo, limao, melancia, pequi, pitanga, sapoti, umbu. Na figura 4.9, o desenho apresenta a topologia de rede do SGCLab.

Além dessas máquinas, monitoraremos os servidores mon-ca (servidor NAGIOS que monitora autoridades certificadoras da federação IGTF), mon-gsoc (servidor NAGIOS antigo que monitora máquinas da rede do SGCLab e que servirá exemplos de grupo de máquinas para monitoração do novo servidor NAGIOS, a ser explicado mais a frente), SGCLab, sgcweb, sinergia, snvms (servidores importantes para o funcionamento dos serviços da rede SGCLab), sn23 (máquina que hospeda a autoridade certificadora, sob a responsabilidade do professor Vinod Rebello).

4.4 Implementação da Monitoração

A ferramenta escolhida para a implantação do monitoramento, a ferramenta NAGIOS, foi instalada na máquina virtual sgcmon, onde foram instalados também os plugins básicos que a ferramenta precisará para funcionar. Com a ferramenta funcionando, começamos a configurar o servidor para monitorar a rede. Para facilitar a monitoração, separamos os componentes da rede do IC em grupos de máquinas, de acordo com suas similaridades[18] [19] [20] [21].

Para o início da monitoração, iremos como dito anteriormente nos focar nos servidores

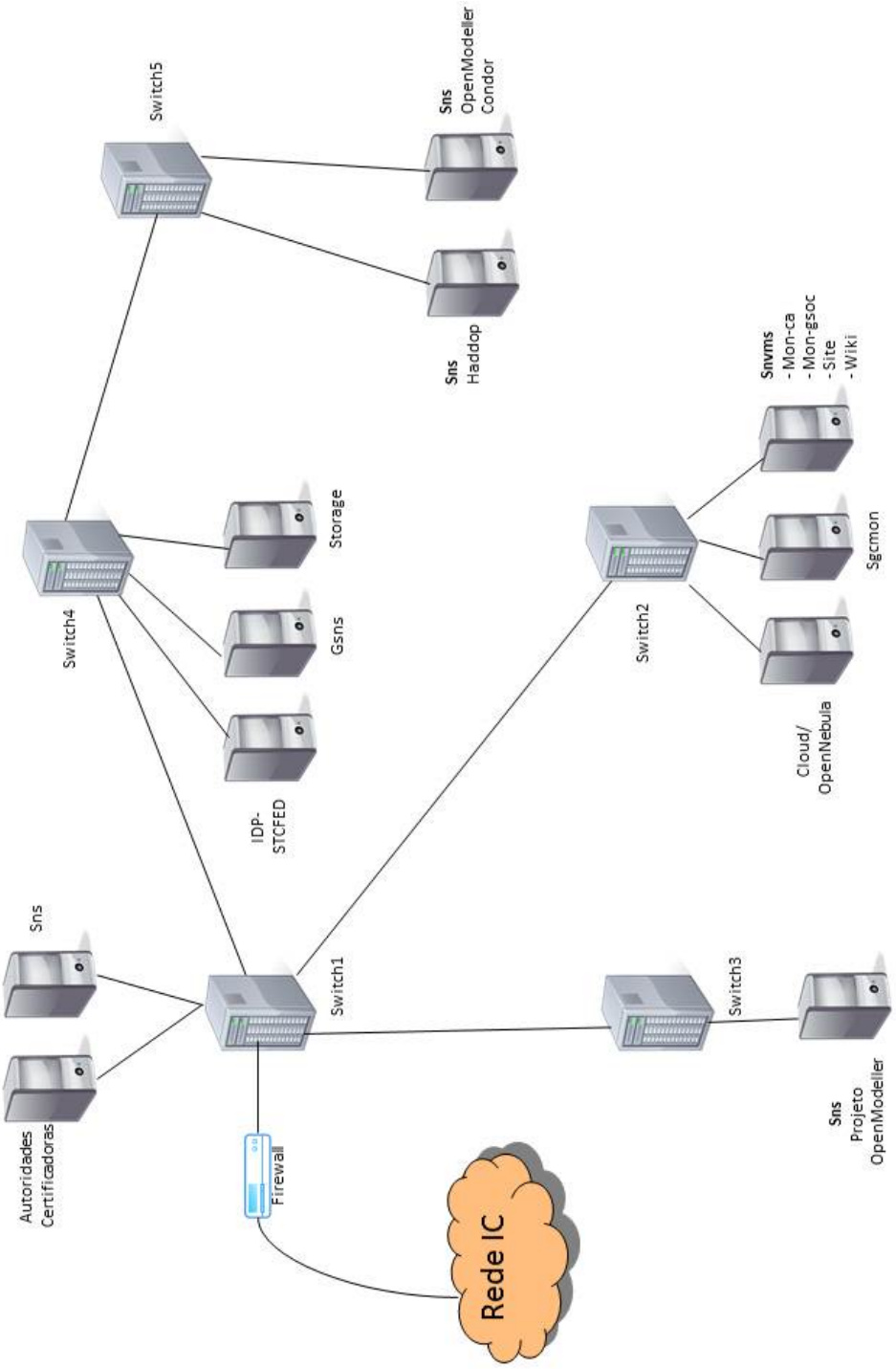

Figura 4.9: Rede do laboratório SGCLab.

citados anteriormente, os servidores mais importantes citados pelo grupo de suporte do IC. Iremos também usar no nosso monitoramento os máquinas da sub rede do SGCLab, o servidores SNs e os servidores mon-ca, mon-gsoc, SGCLab, sgcweb, sinergia, snvms, sn23. Usaremos as estações de trabalho utilizadas pelos alunos da pós-graduação do IC em nosso monitoramento.

Criamos 7 grupos de monitoramento inicialmente, com os seguintes nomes:

- **servidoresICnivel1**, composto pelos servidores abacate, acai, dida-fw, dmzhost1, dmzhost2, dracula, fruteira, gsstore, guarana, lcc-fw, mangamx, mangostin, mxsec, taffarel, tangerina,
- **servidoresICnivel2**, composto pelos servidores mon-ca, mon-gsoc, sgclab, sgcweb, sinergia, sn23, snvms,
- **Sns**, composto pelos servidores SNs mencionados anteriormente,
- **Impressoras**, composto pela impressora dccprinter,
- **maquinasFrutas**, composto pelos terminais que foram nomeados com nome de frutas, mencionados anteriormente,
- **internet**, esse grupo foi composto para medir a conectividade de rede, com a monitoração dos sites da UFF e do google e por fim o
- **Servidor_Nagios**, grupo que mostra o servidor NAGIOS em si.

Para monitorar os serviços de cada máquina, o modo de monitoramento do NAGIOS escolhido foi o NRPE(Nagios Remote Plugin Executor), explicado no capítulo 3. Este modo foi escolhido por se adequar aos objetivos do monitoramento, tornar o monitoramento mais próximo da experiência que o usuário teria se sofresse com os problemas. Com o NRPE, temos mais segurança, visto que o tráfego entre o servidor NAGIOS e o cliente é encriptado. O NRPE usa conexão tcp, e a comunicação entre o servidor e cliente é feita de forma que somente o servidor inicie a conexão e o cliente só aceite a conexão do servidor. Com o NRPE e um plugin adequado, podemos monitorar virtualmente tudo dentro do cliente.

Com o NRPE instalado, alguns servidores tiveram especificados pela equipe do suporte os serviços que deveriam ser monitorados e também que componentes de hardware do servidor deveriam ser monitorados, abaixo, são listados alguns desses componentes e serviços.

Componentes:

- Uso de CPU em porcentagem

- Uso da memória em porcentagem

- Load Average

- IOWait

- Temperatura

Serviços:

- Conectividade

- Tamanho da fila de e-mails

- DNS

Com isso, podemos dar início a configuração do servidor novo sgcmon. Discutimos com a equipe de suporte do IC e delineamos a estratégia de monitoramento para cada grupo. Para os grupos SNs, maquinasFrutas e impressoras a equipe somente desejava saber o status delas, se estavam ligadas ou não, logo nesses grupos só testamos sua conectividade, através de um plugin que fazia ping para cada máquina.

Os servidores do grupo servidoresICnivel1, objetos de nosso estudo e os servidores do grupo servidoresICnivel2 tiveram atenção especial e além de terem sua conectividade testada, testamos mais outros serviços deles, tais com o monitoramento de backups, que infelismente não foi implementado por falta de tempo. Decidido os grupos, a próxima etapa foi a discursão da frequência de monitoramento de cada grupo. Definimos como frequência o intervalo de tempo que o servidor NAGIOS irá checar as outras máquinas da rede pra receber dados sobre eles.

Focando-se no grupo de servidores nível 1, se faz necessário frequências altas, pois caso algo aconteça com as máquinas desse grupo, serviços essenciais para os usuários do IC podem não funcionar de forma correta ou até parar de funcionar. Nesse grupo definimos em 1 minuto para teste de conectividade e 5 minutos para serviços. Para outros grupos definimos frequências maiores, entre 5 e 10 minutos para conectividade. Definidos os grupos, serviços e frequências, configuramos a ferramenta.

A medida que a configuração dos serviços nas máquinas avançava, conversas eram mantidas com a equipe do suporte. Com isso mais serviços e máquinas foram adicionados e/ou removidos, bem como os serviços a serem monitorados. Nas figuras 4.10 e 4.11, mostramos como ficou a monitoração de serviços do servidor Mangamx na página da web do servidor sgcmon.

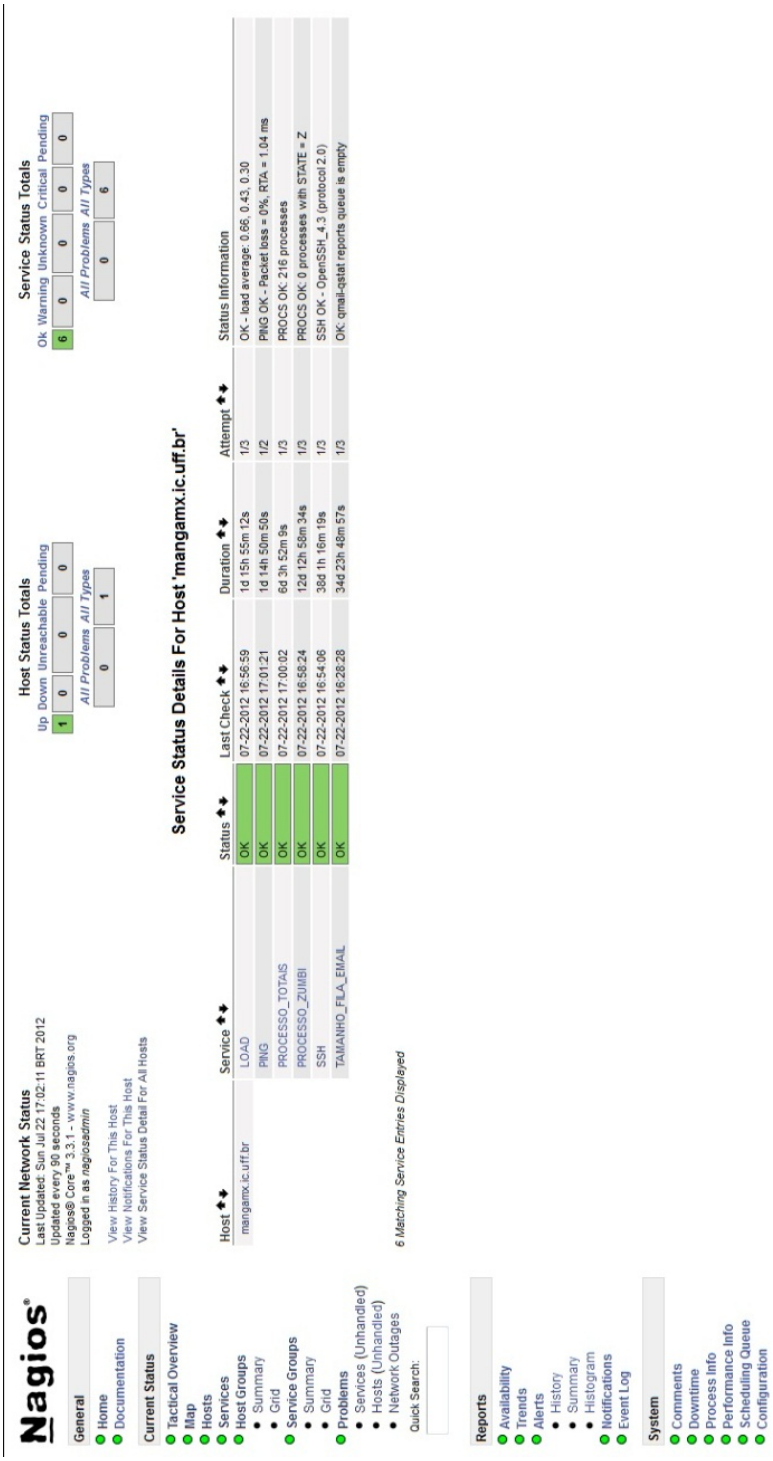

Figura 4.10: Visão especifica do servidor mangamx, com seus serviços.

Foi feito um período de testes para confirmar que os plugins estão funcionando com os limites corretos. Nesse período de teste, foi verificado que vários plugins estavam dando "falsos negativos" para problemas, com isso foi discutido com o suporte e alterações nos limites dos alarmes dos plugins foram feitos para refletirem a realidade do ambiente da rede. Foram também sugeridos frequências dos alarmes para os plugins, de acordo com a

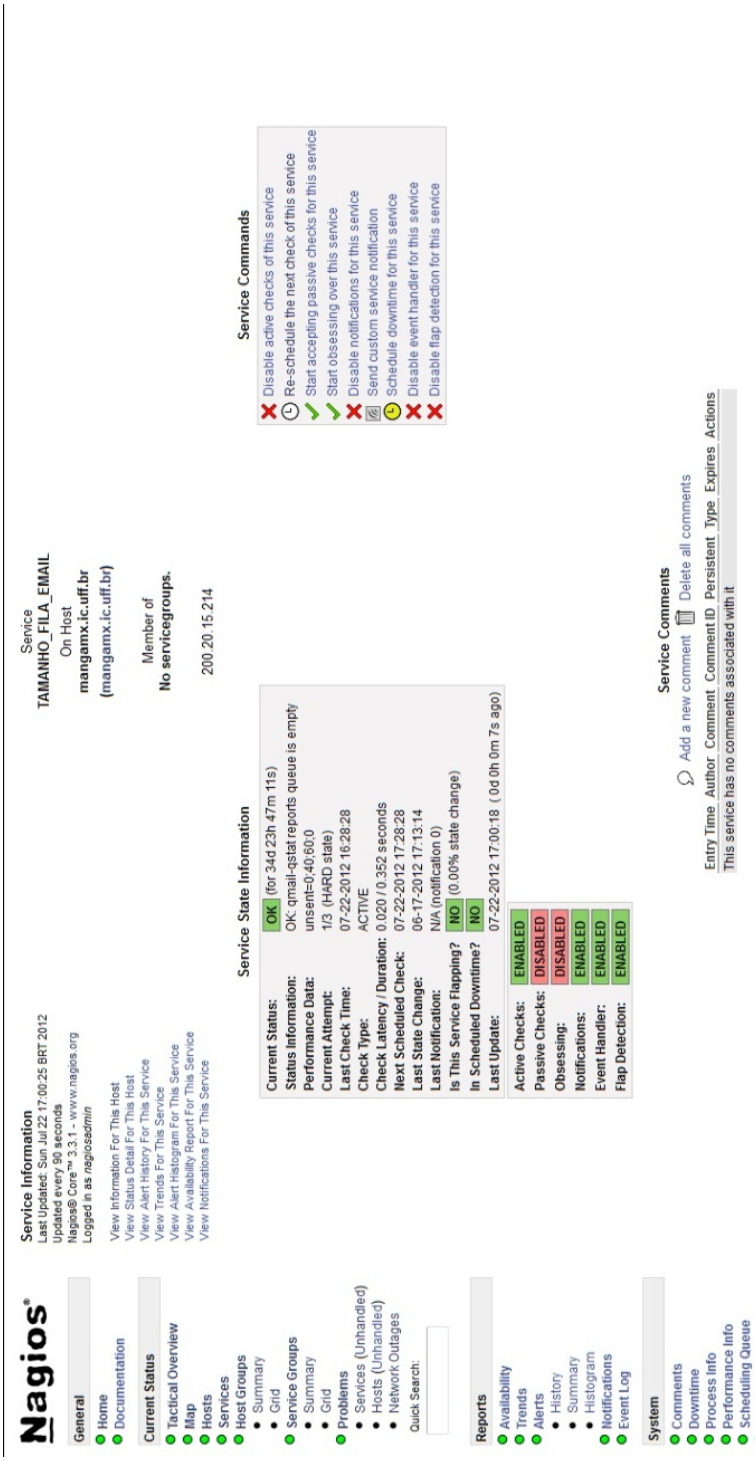

Figura 4.11: Visão específica do serviço TAMANHO_FILA_EMAIL, que verifica o tamanho da fila de e-mails que no servidor de e-mails e alarma quando a fila tem um certo número de e-mails enfileirados.

importância do serviço e do servidor, e a adição de novos servidores, no capítulo 5 mostrarmos alguns dos alarmes mandados pela ferramenta. Com isso, temos o monitoramento das maquinas mostrados nas figuras 4.12, 4.13 e 4.14.

Figura 4.12: Tela mostrando o grupo Impressoras, Internet e Maquinas_Frutas.

4.5 Resumo

Os servidores do Instituto de Computação necessitavam ser monitorados, a fim de permitir uma rápida resposta aos problemas que possam vir a aparecer.

A solução adotada, em conjunto com a equipe de suporte, foi separar os servidores

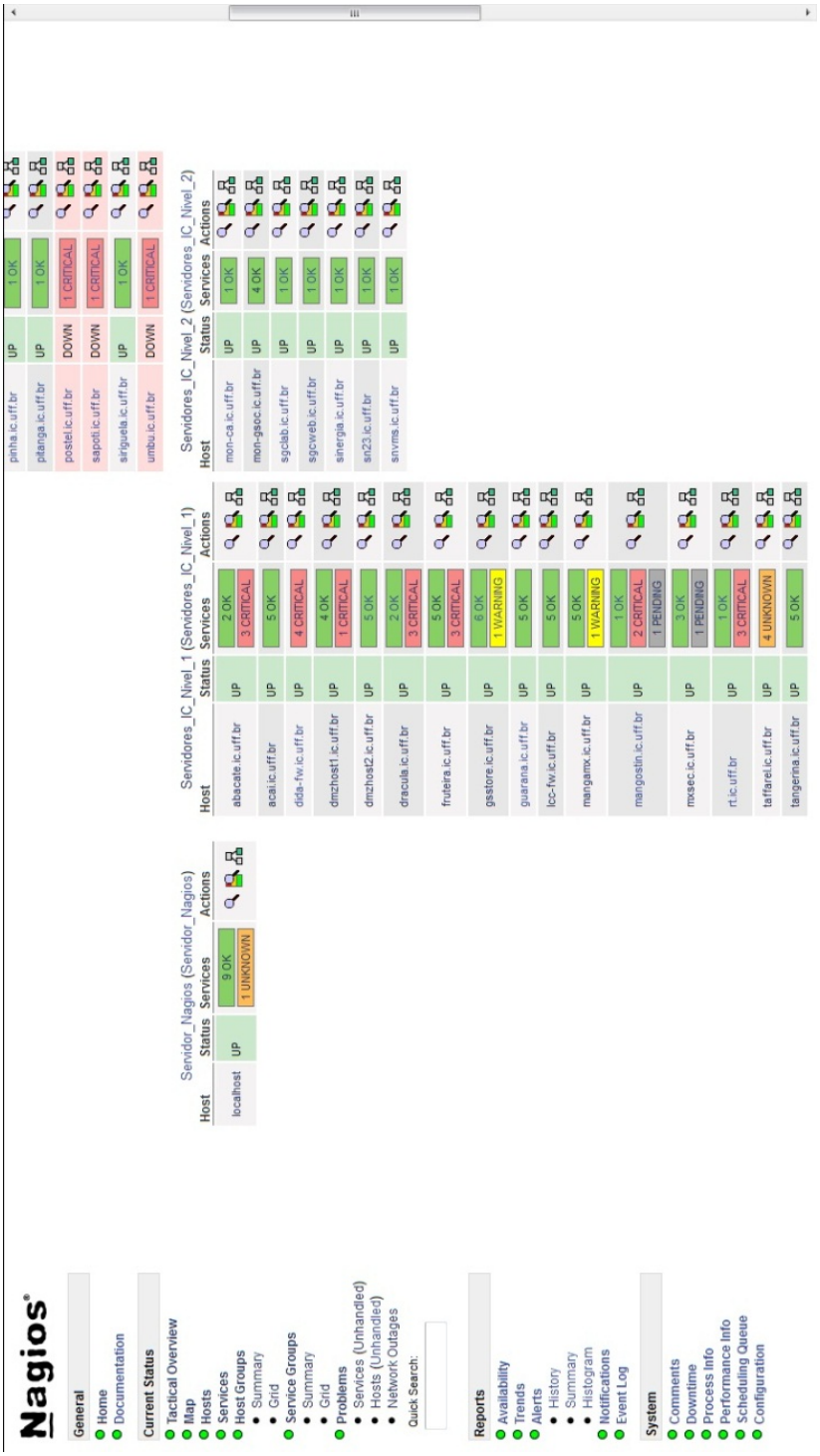

Figura 4.13: Tela mostrando o grupo Servidor_Nagios, Servidores_IC_Nivel_1, Servidores_IC_Nivel_2.

em grupos, de acordo com sua importância para o funcionamento da rede do Instituto. Criamos grupos de servidores e máquinas. A partir dai, foi dado um período de teste para validar se as configurações foram acertadas. A partir dos dados coletados, ajeitamos as configurações de acordo com as demandas levantadas pela equipe do suporte.

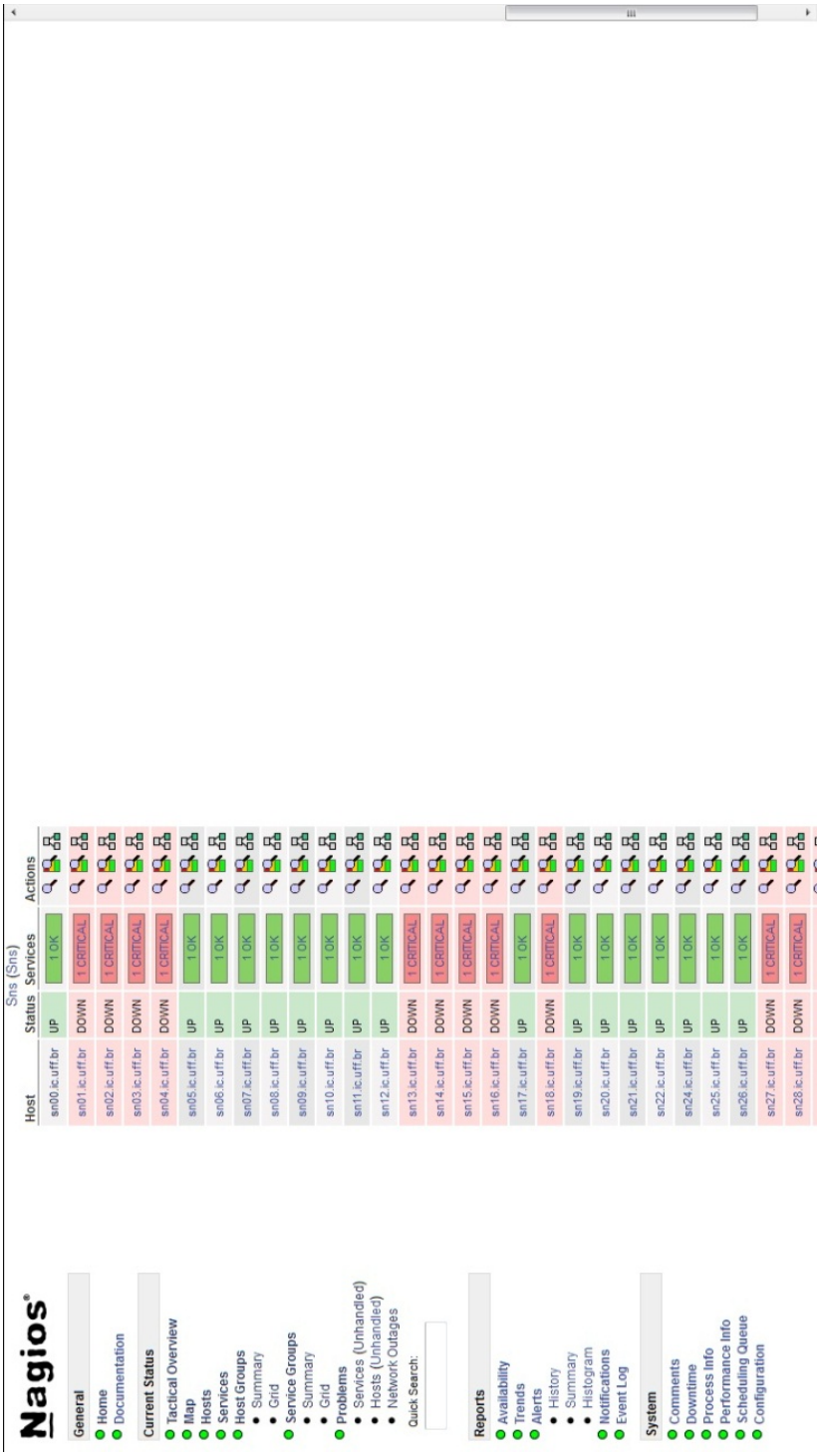

Figura 4.14: Tela mostrando o grupo Sns.

Capítulo 5

Análise de Disponibilidade

Para mostrar que a ferramenta está cumprindo o que se propõe, analisaremos nesse capítulo os relatórios de disponibilidade fornecidos por ela. Verificaremos seus serviços e assim poderemos mostrar o comportamento da rede em que os nós estão.

5.1 Relatório de Disponibilidade

A ferramenta nos fornece um relatório de disponibilidade para cada um de seus nós. Nele podemos ver o estado da cada serviço do nó, bem como o seu próprio estado, além de entradas no log do NAGIOS dele. Temos para cada estado possível para servidor (UP, DOWN, UNREACHABLE, UNDETERMINED), a razão para o estado, o tempo em que ficou o estado e as porcentagens de tempo total e tempo conhecido em que o estado estava ativo. Para os serviços mostramos as porcentagens de tempo em que o serviço ficou OK, Warning, Unknown, Critical e Undertemined, com a média para cada.

Para amostra, iremos analisar os relatórios das máquinas: lcc-fw, mangamx, mon-gsoc e os testes que são feitos para avaliar se o link da uff e para a internet estão online.

5.2 Análise dos Relatórios:

5.2.1 Lcc-fw

Firewall responsável pelo controle do fluxo de dados para o laboratório de graduação do Curso de ciência da computação, seu relatório de disponibilidade tem essa configuração

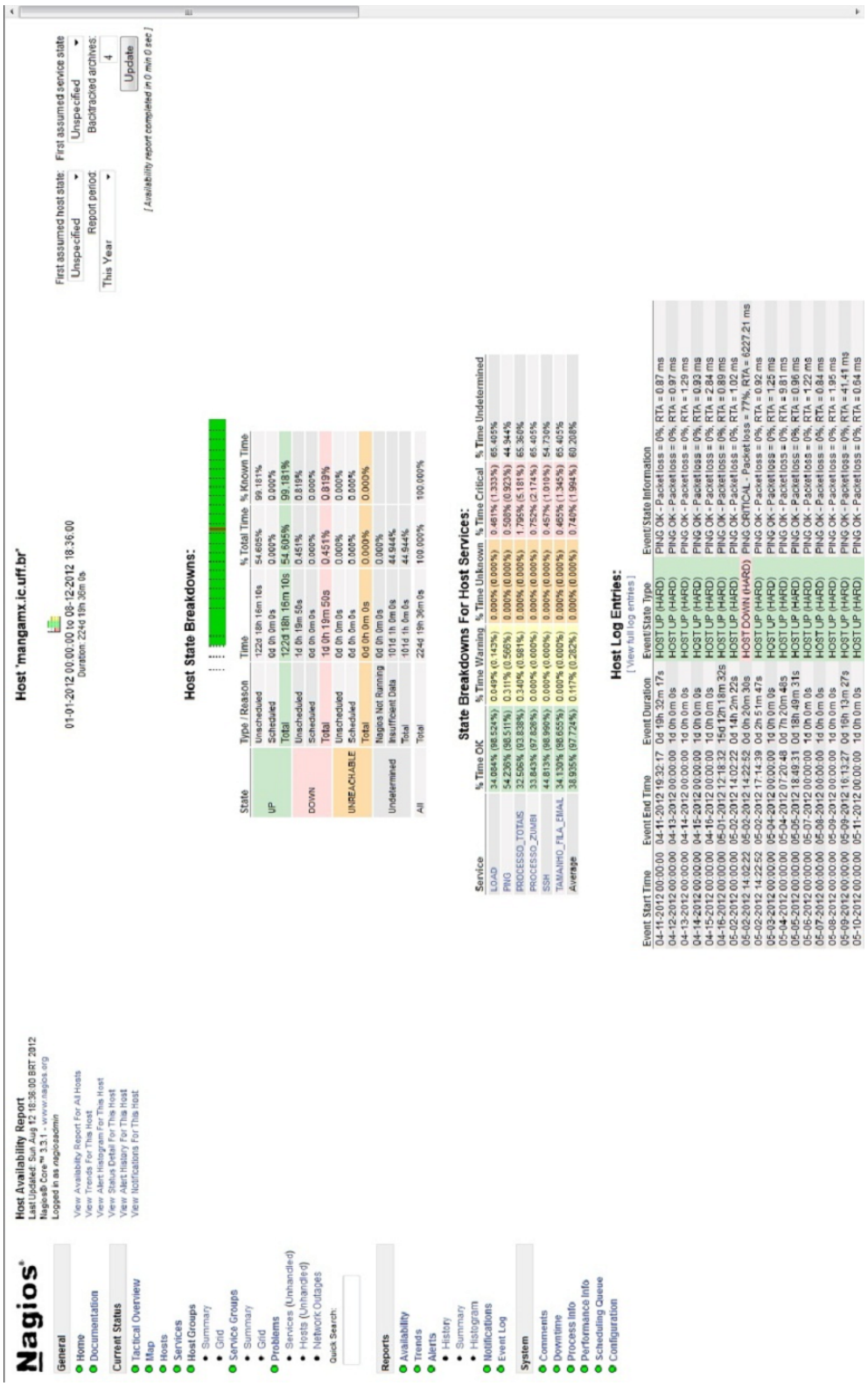

Figura 5.1: Tela exemplo que mostra o relatório de disponibilidades do servidor mangamx.

mostrada na figura 5.2

Ao analisarmos o relatório, vimos que neste ano (2012), essa máquina esteve com seu status de UP em 65.640% do tempo e em status DOWN em 34.360%, porcentagens de

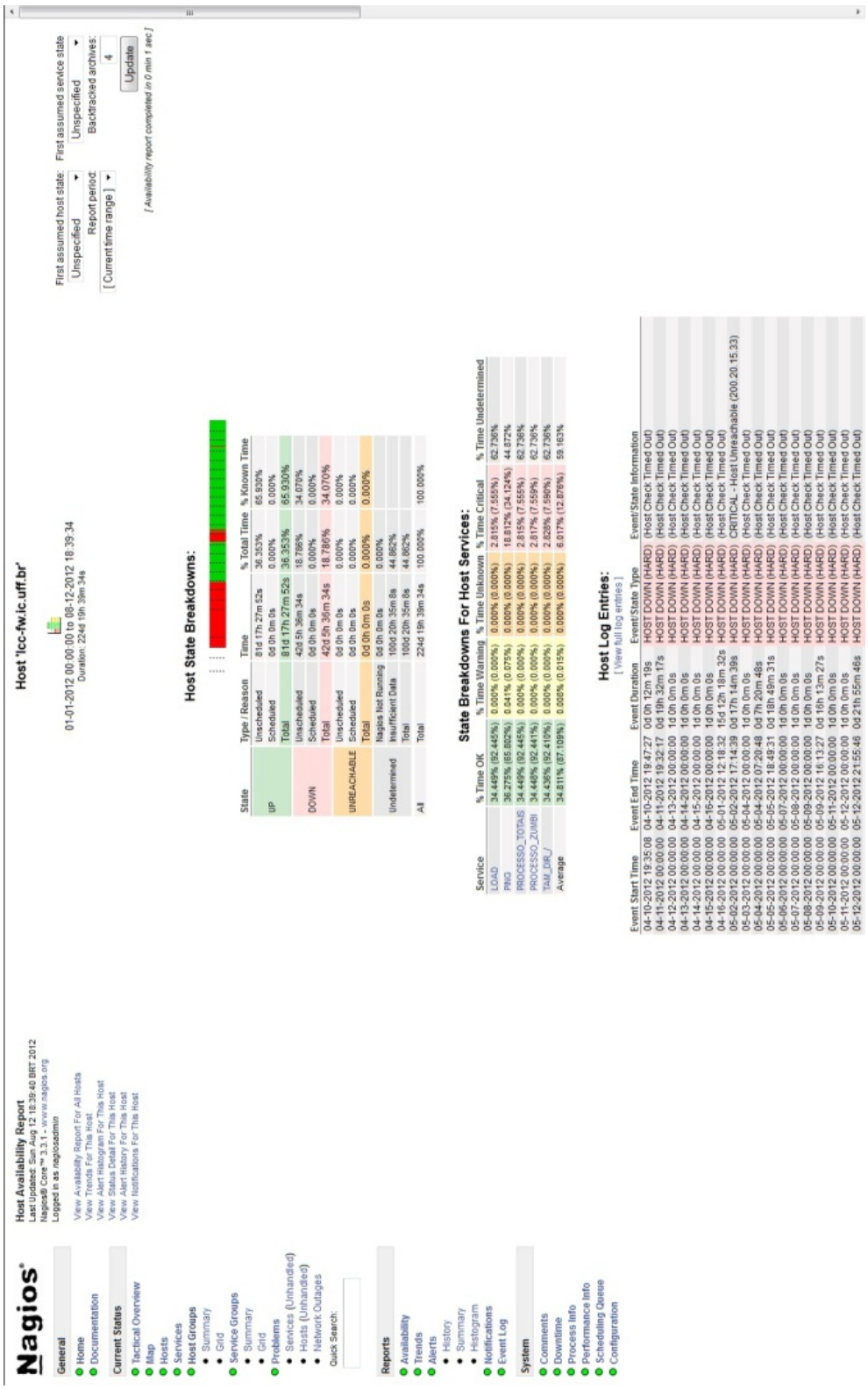

Figura 5.2: Tela mostrando o relatório de disponibilidades do firewall lcc-fw.

tempo conhecido. Ao observarmos a entradas no log do firewall, podemos identificar que a máquina passou a ser monitorada de fato a partir do dia 16 de maio deste ano como podemos ver nas figuras 5.3 e 5.4.

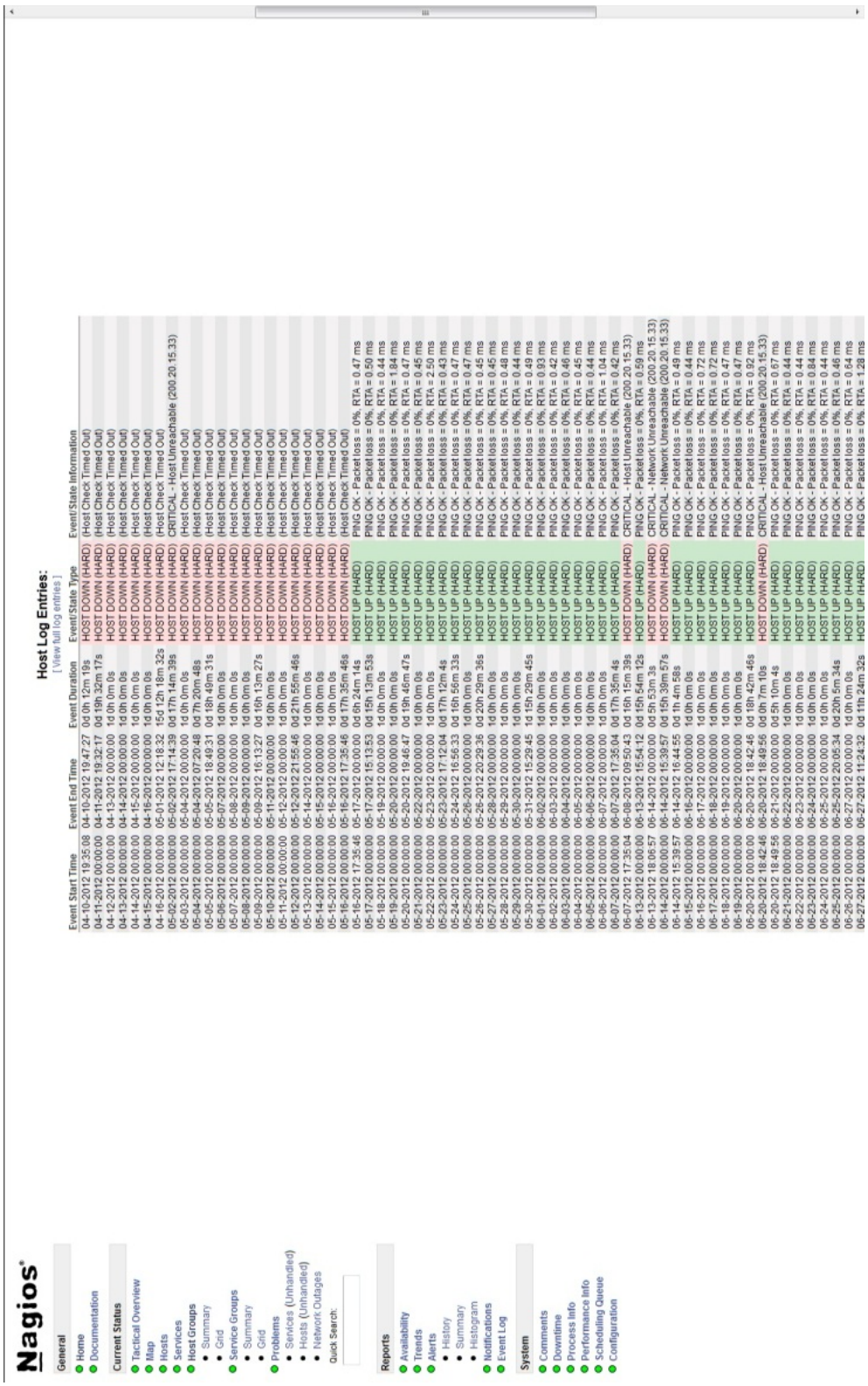

Figura 5.3: Tela mostrando o relatório do lcc-fw, mostrando as entradas do log o status do firewall.

Nos logs, vimos que a maioria das entradas de problemas (SERVICE CRITICAL) aconteceu por problema de perda de pacotes, um motivo possível dessa perda pode ser

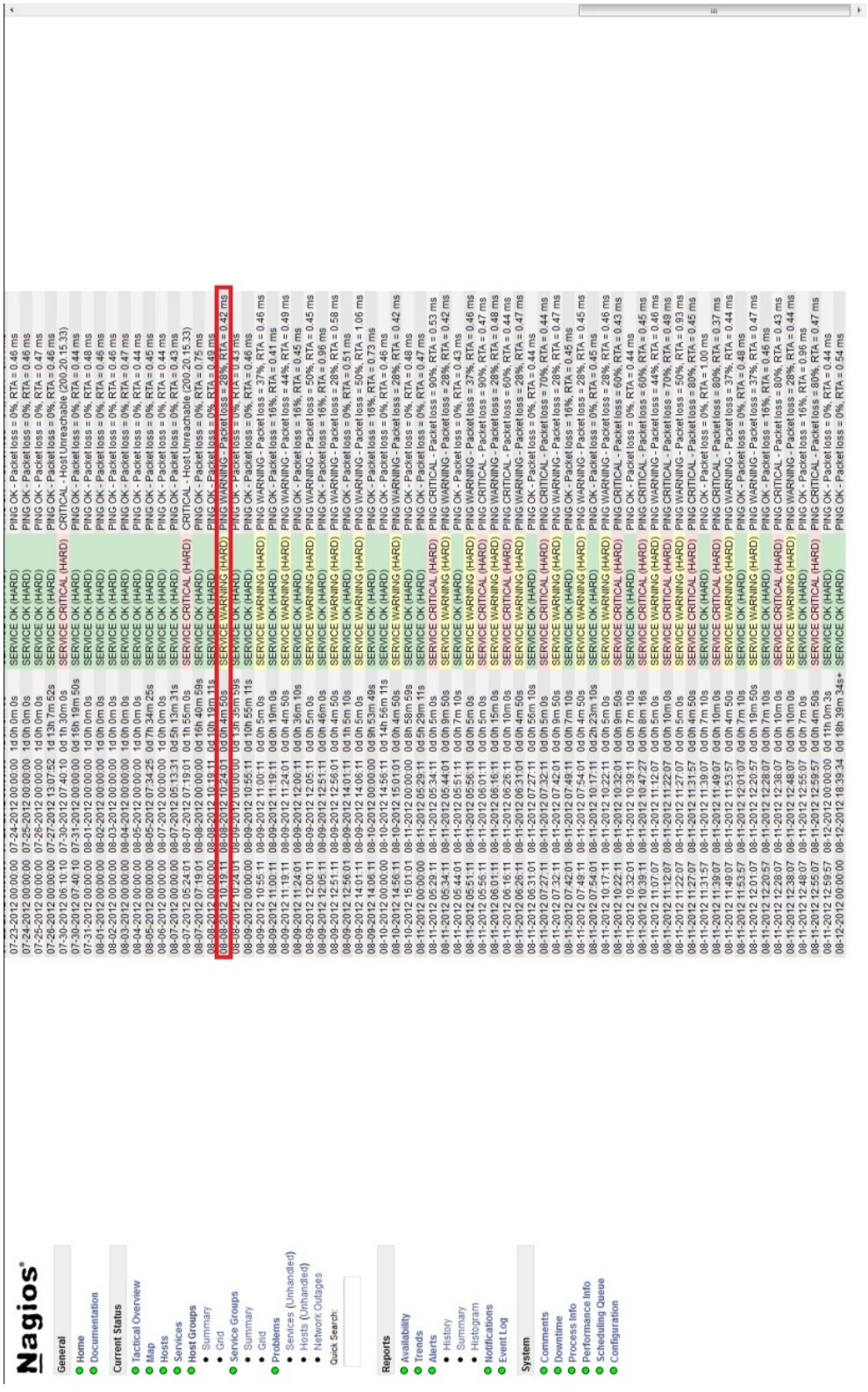

Figura 5.4: Tela mostrando o relatório do lcc-fw, mostrando o status do firewal (Pacotes).

por causa do firewall descartar pacotes de ping porque o firewall assumiu algum tipo de acesso não autorizado, pois em todas as medidas de RTA, que é a média do de tempo (em milisegundos) que o pacote de ping leva para ir do servidor nagios até a máquina ao qual

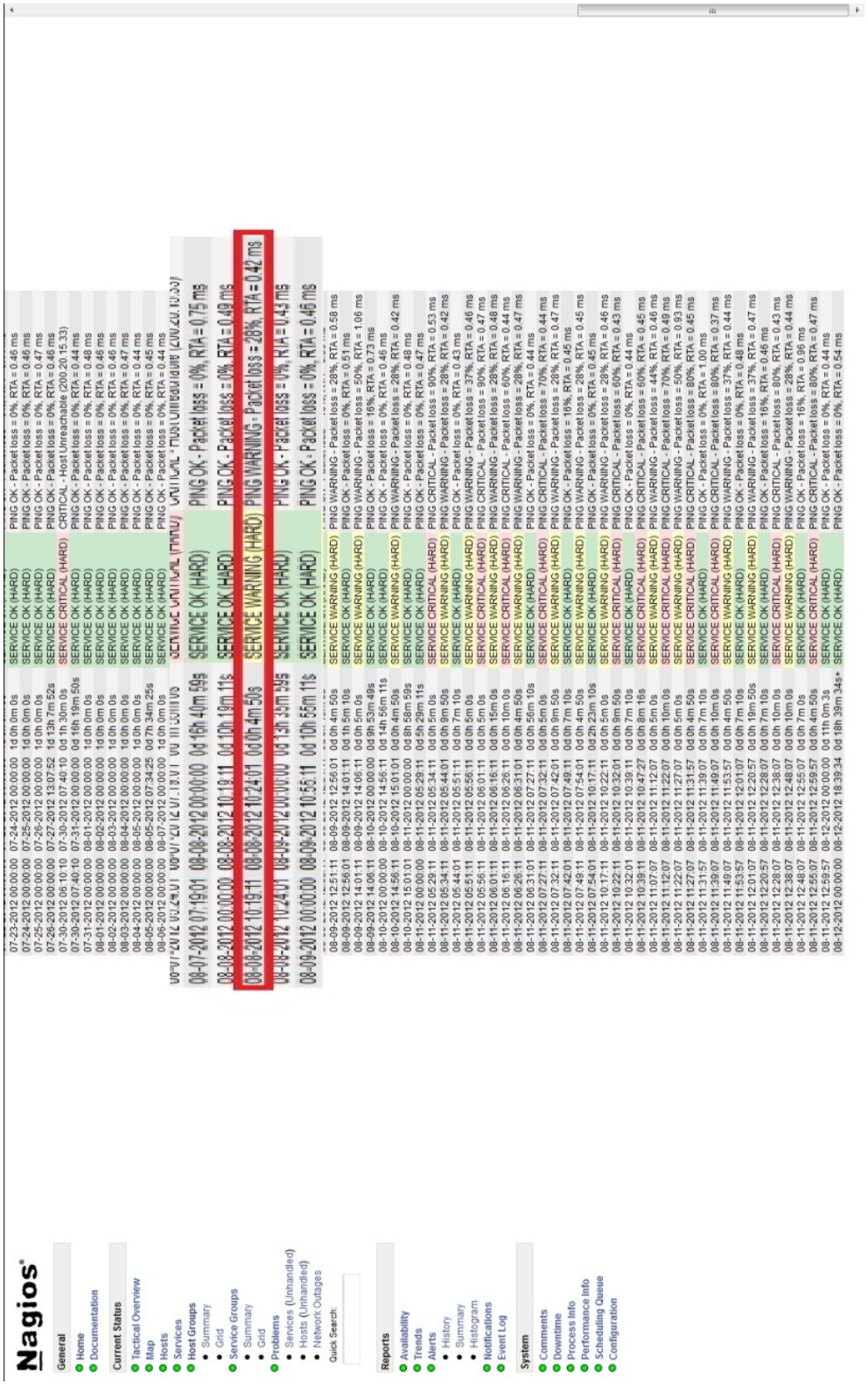

Figura 5.5: Tela mostrando o relatório do lcc-fw, mostrando o status do firewal (Pacotes) detalhado.

foi feita o ping e voltar para o servidor NAGIOS foram menores de 1 milisegundo (RTAs abaixo de 100 milisegundos são considerados bons) e o tempo de problema medido não

foi alto (menor que 10 minutos).

5.2.2 Mangamx

O servidor mangamx é o servidor de e-mails do Instituto de computação da UFF, nele além de ser necessário saber de sua disponibilidade, é necessário também saber sobre sua fila de envio de e-mails, onde se torna perigoso se essa fila estiver muito grande (valor determinado pelo grupo de suporte). Seu relatório é 5.7.

Analisando o relatório, vimos uma alta porcentagem de tempo no estado UP, tendo menos de 1% no estado DOWN. Este estado DOWN deve-se a pequenos problemas de comunicação entre o servidor NAGIOS com o agente de monitoramento instalado no servidor mangamx. Podemos assim assumir que este servidor está funcionando bem.

Vendo o relatório do serviço que mede a quantidade de e-mails a enviar, podemos afirmar que não tivemos problemas de enfileiramento, que poderia significar que os emails não estão sendo enviados, pois o status OK do serviço esteve por 98.654% do tempo de monitoramento do serviço. Os únicos problemas apresentados foram de comunicação entre o agente na máquina e o servidor NAGIOS. Através desse relatório, podemos ver também que a fila de e-mails teve no máximo 9 emails, talvez seja necessário um ajuste nos limites do alarme para que ele fique mais próximo da realidade.

5.2.3 Mon-gsoc

O servidor mon-gsoc é um servidor NAGIOS configurado anteriormente onde se monitora a autoridade certificadora que é mantida pelo professor Vinod Rebello do laboratório SGCLab. Nela são monitorados a lista de certificados revogados e seu próprio certificado, necessário para seu funcionamento. O servidor tem esse relatório mostrado na figura 5.7.

Ao analisar o relatório, é possível, apesar de serem poucos, intervalos de tempo grandes em que foi avisado que a máquina estava com estado DOWN, isso foi por problemas no servidor de máquinas virtuais caiu e a máquina não subiu corretamente, além de problemas de comunicação entre a agente na máquina e o servidor NAGIOS. Analisando também os relatórios de certificados_revogados_ca e certificados_ca, vimos que o monitoramento do certificados revogados da ca está funcionando corretamente e está avisando quando é necessário a atualização desses certificados bem como tivemos problemas de comunicação entre o servidor NAGIOS e a máquina5.11 e 5.10

Figura 5.6: Tela mostrando o relatório do MANGAMX.

No relatório de certificados_ca, podemos ver que o problema foi de comunicação do agente com o servidor NAGIOS. No certificados_revogados, não se configura problema, quando o status do serviço muda, é uma forma de avisar ao administrador da autoridade

Figura 5.7: Tela mostrando o relatório de TAMANHO_FILA_DE_EMAIL.

certificadora que a lista necessita ser renovada 5.8.

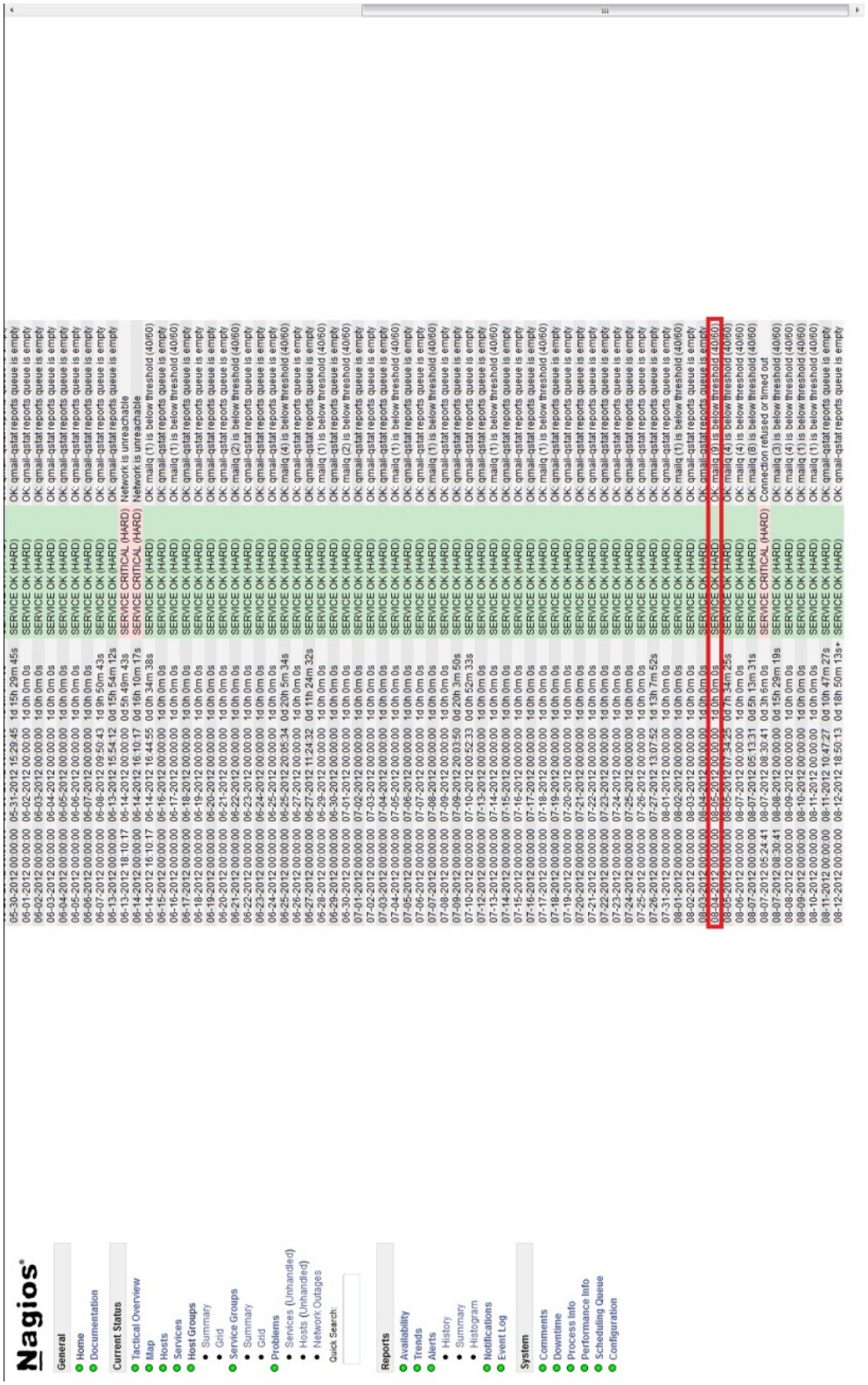

Figura 5.8: Tela mostrando a entrada no log.

5.2.4 Links Google e UFF

Monitoramos os sites da google e da UFF para poder saber quando a comunicação do IC para o mundo é perdida. Os relatórios de disponibilidade deles são 5.13 e 5.14

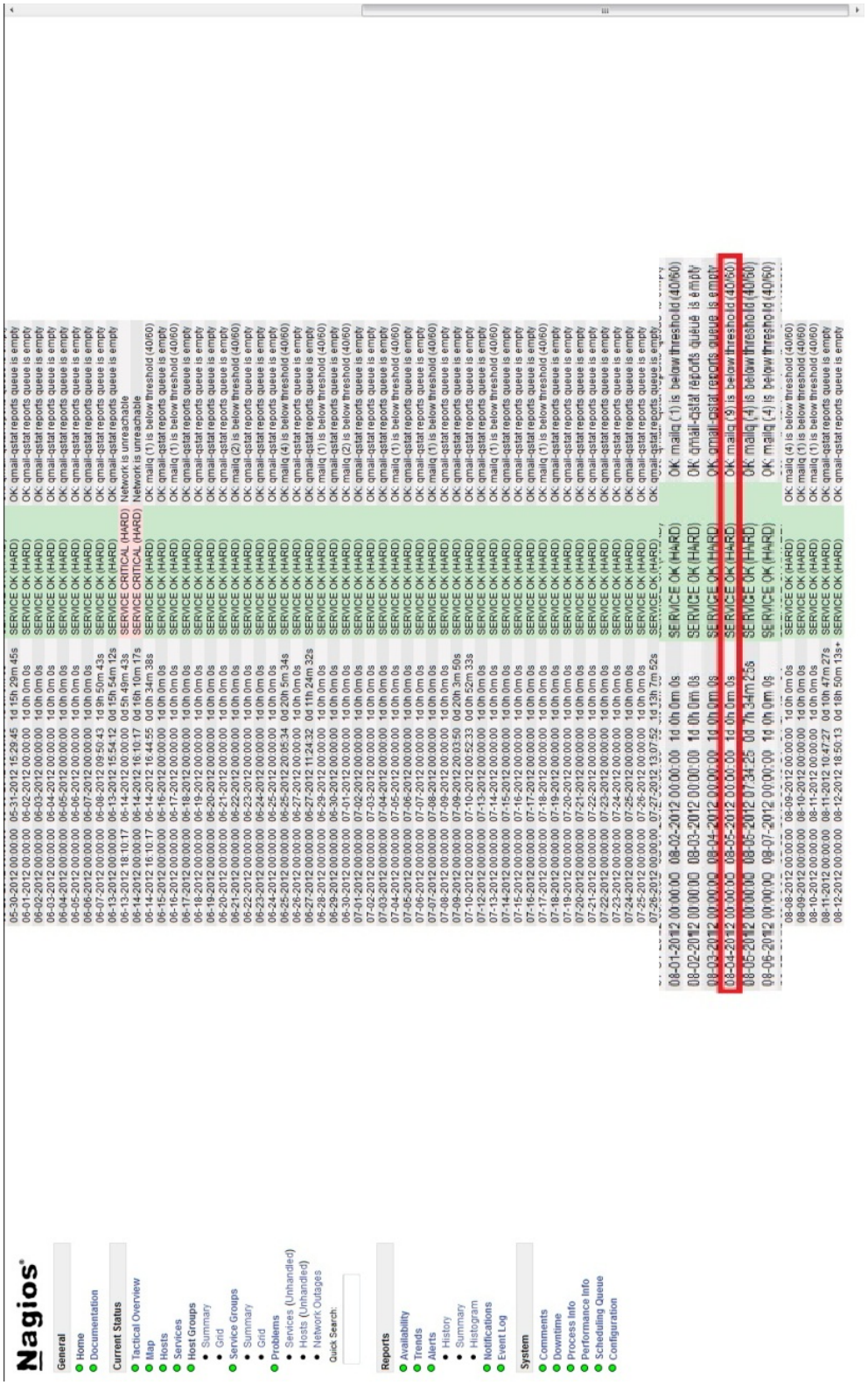

Figura 5.9: Tela mostrando a entrada no log (detalhado).

Nesses relatórios podemos ver que os problemas encontrados foram em se entender a URL do google e da UFF. Esses problemas foram resolvidos ao reiniciar o NAGIOS e trocar a URL do google por seu IP.

Figura 5.10: Tela mostrando o relatório do mong-soc.

5.3 Resumo

Nesse capítulo mostramos alguns relatórios de disponibilidades de servidores da UFF. Através desses relatórios, conseguimos ver como cada um dos servidores escolhidos como

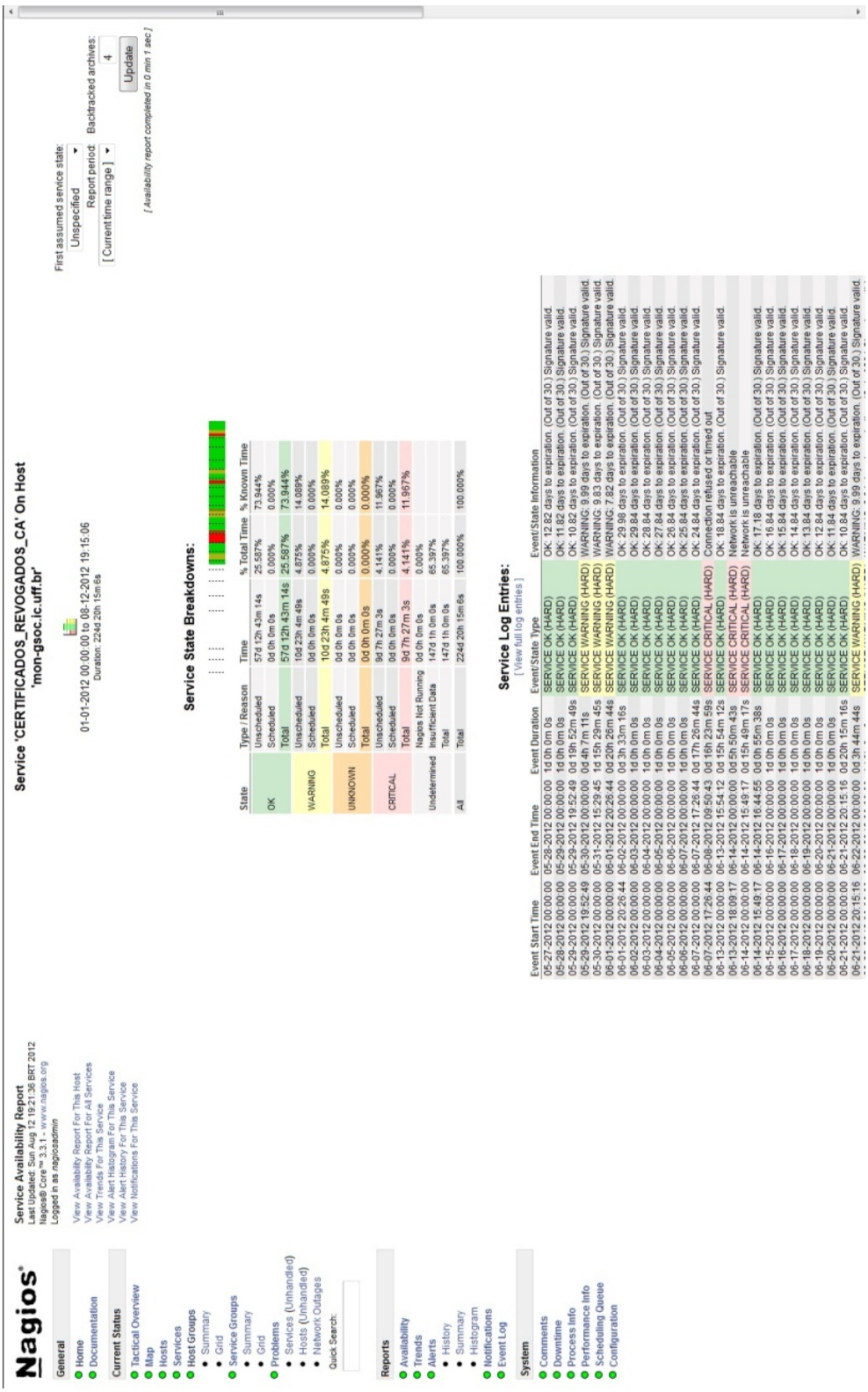

Figura 5.11: Tela mostrando o relatório do serviço CERTIFICADOS_REVOGADOS_CA.

exemplo para demonstração se comportou desde o momento em que a monitoração se iniciou. Vimos que a maioria dos servidores tiveram alguns mínimos problemas, desde quedas pequenas de comunicação até problemas de configuração e que a monitoração está

Figura 5.12: Tela mostrando o relatório do serviço CERTIFICADOS_CA.

funcionando como deveria.

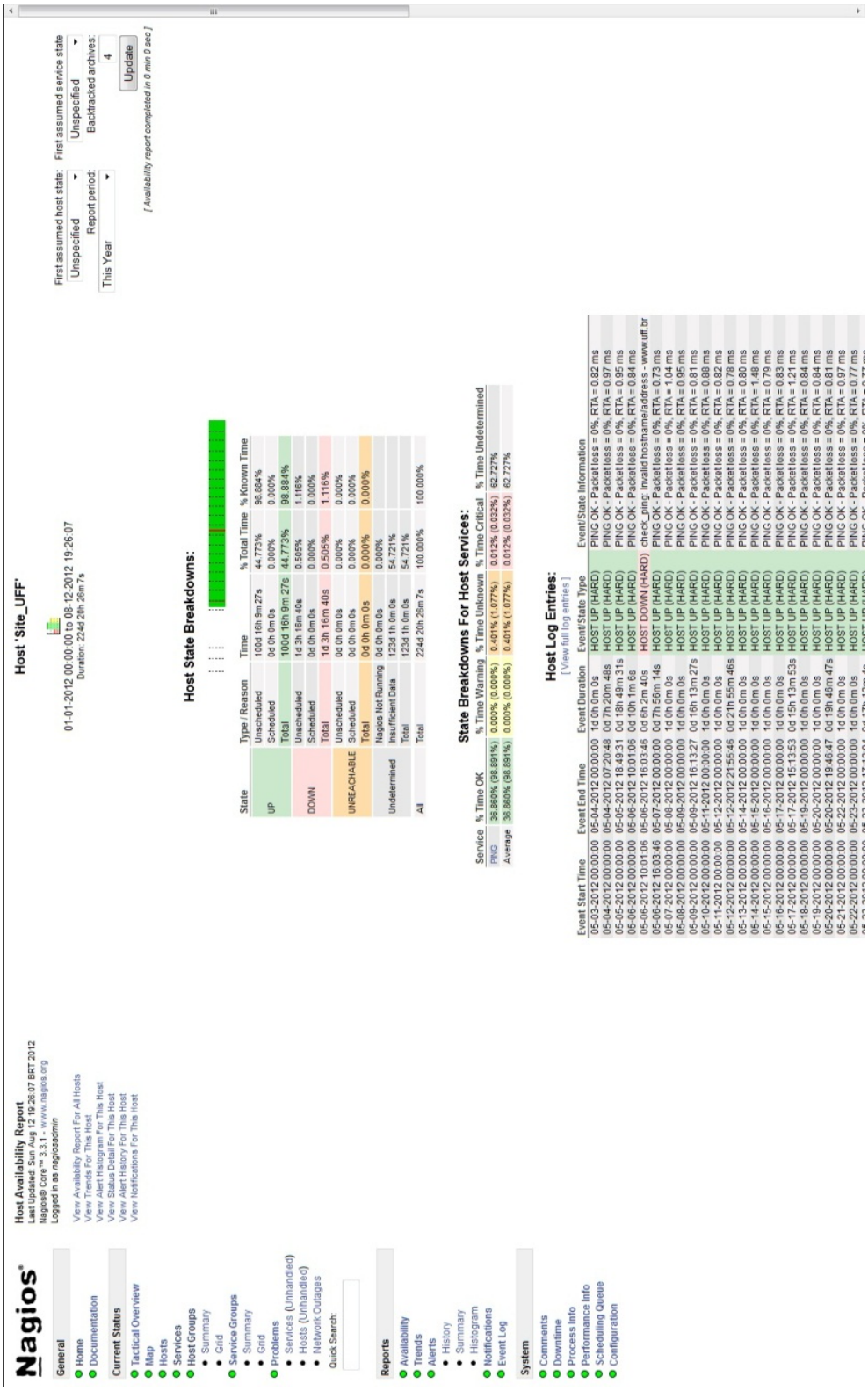

Figura 5.13: Tela mostrando o relatório do Site_UFF.

Figura 5.14: Tela mostrando o relatório do Google.

Capítulo 6

Conclusões e Trabalhos Futuros

A monitoração é um processo importante de controle, onde se pode ter ciência de todos os acontecimentos do sistema que se observa. É importante também pois através dessa observação, podemos prevenir problemas futuros ou diminuir e até erradicar problemas que acontecem.

Nesse trabalho o objetivo foi prover uma solução de monitoramento para a equipe de suporte do Instituto de Computação da UFF pudesse gerenciar as máquinas sob sua jurisdição, antes desse trabalho, a equipe não tinha nenhum modo de monitoração anterior e com isso, a cada problema que acontecia ou que viesse acontecer a equipe não era capaz de responder a tempo de impedir os transtornos ocasionados pelo problema. Um problema clássico sofrido pelo IC são as constantes faltas de luz e picos de energia que acabam comprometendo os serviços prestados pela rede do IC, sem a monitoração, a equipe só saberia desse tipo de problema quando os usuários da rede reportassem alguma falha do serviço ou se algum membro do da equipe notasse. Para entender o que é monitorar, foi feito um estudo sobre alguns conceitos, mostrados no capítulo 2. Enumeramos algumas ferramentas de monitoramento, explicando como elas funcionam e para qual foram desenvolvidas.

No capítulo 3, falamos sobre a ferramenta escolhida para o trabalho, a ferramenta NAGIOS, falamos sobre sua história, como foi criado, seu funcionamento. Mostramos o motivo da escolha e o que torna a ferramenta única. No capítulo 4, para o inicio do monitoramento, foram escolhidas os servidores mais importantes do instituto, de acordo com a avaliação da equipe do IC. Adicionamos mais grupos de servidores aos já escolhidos, como forma de avaliação da ferramenta. Instalamos a ferramenta e seus plugins, seguindo

os passos de seu desenvolvedor, após isso, fizemos a configuração da ferramenta para ela ser capaz monitorar esses servidores. De acordo com as orientações do grupo do suporte, fizemos também a configuração para monitoração dos serviços mais importantes desses servidores, estabelecendo as frequências dos alarmes desses servidores e serviços.

No capítulo 5, para mostrar como a ferramenta pode ser útil analisamos relatórios de disponibilidade de alguns servidores e vimos que através deles, podemos saber quanto tempo o servidor ficou indisponível, bem como os serviços relacionados ao servidor. Esse trabalho beneficiará a equipe do suporte do IC, pois assim dará poder para a equipe possa estar mais preparada para possíveis problemas vindouros e criar melhorias para a rede.

Como trabalhos futuros, projetar a ampliação da monitoração na rede para monitorar todos os computadores do IC, atualmente ela monitora a maior parte dos servidores e máquinas do laboratório de pós-graduação do instituto de computação. De acordo com o desenho da topologia abaixo, em nossa implementação inicial, focamos nos servidores principais do IC, servidores que são a espinha dorsal da rede e que sem eles, o instituto não funcionaria. Com isso não monitoramos as máquinas do laboratório de graduação do IC, nem as máquinas da secretaria do curso e a totalidade das máquinas do laboratório de pós-graduação.

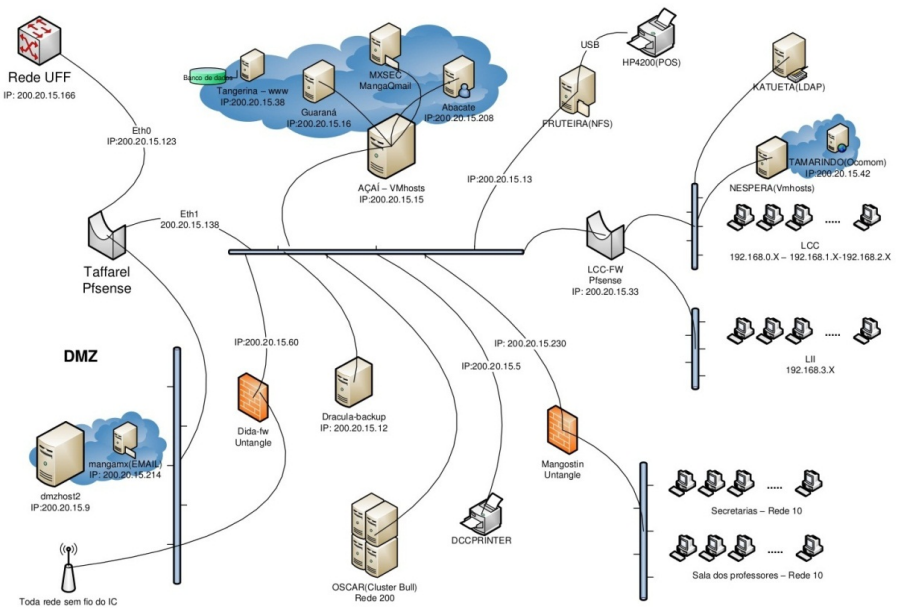

Figura 6.1: Rede IC.

Estudar melhorias na topologia de monitoramento para otimização, atualmente temos um único servidor NAGIOS (sgcmon) que monitora tudo, através de um plugin NAGIOS

chamado NRPE, explicado no capítulo 3. Para cumprir a meta de monitorar todos os servidores e máquinas do instituto, estudar se a atual implementação será adequada. O NAGIOS permite uma infinidade de topologias de monitoramento, para tipos de rede e tipos de máquinas. O monitoramento atual pode onerar o tráfego de rede do instituto, bem como os firewalls podem obrigar com que sejam necessários vários servidores NAGIOS entre as redes que são divididas por elas. O próprio servidor NAGIOS, caso sofra algum problema técnico, no atual modelo, seriam necessários reinstalar a ferramenta, para isso, podemos instalar um segundo monitor que assumirá em caso de falha do segundo.

Implantação de um projeto para enviar alarmes através de SMS. Atualmente no modelo de monitoramento, o alarme que o NAGIOS manda para avisar que alguma máquina está com problema é através do email. Caso a haja um problema na internet, uma falta de energia no laboratório onde o servidor NAGIOS se encontra, ou ainda um simples problema no servidor que o nagios usa pra enviar emails, o aviso não seria enviado. Para contornar o problema, o NAGIOS dá a opção de envio de alarmes através de envio de SMS, de acordo com o esquema mostrado na figura 6.2.

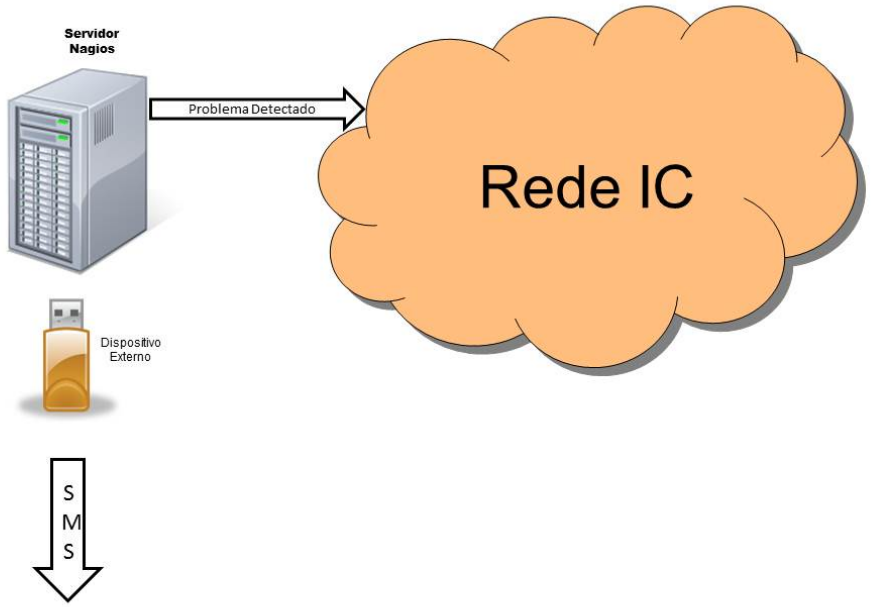

Figura 6.2: Envio de mensagens SMS.

Esse esquema não foi implantado, pois como é visto no esquema, é necessário um dispositivo externo para poder enviar os SMS, tais como um modem 3G ou um celular. Necessitamos também contratar um plano de telefonia para podermos enviar os avisos. Também se torna necessário um período de teste para verificar quantos SMS serão neces-

sários por mês para esse tipo de aviso.

Desenvolvimento próprio de ferramentas de integração entre servidores NAGIOS, atualmente, temos um servidor NAGIOS que faz a monitoração de autoridades certificadoras da organização IGTF. A organização mantem um NAGIOS localizado na europa, a associação asiática mantem outro na asia e existe outro, sob responsabilidade do SGCLab no Brasil. Foi iniciado um projeto que visa exibir os status de cada autoridade certificadora de cada um NAGIOS que as monitoram e um único lugar, com o nome de accms. Isso foi feito para ajudar os administradores desses nagios na identificação de problemas de concetividade. Caso uma autoridade certificadora esteja em vermelho em só um desses nagios, pode significar esse nagios está com algum problema de conectividade com a autoridade certificadora, caso seja exibido em tela que nos 3 nagios esta mesma autoridade esta com alerta vermelho, siginifica que ela pode estar com problema. Foi feito uma versão beta, porém é necessária sua melhoria.

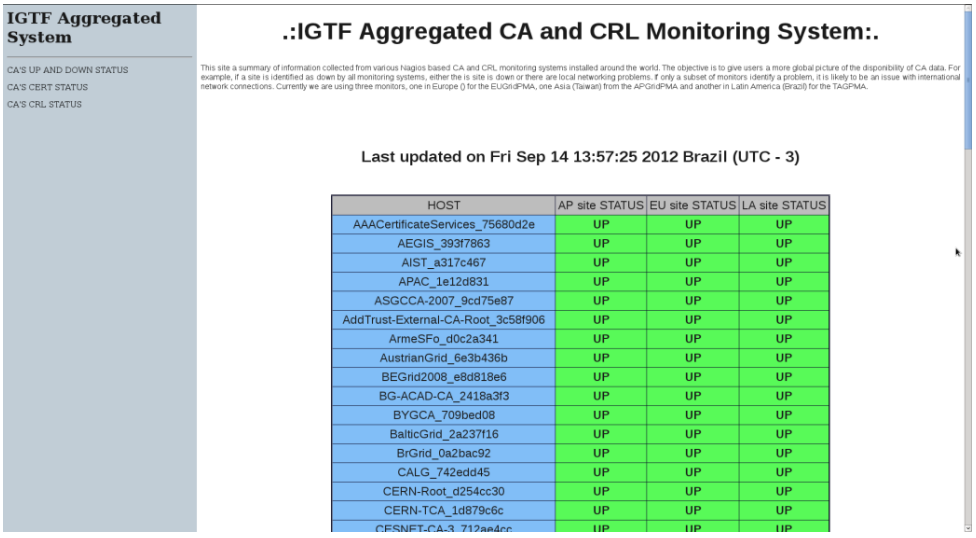

Figura 6.3: Foto da página do agregador accms.

Referências

[1] SNORT, network intrusion detection system. Último acesso 01/12/2011. http://www.snort.org/.

[2] CA Willy Introscope. Último acesso 16/09/2012. http://www.ca.com/br/application-management.aspx.

[3] WIKIPEDIA Monitoring tools. Último acesso 16/12/2011. http://en.wikipedia.org/wiki/Network_monitoring.

[4] NETWORK Monitoring Definition and Solutions. Último acesso 16/12/2011. *http* : *//www.cio.com/article/*133700/*Network_Monitoring_Definition_and_Solutions* .

[5] CLOUD Downtime costs. Último acesso 16/12/2011. http://searchcloudcomputing.techtarget.com/news/2240158511/Cloud-outage-report-of-13-providers-reveals-downtime-costs .

[6] WIKIPEDIA comparison table. Último acesso 16/12/2011. http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems.

[7] GANGLIA, monitoring system for high-performance computing systems such as clusters and Grids. Último acesso 16/09/2011. http://ganglia.sourceforge.net/.

[8] CACTI, The Complete RRDTool-based Graphing Solution. Último acesso 16/09/2012. *http* : *//www.cacti.net/*.

[9] GROUNDWORK Monitor. Último acesso 16/09/2011. http://www.gwos.com/.

[10] MICROSOFT Network Monitor. Último acesso 16/09/2011. http://www.microsoft.com/en-us/download/details.aspx?id=4865.

[11] WHAT'S UP GOLD. Último acesso 16/09/2011. http://www.whatsupgold.com/index.aspx.

[12] NAGIOS Core. Último acesso 16/12/2011. http://www.nagios.org/.

[13] NETSAINT. Último acesso 16/12/2011. http://netsaint.sourceforge.net/.

[14] SCHUBERT, M. et al. *Nagios 3 Enterprise Network Monitoring Including Plug-Ins and Hardware Devices.* [S.l.]: Syngress Publishing, Inc., 2008. ISBN 9781597492676.

[15] BARTH, W. *Nagios System and Network Monitoring, 1st ed.* [S.l.]: William Pollock, 2005. ISBN 1593270704.

[16] KOCH, M. Uma proposta de solução de gerenciamento de contabilização utilizando nagios e cacti. Disponível em: <https://www.repositorioceme.ufrgs.br/bitstream/handle/10183/15980/000695290.pdf?sequence=1>.

[17] NAGIOS Remote Plugin Executor. Último acesso 16/12/2011. http://nagios.sourceforge.net/docs/nrpe/NRPE.pdf .

[18] COSTA, M. G.; ALMEIDA, E. S. de. Monitoramento do estado real dos recursos computacionais de um datacenter com nagios. Disponível em: <http://fatecindaiatuba.edu.br/reverte/index.php/revista/article/view/42/45>.

[19] DIAS, D. B. N. D. A.; SOUZA, W. G. L.; FILHO, E. J. M. A. Redes monitoradas com cacti e nagios. Disponível em: <http://www3.iesam-pa.edu.br/ojs/index.php/computacao/article/view/230/221>.

[20] MOURA, M. D. de; BECKER, P. C. Utilização da ferramenta nagios para monitoramento de sinal de antenas de rede wireless. Disponível em: <http://sites.setrem.com.br/stin/2012/anais/Pedro.pdf>.

[21] ZANIKOLAS, S.; SAKELLARIOU, R. A taxonomy of gridmonitoring systems. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0167739X04001190>.

[22] NAGIOS Remote Plugin Executor Site. Último acesso 16/12/2011. http://exchange.nagios.org/directory/Addons/Monitoring-Agents/NRPE-2D-Nagios-Remote-Plugin-Executor/details .

[23] NAGIOS Remote Plugin Executor Site Details. Último acesso 16/12/2011. http://exchange.nagios.org/directory/Addons/Monitoring-Agents/NRPE-2D-Nagios-Remote-Plugin-Executor/details.

APÊNDICE A – Instalação Servidor Nagios

Este apêndice ensina como instalar o servidor nagios

A.0.1 Pré-requisitos:

- Apache
- PHP
- GCC compiler
- GD development libraries

Use o comando abaixo para a instalação:

```
yum install httpd php gcc glibc glibc-common gd gd-devel
```

Crie o usuário nagios com senha:

```
usr/sbin/useradd -m nagios
passwd nagios
```

Crie um novo grupo nagcmd para permitir comandos externos sejam submetidos através da interface web. Adicione o usuário nagios e apache neste grupo:

```
/usr/sbin/groupadd nagcmd
/usr/sbin/usermod -a -G nagcmd nagios
/usr/sbin/usermod -a -G nagcmd apache
```

Prepare um diretório para download dos arquivos de instalação:

```
mkdir /root/opt/nagios

cd /root/opt/nagios
```

Descompacte o arquivo baixado no site `http://nagios.org/download/core/thanks/` e entre no diretório `/root/opt/nagios`. Execute o script de configuração do servidor nagios, compile seu código fonte e instale seus arquivos binários:

```
./configure -with-command-group=nagcmd

make all

make install

make install-init

make install-config

make install-commandmode
```

Instale o arquivo de configuração web, crie o usuário administrador do nagios e lhe de uma senha:

```
make install-webconf

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

service httpd restart
```

Agora, devemos instalar os plugins do nagios. Acesse novamente a pasta `/root/opt/nagios` e baixe os plugins na pagina `http://www.nagios.org/download/plugins/`. Descompacte os arquivos e acesse a pasta criada. Execute o arquivo de configuração, compile e instale os plugins:

```
./configure -with-nagios-user=nagios -with-nagios-group=nagios

make

make install
```

Adicione o nagios a lista de serviços que iniciam quando o sistema operacional inicia e inicie o nagios:

```
chkconfig -add nagios

chkconfig nagios on

service nagios start
```

Caso aconteça algum erro na inicialização do nagios, utilize esse comando que identificará o erro:

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

Como nossa instalação foi feita em um sistema Linux (CentOS) baseado na distribuição Fedora, ele virá com o SElinux ativado em modo impositivo. Devemos deixar ele em modo permissivo. Para verificar o modo que está o SElinux, utilize o comando getenforce, caso a resposta desse comando for diferente de 0, devemos utilizar o comando setenforce 0, que deixará o o SElinux em modo permissivo. Reinicie o sistema para as modificações surtirem efeito.

Acesse a url `http://<endereço_do_servidor_nagios>/nagios/` com o usuário e senha do nagiosadmin para visualizar seu servidor nagios em ação.

APÊNDICE B - Instalação Nagios Remote Plugin Executor (NRPE)

Este apêndice ensina como instalar o Nagios Remote Plugin Executor (NRPE)

B.0.2 Instalando no lado do Servidor Nagios:

Baixe a versão mais nova do plugin no site do nagios[22] no diretório /root/opt/nagios.

Extraia a versão e acesse sua pasta. Compile e instale o plugin

```
item ./configure

make all

make install-plugin
```

Instalando na máquina a ser monitorada: Crie o usuário nagios e dê a ele um password:

```
/usr/sbin/useradd nagios

passwd nagios
```

Agora, devemos instalar os plugins do nagios para o NRPE usar. Acesse a pasta `/root/opt/nagios` e baixe os plugins na pagina `http://www.nagios.org/download/plugins/`. Descompacte os arquivos e acesse a pasta criada. Execute o arquivo de configuração, compile e instale os plugins:

```
./configure -with-nagios-user=nagios -with-nagios-group=nagios

make
```

```
make install
```

Edite as permissões para o diretório dos plugins e também as dos próprios plugins:

```
chown nagios.nagios /usr/local/nagios
```

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

Instale o Xinetd, se seu sistema não o tiver: `yum install xinetd`

Baixe a versão mais nova do plugin no site do nagios[23] no diretório `/root/opt/nagios`.

Extraia a versão e acesse sua pasta. Compile e instale o plugin, seu daemon e instale ele sobre o xinetd

```
./configure
```

```
make all
```

```
make install-plugin
```

```
make install-daemon
```

```
make install-daemon-config
```

```
make install-xinetd
```

No arquivo /etc/xinetd.d/nrpe, modifique a seguinte linha: `only_from = 127.0.0.1` para ip do servidor nagios.

Adicione a entrada para o daemon do NRPE em /etc/services e reinicie o serviço do Xinetd:

```
nrpe 5666/tcp # NRPE
```

```
service xinetd restart
```

Testando se o Nrpe funciona e se há conversa entre o servidor nagios e o nrpe na máquina alvo:

Testando se o Nrpe Funciona:

Na máquina cliente, verifique se o nrpe está rodando com o xinetd:

```
netstat -at || grep nrpe
```

Se a resposta do comando for iqual a esta `(tcp 0 0 *:nrpe *:* LISTEN)`, tudo ok. Caso contrário verifique se o xinetd está instalado, se o nrpe está corretamente rodando com o xinetd, se adicionou a referencia ao xinetd corretamente em /etc/services. Teste se o daemon do NRPE está funcionando corretamente:

```
/usr/local/nagios/libexec/check_nrpe -H <ip_maq_local>
```

Se o que retornar for: `NRPE v<versão_do_nrpe>`, tudo ok.

Testando a comunicação entre o servidor nagios e o nrpe:

No servidor nagios, use o comando:

```
/usr/local/nagios/libexec/check_nrpe -H <ip_maq_remota>
```

Se o que retornar for: `NRPE v<versão_do_nrpe>`, há conexão, então tudo ok.