ESCOLA POLITÉCNICA
DE PERNAMBUCO

d.s.c. UPE
Departamento de Sistemas e Computação

A IMPORTÂNCIA DO MONITORAMENTO DE ATIVOS DE REDES: UM ESTUDO DE CASO COM O SISTEMA CACIC

Trabalho de Conclusão de Curso

Engenharia da Computação

Henrique de Lima Dias
Orientador: Prof. Renato Mariz de Moraes

UNIVERSIDADE
DE PERNAMBUCO

HENRIQUE DE LIMA DIAS

A IMPORTÂNCIA DO MONITORAMENTO DE ATIVOS DE REDES: UM ESTUDO DE CASO COM O SISTEMA CACIC

Monografia apresentada como requisito parcial para obtenção do diploma de Bacharel em Engenharia da Computação pela Escola Politécnica de Pernambuco – Universidade de Pernambuco.

Recife, dezembro de 2008

Agradecimentos

Agradeço primeiramente aos meus queridos pais, Flavio Marcos Dias e Maria Quilma de Lima Dias, que sempre me incentivaram e se dedicaram para me oferecer um ensino de qualidade. Além de conselhos imprescindíveis à formação do meu caráter, sempre com muito carinho e amor que um filho pode receber. Agradeço também a minha querida irmã, Isabela Dias, e ao meu cunhado Bruno Ribeiro, pelo apoio dedicado nos anos de faculdade.

Agradeço ao professor Renato Moraes, pela competência com que desempenhou o papel de orientador e principalmente pelo excelente mestre que foi nas cadeiras que tive a honra de ser seu aluno.

Agradeço a todos os colegas que fazem ou fizeram parte do setor de Informática da Fundação Joaquim Nabuco no meu período de estágio, em especial Adriana Martins, Alexsandro Diniz, André Vale e Hugo Apolônio. Todos contribuíram bastante para a realização deste projeto.

Agradeço a todos os professores do Departamento de Sistemas e Computação da Universidade de Pernambuco, por contribuírem com a minha formação acadêmica e moral, especialmente a professora Cristine Gusmão, por mostrar a nós, alunos, o verdadeiro caminho do aprendizado.

Agradeço a todos os colegas da POLI com quem tive o prazer de compartilhar os conhecimentos aprendidos no período acadêmico. Em especial, agradeço aos meus grandes amigos Adriano Falcão, Adriano Rocha, Fagner Araújo, Fernando Rocha, Francisco Hamilton, George Silva, Leonardo David, Luiz Cláudio Dória, Marcelo Pita, Marcos Torres, Mateus Peregrino, Rafael Bezerra, Sérgio Guerra, Teógenes Bezerra, Thiago Melo e Túlio Alcântara. Obrigado a todos vocês pela força, apoio e companhia no decorrer do curso.

Finalmente, agradeço a Pryscilla Izabel Dias, minha namorada e que sempre esteve ao meu lado nos momentos de alegria e também de dificuldades. Você é uma pessoa incrível e desejo compartilhar diversos outros momentos de felicidade ao seu lado.

Resumo

A expansão das redes de computadores e o surgimento de novas tecnologias estão crescendo a cada dia. Atualmente, as redes e os recursos associados a elas são fundamentais e de extrema importância para uma organização. É imprescindível que elas não falhem e que os tempos de indisponibilidade sejam minimizados. Com isso, a administração e gerência dos recursos de Tecnologia da Informação (TI) têm sido uma demanda constante no ambiente corporativo, necessitando então de um monitoramento eficaz destes recursos. Para comprovar a importância do monitoramento de ativos de redes, esta monografia apresenta a implementação do sistema CACIC (Configurador Automático e Coletor de Informações Computacionais). A ferramenta foi desenvolvida pela Empresa de Tecnologia e Informações da Previdência Social (DATAPREV) e deverá ser implantada em todos os órgãos do Serviço Público Federal. Este trabalho descreve como ela foi implantada na Fundação Joaquim Nabuco (FUNDAJ). Aqui serão apresentados detalhes de configuração, utilização dos recursos e resultados obtidos pelo CACIC. Também serão apresentadas as modalidades de monitoramento de ativos de redes e alguns exemplos de ferramentas disponíveis no mercado. Para qualquer que seja a ferramenta utilizada para monitorar os ativos de redes, é importante saber que essa prática provê aos gestores e administradores de parques computacionais um importante auxílio na tomada de decisões estratégicas sobre a infra-estrutura instalada.

Abstract

The expansion of computer networks and the emergence of new technologies are growing every day. Nowadays, the networks and facilities associated with them are essential and extremely important to a corporation. It is important that they do not fail and that the periods of unavailability are minimized. With this, the administration and management of Information Technology (IT) resources have been a constant demand in the corporate environment, then requesting an efficient monitoring of these resources. To prove the importance of active network monitoring, this paper presents the implementation of the CACIC system (Automatic Configurator and Computing Information Collector). The tool was developed by Empresa de Tecnologia e Informações da Previdência Social (DATAPREV) and should be implemented in all organs of the Federal Public Service. This work describes its implementation in Fundação Joaquim Nabuco (FUNDAJ). Here are presented details of configuration, use of resources and results achieved by CACIC. Also presented are the procedures for active network monitoring, and some examples of tools available on the market. For whatever the tool used to active network monitoring, it is important to know that this practice provides the directors and managers of computing parks an important aid in making strategic decisions on the installed infrastructure.

Sumário

Índice de Figuras

Índice de Tabelas

Índice de Listagens

Tabela de Símbolos e Siglas

CACIC – Configurador Automático e Coletor de Informações Computacionais

FUNDAJ – Fundação Joaquim Nabuco

DATAPREV – Empresa de Tecnologia e Informações da Previdência Social

MPOG – Ministério do Planejamento, Orçamento e Gestão

TCP/IP – *Transmission Control Protocol / Internet Protocol* (Protocolo de Controle de Transmissão / Protocolo da *Internet*)

SNMP – *Simple Network Management Protocol* (Protocolo de Gerenciamento de Rede Simples)

OSI – *Open Systems Interconnection* (Interconexão de Sistemas Abertos)

CMIP – *Common Management Information Protocol* (Protocolo de Gerenciamento de Informação Comum)

RFC – *Request for Comments* (Pedido de Comentários)

MIB – *Management Information Base* (Base de Gerenciamento de Informação)

MRTG – *Multi Router Traffic Grapher* (Gráfico de Tráfego Multi Rota)

RRDToll – *Round-Robin Database Tool* (Ferramenta de Banco de Dados Round-Robin)

LAMP – Linux, Apache, MySQL, PHP

SMS – *Short Message Service* (Serviço de Mensagens Curtas)

SLTI – Secretaria de Logística e Tecnologia da Informação

GPL – *General Public License* (Licença Pública Geral)

TI – Tecnologia da Informação

IP – *Internet Protocol* (Protocolo da *Internet*)

MAC – *Media Access Control* (Controle de Acesso ao Meio)

RAM – *Random Access Memory* (Memória de Acesso Aleatório)

SGBD – Sistema Gerenciador de Banco de Dados

FTP – *File Transfer Protocol* (Protocolo de Transferência de Arquivos)

HTTP – *Hypertext Transfer Protocol* (Protocolo de Transferência Hipertexto)

HTML – *Hypertext Markup Language* (Linguagem de Marcação Hipertexto)

PHP – *Hypertext Preprocessor* (Preprocessador Hipertexto)

SPB – *Software* Público Brasileiro

HD – *Hard Disk* (Disco Rígido)

GD – *Graphics Draw* (Desenhos Gráficos)

CPU – *Central Processing Unit* (Unidade Central de Processamento)

BIOS – *Basic Input/Output System* (Sistema Básico de Entrada e Saída)

DNS – *Domain Name System* (Sistema de Nome de Domínio)

DHCP – *Dynamic Host Configuration Protocol* (Protocolo de Configuração Dinâmica de *Hosts*)

WINS – *Windows Internet Name Service* (Serviço de Nome de Internet *Windows*)

Capítulo 1

Introdução

Em decorrência dos benefícios que as redes de computadores oferecem, o seu crescimento é cada vez maior, uma vez que seus recursos e aplicações tornam-se ainda mais indispensáveis para as organizações que as utilizam. Com esta expansão, a possibilidade de ocorrerem problemas também aumenta, podendo levar as redes a um estado de inoperância ou a níveis inadequados de desempenho [28].

O rápido crescimento e a proliferação de novas tecnologias têm mudado a característica das redes de computadores nos últimos anos. O monitoramento, em tempo real, da infra-estrutura de redes e seus ativos (servidores, estações de trabalho e impressoras) vem se tornando indispensável na gestão da tecnologia da informação. Desta forma é possível obter as informações necessárias sobre estes equipamentos de modo rápido, sintético, preciso e confiável, facilitando as tomadas de decisão do gestor no momento do planejamento, adequação e expansibilidade do parque tecnológico. A verificação da performance de serviços e a resolução de problemas diversos, como conectividade e integração de plataformas, também ocorrem mais facilmente.

Entretanto, devido ao surgimento de novas aplicações, muitas vezes heterogêneas, o monitoramento das redes de computadores pode se tornar um verdadeiro desafio. Dependendo do tamanho da rede, tarefas antes consideradas simples, hoje podem ser bastante complexas, podendo até mesmo interferir no custo do gerenciamento. De acordo com [30], este custo pode chegar a 15% do total gasto com sistemas de informação em uma determinada empresa. Desta forma, o controle de uma rede de computadores não pode ser realizado apenas por esforço humano. A utilização de soluções automatizadas torna-se mais adequado.

Os sistemas de monitoramento permitem aos administradores de redes de uma organização saber instantaneamente se esses recursos estão operacionais ou não, sendo possível assegurar uma qualidade mínima dos serviços disponíveis a

seus usuários. De um modo geral, o controle dos ativos procura garantir o correto funcionamento de sistemas de informação que estão disponíveis nas redes de computadores.

A utilização de tecnologias *Web* é uma tendência no monitoramento de ativos de redes, uma vez que seu custo de implementação é reduzido. O acesso às informações geradas por essas tecnologias pode ser feito a partir de qualquer local e é totalmente independente de plataforma [10]. Por conta desses fatos, esta monografia desenvolveu como estudo de caso a implantação do sistema CACIC (Configurador Automático e Coletor de Informações Computacionais) na Fundação Joaquim Nabuco (FUNDAJ) a fim de se obter dados que comprovassem a importância do monitoramento dos ativos de redes de computadores.

O CACIC, considerado a primeira experiência consolidada de *software* livre desenvolvido e distribuído com segurança pelo setor público brasileiro, é um sistema de monitoramento que torna disponíveis informações através de uma interface *Web*, tais como: número de equipamentos e suas distribuições, configurações de *hardware*, *software* e rede, atualizações de segurança, variáveis de ambiente, uso do disco, impressoras e pastas compartilhadas, além de outras funcionalidades que serão vistas mais à frente. O sistema possibilita a manutenção periódica dos computadores ao permitir que problemas corriqueiros como a sobrecarga de espaço em disco, *software* de execução duvidosa e o pleno funcionamento do anti-vírus sejam diagnosticados com antecedência [15].

Desenvolvido pela Empresa de Tecnologia e Informações da Previdência Social (DATAPREV), o CACIC está sendo adotado pelo governo federal, por meio do Ministério do Planejamento, Orçamento e Gestão (MPOG), para fornecer uma solução completa de gerenciamento dos recursos computacionais da Administração Pública Federal direta, autárquica e fundacional [12]. Por ser vinculada ao Ministério da Educação, a FUNDAJ faz parte desse projeto, servindo assim de motivação para o desenvolvimento desta monografia.

O objetivo central deste trabalho é comprovar através dos resultados obtidos e analisados no estudo de caso que são vários os benefícios proporcionados pelo monitoramento de ativos de redes em uma organização.

Capítulo 2

Monitoramento de Ativos de Redes

Quando foram inventadas, as redes de computadores tinham como principal objetivo compartilhar documentos e dispositivos da rede, tais como impressoras, discos, *modems*, etc. Entretanto, ao longo do tempo e com a diminuição dos preços dos equipamentos, as redes tornaram-se parte do cotidiano dos usuários, motivando assim, o seu crescimento. Dessa forma, a complexidade das redes de computadores também aumentou, tornando necessário um gerenciamento eficaz e preciso para garantir uma qualidade de serviço.

A gerência de uma rede de computadores compreende o monitoramento de ativos de redes englobando *hardware* e *software* em um ambiente corporativo. Em locais com poucos ativos conectados, apenas uma pessoa é capaz de monitorá-los. Todavia, considerando um ambiente onde a rede está distribuída em várias salas, ou até mesmo em prédios diferentes, o monitoramento torna-se oneroso, consumindo tempo e recursos. Nas redes de longa distância, o monitoramento é mais complexo e indispensável, já que cobre uma área geográfica extensa e abrange um grande número de equipamentos e usuários dependentes de seus serviços. Hoje, graças às tecnologias existentes, é possível monitorar os ativos em uma rede como essa, mesmo que utilize plataformas diferentes e que a rede seja heterogênea [28].

O monitoramento dos ativos de redes é uma avaliação contínua das variáveis operacionais, cujo principal objetivo é detectar antecipadamente anomalias com uma baixa taxa de falsos positivos, ou seja, alarmes-falsos, garantindo assim um bom funcionamento e confiabilidade das redes de computadores monitoradas [36].

2.1 Protocolos de Monitoramento

Os protocolos de monitoramento de redes descrevem um formato para o envio de informações entre os ativos de redes monitorados e as máquinas responsáveis pelo armazenamento de tais informações.

Os protocolos permitem que dados dos ativos de rede possam ser monitorados durante o seu funcionamento sem custos excessivos. Esses dados não oferecem uma análise pronta da rede, porém, podem ser utilizados em processos que colaborem para o desenvolvimento de indicadores de performance da rede [33].

As tecnologias mais conhecidas no monitoramento de ativos de redes baseadas no modelo *Transmission Control Protocol / Internet Protocol* (TCP/IP) utilizam o protocolo de comunicação *Simple Network Management Protocol* (SNMP) e as redes baseadas no modelo *Open System Interconnections* (OSI) utilizam o protocolo *Common Management Information Protocol* (CMIP).

Entre os dois protocolos, o SNMP é o que obteve o maior sucesso, pois baseia-se no fato de ter sido o primeiro protocolo de monitoramento não proprietário, público, fácil de ser implementado e que possibilita o gerenciamento de ambientes heterogêneos. Já o protocolo CMIP, devido à sua complexidade de implementação e ao grande número de pré-requisitos para o seu funcionamento, não é um modelo tão comum quanto o baseado em TCP/IP, sendo utilizado principalmente em sistemas de telecomunicações [28].

Nesta monografia foi dada ênfase ao protocolo SNMP, uma vez que ele é o mais utilizado atualmente e também é o protocolo utilizado no estudo de caso implementando neste trabalho.

2.2 SNMP

Segundo [31], uma arquitetura de monitoramento e gerenciamento de redes no modelo TCP/IP apresenta quatro componentes: ativos de redes gerenciados (estações de trabalho, servidores, impressoras, etc), estações de monitoramento, informações de monitoramento e um protocolo de monitoramento, que como visto anteriormente, tem-se o SNMP como um dos mais utilizados atualmente. O monitoramento é realizado através de estações gerentes com um *software* especial. Estas estações possuem processos que se comunicam com os agentes emitindo comandos e obtendo respostas.

Desenvolvido para facilitar a troca de informações de monitoramento entre ativos de redes, o protocolo SNMP pertence à camada de aplicação e está especificado na *Request for Comments* (RFC 1157) [11].

O SNMP funciona baseado no conceito de agente e gerente. O agente é um programa executado na máquina monitorada e tem a função de coletar informações da respectiva máquina. O agente deve responder às requisições do gerente enviando, quando programado, as informações coletadas de forma automática. Todos os ativos de redes monitorados devem possuir um agente instalado e uma base de informações chamada *Management Information Base* (MIB), de onde serão coletados os dados [18]. Cada uma das variáveis armazenadas na MIB relaciona-se com determinada funcionalidade do ativo de rede monitorado. Dessa forma, cada tipo de ativo de rede tem o conjunto de variáveis da MIB que melhor representa seu funcionamento.

Como exibido na Figura 1, o gerente é um programa que é executado em um servidor e, mediante a comunicação com um ou mais agentes, obtêm e armazena informações de monitoramento referentes a cada um dos ativos que hospedam o agente [23]. Para obter essas informações é utilizada uma técnica chamada *pooling*, que é uma interação do tipo pergunta-resposta entre gerente e agente [28].

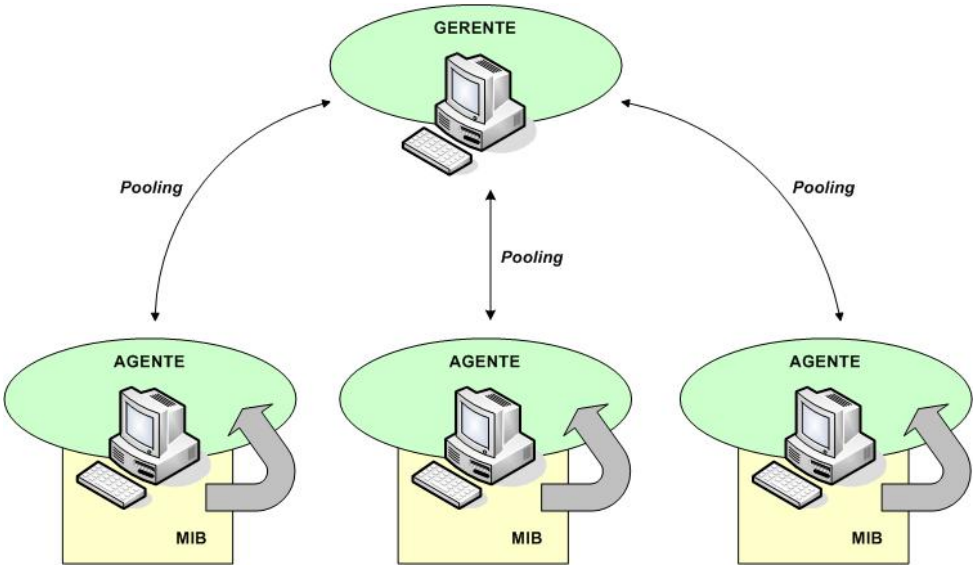


Figura 1. Funcionamento do protocolo SNMP.

Em redes extremamente grandes, a utilização do SNMP não é recomendada devido à limitação de performance do *pooling*, uma vez que a probabilidade de erros e ruídos acontecerem aumenta. Por conta disso, sugere-se que o monitoramento seja subdivido em partes menores quando um situação como esta for notada [23].

Os fabricantes de *gateways, bridges* e roteadores foram os primeiros a implantar o SNMP. Geralmente, o fabricante desenvolve o agente SNMP para em seguida desenvolver uma interface para a estação gerente da rede.

Implementações básicas do SNMP possibilitam monitorar e isolar falhas. As aplicações mais avançadas permitem gerenciar o desempenho e a configuração da rede. Estas aplicações, geralmente, incorporam alarmes e menus para facilitar a interação com o profissional que está monitorando os ativos de redes [28].

2.3 Modalidades de Monitoramento

Ao escolher uma determinada tecnologia de monitoramento de redes de computadores, uma organização pode se submeter a certas restrições que as levam a ficar dependentes da tecnologia escolhida, devido à dificuldade de troca dessa tecnologia por uma outra no futuro. A esse processo é dado o nome de aprisionamento tecnológico [4].

As dificuldades de mudança decorrem das incompatibilidades entre as tecnologias, que podem gerar altos custos. Por conta disso, as organizações que trabalham com redes de computadores devem escolher os sistemas de monitoramento já pensando em uma possível migração para outro sistema. É preciso levar em consideração quais as melhores modalidades de monitoramento que mais se adequam à necessidade da empresa.

Os sistemas de monitoramento podem ser classificados quanto à sua abrangência de gerência (local e *Web*) e quanto ao custo e restrições do *software* (proprietário e livre).

A escolha inadequada da tecnologia de monitoramento pode forçar a organização a continuar utilizando o sistema vigente, ou seja, leva a um aprisionamento aos sistemas já instalados.

2.3.1 Monitoramento Local *versus* Monitoramento *Web*

Para monitorar as redes de computadores, administradores tipicamente utilizam uma combinação de diversas ferramentas, uma vez que elas costumam apresentar tecnologias heterogêneas, ou seja, com diferentes modelos de informação, métodos de acesso e protocolos [26].

Além das ferramentas de monitoramento não serem integradas, elas comumente têm um enfoque local, sendo portanto limitadas no escopo de monitoramento, ou seja, apresentam o problema da escalabilidade, sendo adequadas para gerenciar somente ambientes de pequeno porte. Esses motivos contribuem para explicar o porquê da tarefa de monitoramento ser tão complexa.

Já com o monitoramento *Web* é possível diminuir a distância entre os dispositivos e o administrador da rede, permitindo que o gerenciamento dos ativos de redes seja realizado de qualquer lugar do mundo, sendo preciso apenas a existência de um navegador cliente, que se conecta a um servidor onde estão armazenadas todas as informações necessárias para o monitoramento.

Fazendo-se uma comparação entre os sistemas de monitoramento local e *Web* pode-se levantar alguns pontos, dentre os quais:

- O monitoramento local não consegue escalar bem para redes grandes: com o tamanho crescente da rede, a carga de processamento pode chegar a um ponto onde não seja mais possível monitorar os ativos de redes por completo. O monitoramento *Web* também apresenta certas limitações quanto à escalabilidade, mas tal problema pode ser contornado com a divisão da rede em setores independentes. Dessa forma, estes setores é que passam a ser monitorados, garantindo assim, o gerenciamento de redes extremamente grandes;

- No gerenciamento local existe a falta de flexibilidade, já que as funções de monitoramento e características dos ativos de redes são normalmente pré-definidas e limitadas. Além disso, um serviço só poderia ser testado localmente ou diretamente pelo gerente central;

- As tecnologias baseadas no monitoramento *Web* têm como principais características o fácil acesso de qualquer ponto da rede corporativa ou da *Internet* e a tendência de redução de custos, com a utilização de interfaces baseadas em navegadores *Web*;

- Outras grandes vantagens do monitoramento *Web* são o alto grau de interoperabilidade e a independência de plataforma para acessar os dados gerados pelos sistemas pertencentes a esta modalidade de monitoramento.

2.3.2 *Software* Proprietário *versus Software* Livre

Os sistemas de monitoramento de ativos de redes também podem ser divididos em *software* proprietário e *software* livre.

O *software* proprietário é regido por uma série de normas que visam limitar o seu uso ao número de licenças adquiridas e é necessário pagar por cada cópia instalada. A livre distribuição não é aceita e é considerada um ato ilícito. Também não é permitido acesso ao código-fonte, nem tão pouco alterá-lo, o que torna a personalização e, conseqüentemente, melhorias e correções no programa, impossíveis.

Já o s*oftware* livre pode ser distribuído de forma gratuita. Ele possui as premissas de liberdade de instalação; plena utilização; possibilidade de modificações e aperfeiçoamentos para necessidades específicas; distribuição da forma original ou modificada, com ou sem custos. Contrapõe-se ao modelo do *software* proprietário onde o usuário de *software* não tem permissão para redistribuí-lo nem alterar seu funcionamento para ajustar-se às suas necessidades [27].

2.4 Sistemas de Monitoramento

Diversos sistemas de monitoramento estão disponíveis no mercado atualmente. Eles podem variar entre simples executáveis e conjuntos de programas que funcionam cooperando entre si. Os sistemas de monitoramento procuram apoiar os administradores de redes através da obtenção de métricas e informações que auxiliam a tomada de decisões relacionadas à infra-estrutura de rede de forma mais eficiente.

Com o objetivo de identificar as características e aspectos importantes de algumas ferramentas de monitoramento, foram estudadas quatro delas: CACIC [6], Cacti [7], 3Com *Network Supervisor* [1] e GFI LANguard [24]. Um estudo mais aprofundado foi feito com o sistema CACIC, exposto no estudo de caso desta monografia.

A análise foi feita com base nos seguintes critérios:

- Usabilidade: facilidade de navegação na ferramenta;
- Preço: valor de uma licença anual, caso não seja gratuita;
- Plataforma: em quais o sistema pode ser executado;
- Dependência: relação com outras tecnologias;
- Idiomas: análise sobre idiomas disponíveis;
- Integração: capacidade de integrar-se com outras áreas ou ferramentas;
- Complexidade: grau de dificuldade para utilizar a ferramenta;
- Eficiência *versus* limitações: relação de pontos positivos e negativos de cada ferramenta.

A coleta das características citadas anteriormente foi de grande importância para realizar uma análise consistente entre as ferramentas estudadas. Porém, o objetivo principal desse estudo analítico é comparar alguns requisitos dos sistemas com o CACIC.

A seguir será feita uma rápida apresentação dos sistemas estudados. Nessa descrição serão expostas características gerais e principais funcionalidades.

2.4.1 Cacti

O Cacti é um sistema que recolhe e exibe informações sobre o estado dos ativos de redes de computadores através de gráficos, como mostra a Figura 2. Ele foi desenvolvido para ser flexível e para que se adapte facilmente a diversas necessidades, além de ser robusto e de fácil utilização. Sua principal função é monitorar o estado de elementos de rede e programas, bem como o uso de CPU e largura de banda [8].

O sistema tem uma interface e infra-estrutura voltada para o RRDTool[1] e as informações são repassadas para a ferramenta através do protocolo SNMP. Para ser instalado, o sistema necessita do conjunto de programas conhecido como LAMP[2]. O Cacti se encaixa nas modalidades de monitoramento *Web* e *software* livre.

É possível expandir a arquitetura do Cacti através de *plugins* que adicionam novas funcionalidades. Como exemplo, pode-se citar o PHP *Network Weathermap*, que mostra um mapa da rede e o estado de cada elemento.

---

[1] Programa desenvolvido por Tobi Oeticker, criador do famoso sistema de monitoramento *Multi Router Traffic Grapher (*MRTG). O *Round Robin Database Tool* (RRDTool) tem a função de guardar dados coletados em arquivos ".rrd". O número de registros nestes arquivos nunca aumenta, significando que registros antigos são freqüentemente removidos. Isto implica em uma obtenção de figuras precisas para dados recentemente inseridos. É possível obter gráficos diários, semanais, mensais e anuais [7].

[2] Acrônimo para a combinação das tecnologias Linux, Apache, MySQL e PHP.

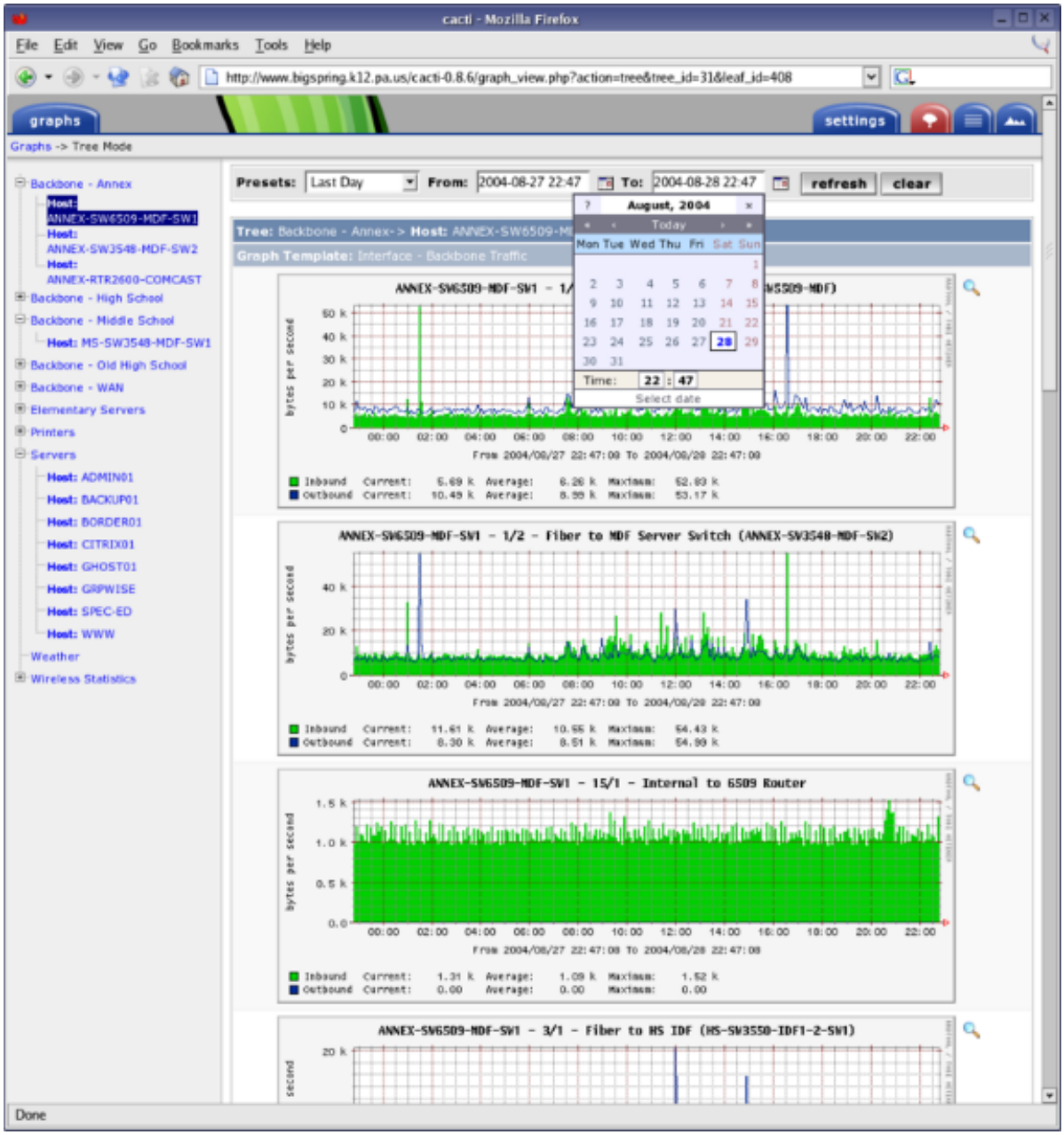


Figura 2. Tela inicial do sistema Cacti.

2.4.2 3Com *Network Supervisor*

o 3Com *Network Supervisor* é um sistema de monitoramento pertencente às modalidades de monitoramento local e *software* proprietário. É de fácil utilização e exibe seus resultados através de gráficos, mapas e displays dos *links* e ativos de redes, como exibido na Figura 3.

O sistema é capaz de mapear dispositivos e conexões de forma que o administrador possa monitorar o nível de sobrecarga, configurar portas e alertas,

enxergar todos os eventos da rede, gerar relatórios em formatos definidos pelo usuário e executar programas de configuração de ativos. Além disso, ele é capaz de detectar configurações errôneas na rede e oferecer sugestões de otimização [1].

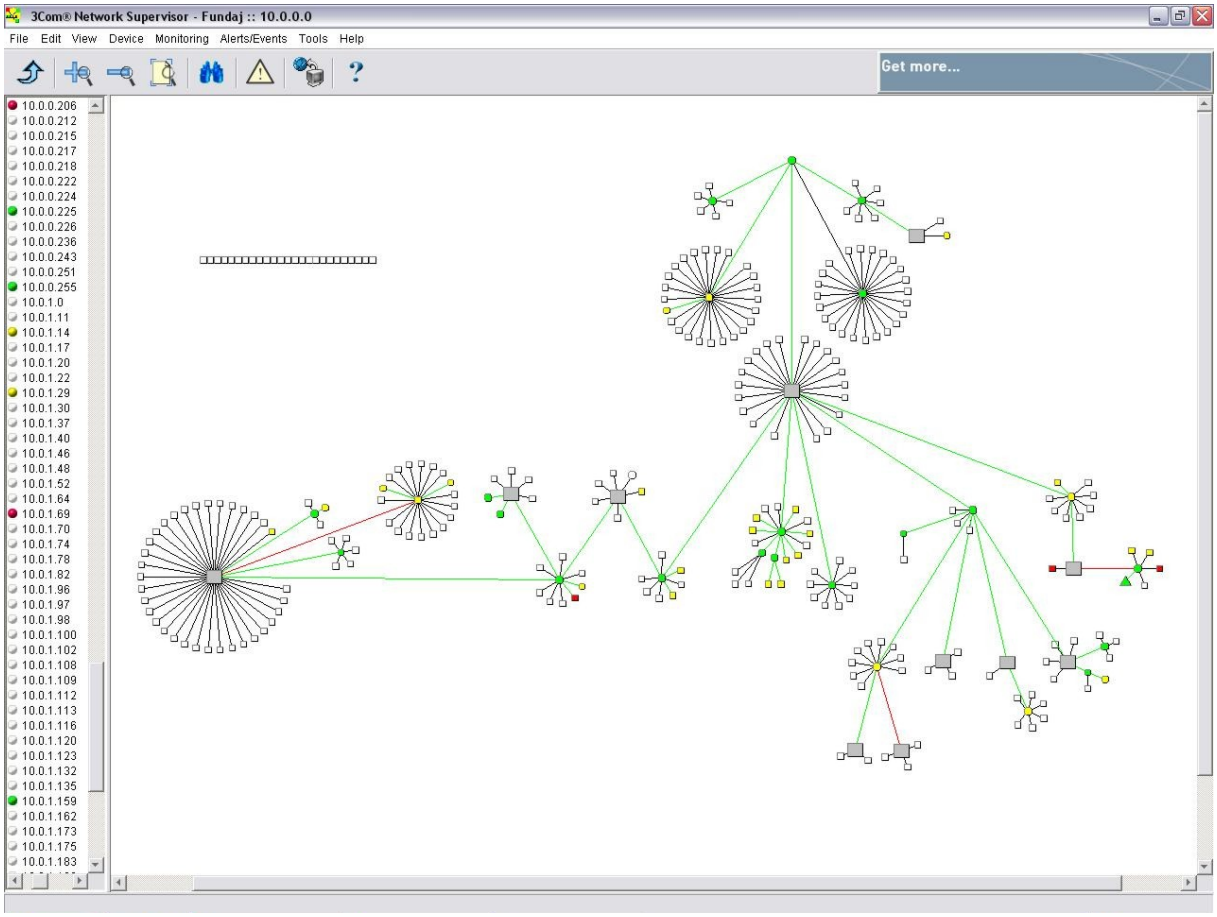


Figura 3. Console do 3Com *Network Supervisor*.

Um ponto fraco do sistema é que ele tem uma limitação de 1500 ativos de redes possíveis de serem monitorados e funcionam de forma limitada com ativos de redes que não sejam da mesma marca do produto, 3Com.

Apesar de ser um sistema de monitoramento local, ele consegue enviar mensagens de alertas via SMS[3] aos administradores para que eles se mantenham

[3] Do inglês *Short Message Service*. Tecnologia bastante utilizada em telefonia celular para enviar mensagens de até 160 caracteres alfanuméricos [9].

permanentemente em contato com sua rede. Além disso, também consegue se comunicar com outros sistemas de monitoramento, como o HP *OpenView*, por exemplo.

2.4.3 GFI LANguard

O GFI LANguard pertence às modalidades de monitoramento local e *software* proprietário. Ele é uma solução que permite ao administrador de um parque computacional identificar, avaliar e corrigir eventuais vulnerabilidades de segurança na rede através do monitoramento de seus ativos, como mostra a Figura 4.

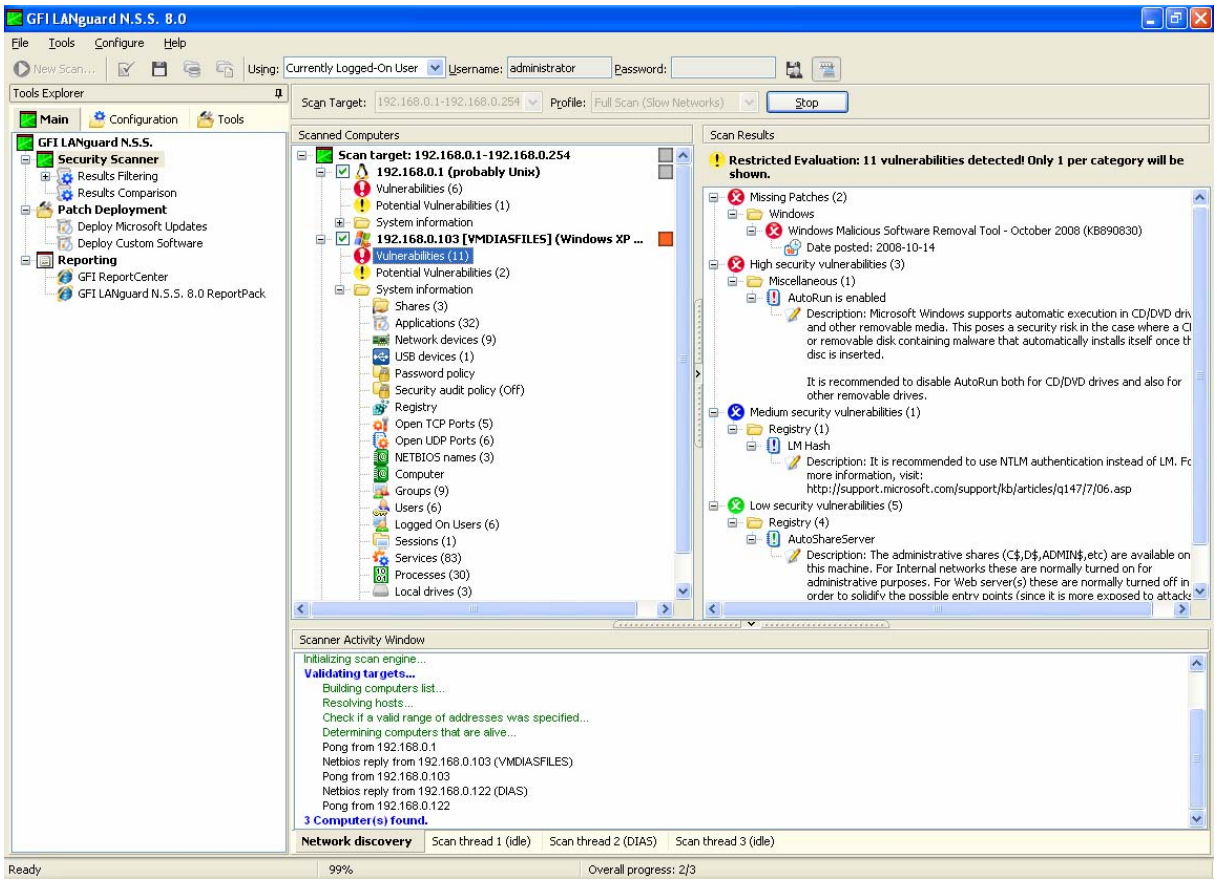


Figura 4. Console de monitoramento do GFI LANguard.

No dia-a-dia, o administrador freqüentemente tem que tratar separadamente os problemas relacionados a questões de vulnerabilidade e auditoria da rede, utilizando, muitas vezes, vários produtos. Entretanto, o GFI LANguard oferece a gestão desses problemas em um único pacote. Através de um console é possível resolver essas questões de uma forma eficaz e rápida. Mais de 15000 tipos de

avaliações de vulnerabilidade estão disponíveis no programa, garantindo assim, que os sistemas e redes monitorados fiquem salvaguardados de ataques de *hackers* e violações de segurança [24].

2.4.4 Comparação Analítica entre os Sistemas de Monitoramento

Após analisar as principais características baseadas nos critérios anteriormente citados, uma comparação analítica do sistema CACIC com os outros três sistemas foi elaborada. O resultado está exposto na Tabela 1.

Tabela 1. Quadro comparativo entre os sistemas analisados.

Sistemas / **Características**	**CACIC**	**Cacti**	**3Com *Network Supervisor***	**GFI LANguard**
Usabilidade	Ótima	Boa	Boa	Ótima
Preço	Grátis	Grátis	$ 49,95	$ 62,25
Plataforma	Microsoft *Windows* / Linux	Microsoft *Windows* / Linux	Microsoft *Windows*	Microsoft *Windows*
Dependência	Apache, MySQL, PHP	Apache, MySQL, PHP	Não existe	Não existe
Idioma	Português	Inglês	Inglês	Inglês
Integração	Sim	Sim	Sim	Não
Complexidade	Baixa	Razoável	Razoável	Baixa
Modalidades	Monitoramento *Web* / *software* livre	Monitoramento *Web* / *software* livre	Monitoramento local / *software* proprietário	Monitoramento local / *software* proprietário

Eficiência *versus* Limitações	Diagnóstico detalhado dos ativos de redes *versus* dependência de outras tecnologias	Resultados exibidos em gráficos *versus* dependência de outras tecnologias	Topologia da rede exibida em mapas *versus* análise demorada	Análise de vulnerabilidades *versus* aprisionamento tecnológico

As características usabilidade, complexidade e eficiência *versus* limitações foram avaliadas com base na utilização das ferramentas no período de desenvolvimento desta monografia, e foram escolhidas de acordo com a opinião pessoal do autor deste trabalho.

Observa-se que o sistema CACIC apresenta o melhor conjunto de resultados dos critérios analisados, enquanto os demais sistemas deixaram a desejar em alguns pontos. Os diferenciais encontram-se no preço, integração, complexidade e modalidades.

Entretanto, todas as ferramentas analisadas pregam que as atividades de monitoramento devem ser executadas de forma contínua, garantindo a análise dos ativos de redes de forma mais eficaz.

Capítulo 3

Estudo de Caso

Para comprovar de forma mais eficiente a importância do monitoramento de ativos de redes, foi realizado um estudo de caso, onde o sistema CACIC foi implantando na FUNDAJ, sendo esta a parte prática da monografia.

3.1 O CACIC

O CACIC é um sistema capaz de fornecer um diagnóstico preciso do parque computacional de qualquer empresa de grande porte, disponibilizando informações centralizadas, ou seja, em um mesmo ambiente de monitoramento, como o número de equipamentos e suas distribuições, configurações de *hardware*, *software* e rede, atualizações de segurança, variáveis de ambiente, uso do disco, impressoras e pastas compartilhadas. Também pode fornecer informações patrimoniais e a localização física dos equipamentos, ampliando assim o controle da rede. Todas essas informações são disponibilizadas para o administrador em uma página *Web* [12].

Resultado de um Consórcio de Cooperação entre a Secretaria de Logística e Tecnologia da Informação (SLTI) do Ministério do Planejamento, Orçamento e Gestão (MPOG) e a Empresa de Tecnologia e Informações da Previdência Social (DATAPREV), desenvolvido pelo Escritório Regional da DATAPREV no Espírito Santo, o CACIC é o primeiro *software* público do Governo Federal sob a licença GPL (*General Public License*). Isto significa que é possível usá-lo de forma livre, sem gastos com licenças e tendo acesso irrestrito ao código fonte [6].

Atualmente o sistema encontra-se na versão 2.4 beta, sendo que no estudo de caso desenvolvido nessa monografia foi utilizada a versão 2.2.2. Por ser um sistema de código aberto, ele está em constante atualização.

3.1.1 Funcionalidades

Segundo [12], o CACIC possui as seguintes funcionalidades:

- Exibição de informações detalhadas sobre os componentes de *hardware* instalados em cada ativo de rede;
- Exibição de informações sobre os *softwares* instalados em cada servidor e estação de trabalho;
- Exibição de informações sobre o patrimônio (número de termo e localização física) de cada ativo de rede;
- Exibição de informações diversas sobre configuração de rede, variáveis de ambiente, uso do disco e pastas compartilhadas;
- Exibição de informações diversas sobre atualização de segurança das estações de trabalho, permitindo assim uma atuação pró-ativa dos administradores de Tecnologia da Informação (TI).

Além dos resultados acima, através do CACIC, as seguintes operações também podem ser obtidas:

- Envio de alertas aos administradores cadastrados em caso de detecção de alteração de *hardware* e de localização física;
- Disponibilização centralizada sobre a distribuição das estações de trabalho por entidade, órgão, sub-orgão, rede, sub-rede, domínio, sistema operacional, endereço IP (*Internet Protocol*), endereço MAC (*Media Access Control*) e nome;
- Recuperação de informações sobre a localização física dos ativos de rede por patrimônio, número de série, entidade, órgão e sub-orgão.

3.1.2 Arquitetura

A arquitetura do CACIC é estruturada em dois módulos: módulo gerente e módulo agente, como mostra a Figura 5. Em algumas implementações do sistema pode existir ainda um terceiro módulo, que é responsável por administrar vários módulos gerentes. A este outro módulo é dado o nome de super-gerente. Para o nosso estudo de caso ele não foi necessário [13].

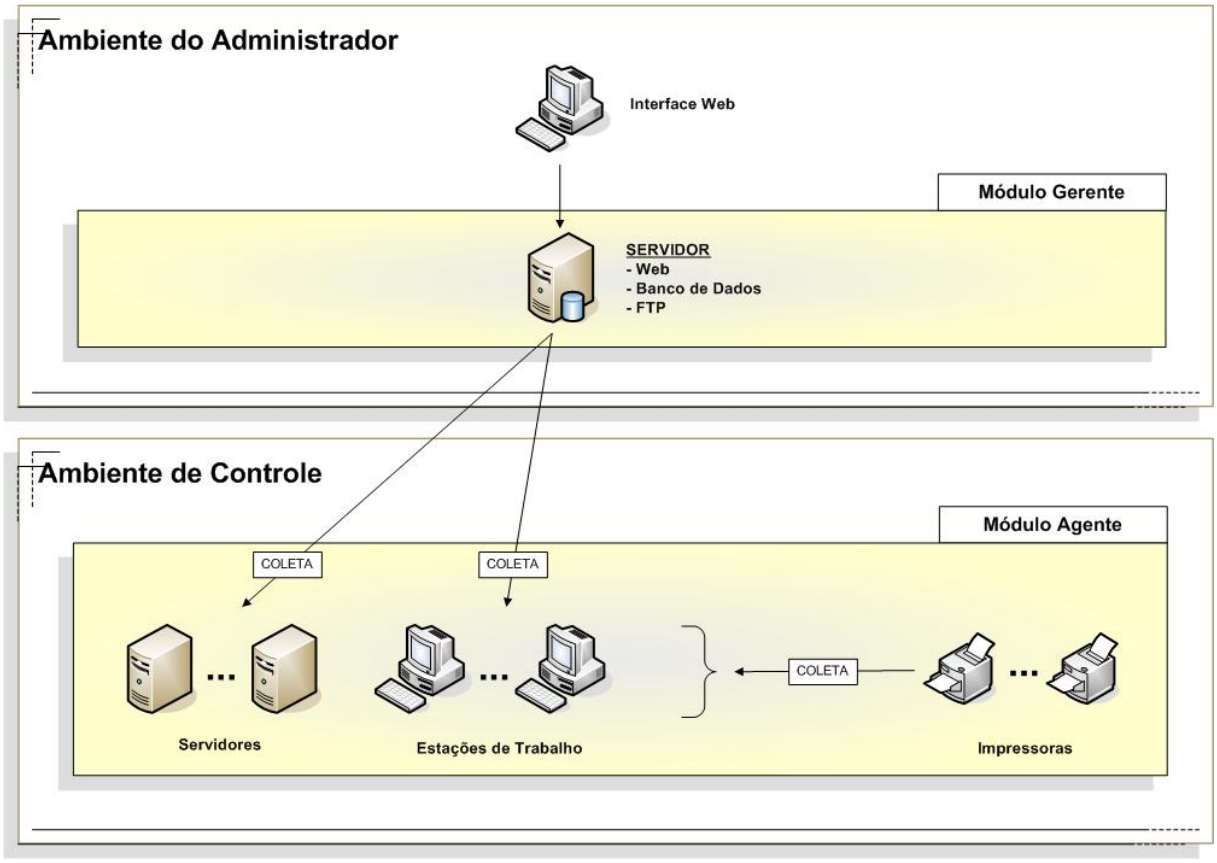


Figura 5. Arquitetura de alto nível do CACIC.

O módulo gerente tem uma função de administração no sistema. Já o módulo agente é responsável pelo controle do CACIC.

3.1.2.1 Módulo Gerente

O módulo gerente é constituído por algumas tecnologias que são instaladas em um servidor *Web* e que devem trabalhar integradas com o objetivo de administrar os módulos agentes que estão instalados nas estações de trabalho e servidores que são monitorados. As tecnologias que compõe este módulo são as seguintes: banco de dados MySQL, servidor FTP ProFTPd, servidor *Web* Apache e linguagem de programação PHP. A Figura 6 mostra a arquitetura de baixo nível do CACIC, onde é possível verificar como o módulo gerente atua no sistema [14].

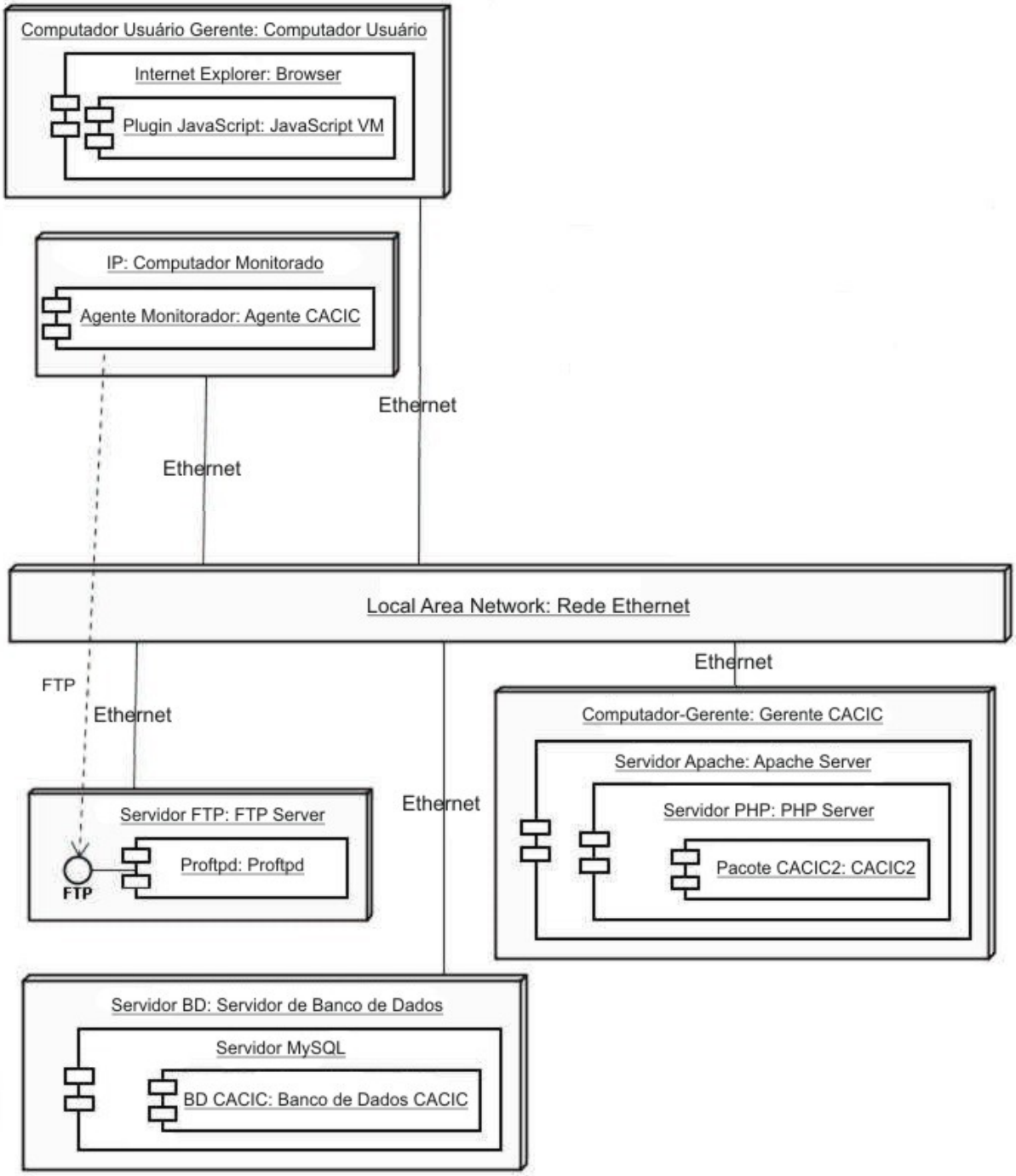


Figura 6. Arquitetura de baixo nível do CACIC.

Os dados coletados pelos agentes são enviados para o módulo gerente, onde são organizados, tratados, armazenados e disponibilizados em forma de relatórios e consultas através de uma interface *Web*. O módulo gerente também é responsável pela configuração de algumas características de comportamento dos módulos agentes. Algumas delas serão descritas nas próximas seções [3].

3.1.2.2 Módulo Agente

Segundo [13], o módulo agente é composto por um pequeno programa compilado que fica em constante operação na estação de trabalho ou servidor que está sendo monitorado. Esse programa é o responsável por coletar os dados de *hardware*, *software* e rede, mantendo o gerente sempre atualizado em relação às informações dos ativos de redes. As coletas são feitas com uma freqüência definida pelo administrador, podendo variar de 2 a 10 horas de intervalo entre elas. Ao final de cada coleta, os dados são enviados para o módulo gerente, como mostra a Figura 5. Ao coletar os dados, o programa compara os dados obtidos com as informações da coleta anterior. Para otimizar o serviço, ele repassa ao gerente apenas os dados que sofreram modificações, evitando assim, sobrecarga na rede. Caso as modificações estejam relacionadas a *hardware* ou patrimônio, informações estas que geralmente se mantêm constantes, o agente envia um alerta para que o módulo gerente notifique por *e-mail* o administrador da rede.

Em relação às impressoras, os dados provenientes delas são repassados para o módulo gerente através do ativo ao qual ela está conectada, ou seja, uma estação de trabalho ou servidor [5].

3.1.3 Requisitos Mínimos de *Hardware* e *Software*

De acordo com [14], para a implantação do módulo gerente são necessários os seguintes requisitos mínimos de *hardware* e *software*:

REQUISITOS MÍNIMOS DE *HARDWARE*:

- Computador Pentium/AMD 500 MHz;
- 128 MB de memória RAM (*Random Acess Memory*);
- 50 MB de espaço disponível em disco rígido;
- Interface de rede.

REQUISITOS MÍNIMOS DE *SOFTWARE*:

- Sistema Operacional LINUX;
- Servidor *Web* Apache-1.3.22;
- Interpretador PHP4;
- Servidor de banco de dados MySQL-4;
- Gerenciador de banco de dados MySQL phpMyAdmin-2.3.3;
- Servidor de *e-mail* MTA Postfix ou *Sendmail*;
- Pacotes de instalação do CACIC.

Para a implantação do módulo agente são necessários os seguintes requisitos mínimos:

REQUISITOS MÍNIMOS DE *HARDWARE*:

- 32 MB de memória RAM;
- 2.5 MB de espaço disponível em disco rígido;
- Interface de rede.

REQUISITOS MÍNIMOS DE *SOFTWARE*

- Sistema Operacional *Windows* 95.

3.1.4 Tecnologias Utilizadas

Neste estudo de caso foram utilizadas diversas tecnologias. O módulo gerente concentrou a maioria delas e portanto merece uma maior atenção. São elas: banco de dados MySQL, servidor FTP ProFTPd, servidor *Web* Apache e linguagem de programação PHP. Nas próximas sub-seções serão detalhadas cada uma delas.

Já no módulo agente, por ser mais simples, foi utilizada apenas uma única tecnologia: a linguagem de programação *Object* Pascal usando Delphi, necessária para o desenvolvimento do conjunto de aplicativos responsável pela coleta e envio dos dados para o módulo gerente. Por não ter sido necessário implementar, nem configurar o conjunto de aplicativos deste módulo, não será feito aqui o seu detalhamento.

Na versão 2.2.2 do CACIC, que foi utilizada neste estudo de caso, o módulo gerente funciona exclusivamente na plataforma Linux. Não existe previsão para o lançamento de uma nova versão que trabalhe com qualquer outra plataforma.

Entretanto, os aplicativos do módulo agente, que na versão 2.2.2 estão disponíveis apenas para a plataforma *Windows*, a partir da versão 2.4 já podem ser executados na plataforma Linux.

3.1.4.1 Banco de Dados MySQL

Um banco de dados é um local onde é possível armazenar informações para uma posterior consulta, quando necessário. Os dados são mantidos e acessados através de um *software* conhecido como Sistema Gerenciador de Banco de Dados (SGBD). Podemos utilizar o termo 'banco de dados' como um sinônimo de SGDB [16].

O MySQL é um dos SGBD's mais populares do mundo. Seu principal foco são as aplicações *Web*, e por conta disto ele é amplamente utilizado na *Internet*. É comum encontrar serviços de hospedagem de *sites* oferecendo o MySQL juntamente com suporte à linguagem PHP, uma vez que ambos trabalham muito bem em conjunto. Um outro fator relevante do seu sucesso é que sua disponibilidade é para praticamente qualquer sistema operacional, como Linux, FreeBSD, *Windows* e Mac OS X. Além disso, o MySQL é um *software* livre (sob licença GPL), podendo assim ser estudado e alterado conforme a necessidade do usuário [17].

O CACIC adota o MySQL como o seu banco de dados pelo fato dele ser compatível com a linguagem PHP, possuir uma baixa exigência de processamento e oferecer uma conectividade segura.

É no MySQL que todos os dados referentes aos ativos de redes e que são obtidos pelos agentes do CACIC ficam armazenados para uma posterior consulta dos administradores da rede.

3.1.4.2 Servidor FTP ProFTPd

O *File Transfer Protocol* (FTP) é um protocolo utilizado para transferir arquivos de uma máquina para outra em uma rede de computadores. Já o servidor FTP é um *software* desenvolvido para gerenciar o FTP.

O servidor FTP pode fornecer um serviço de acesso de usuários a um disco rígido de qualquer computador em uma rede. Seu acesso pode ser privado ou anônimo. No primeiro caso, apenas usuários autenticados do sistema conseguem conectar-se ao servidor a acessar seus arquivos. No segundo modo, qualquer pessoa pode realizar a conexão de forma anônima, ou seja, sem a necessidade de uma conta de usuário [21].

O ProFTPd é o servidor FTP utilizado no CACIC. Ele tem as características de ser simples e facilmente configurável. Foi desenvolvido inicialmente para trabalhar com o servidor *Web* Apache, porém hoje também trabalha com outras tecnologias. O ProFTPd é gratuito e funciona exclusivamente no Linux [32].

No CACIC o ProFTPd é responsável pelo acesso aos arquivos de instalação e também pela atualização dos agentes já instalados nos ativos de redes que são monitorados.

3.1.4.3 Servidor Web Apache

Segundo [2], um servidor *Web* é um programa que recebe pedidos HTTP (*Hypertext Transfer Protocol*), o protocolo padrão da *Web*, de clientes e envia uma resposta com o conteúdo correspondente ao pedido efetuado. Ao utilizarmos um navegador *Web*, é justamente isto que ocorre.

As páginas que encontram-se na Internet, seguem o padrão *Hypertext Markup Language* (HTML), que permite a formatação de documentos e a incorporação de *hyperlinks* com outros documentos armazenados no mesmo computador ou até mesmo em outros computadores remotos. O servidor *Web* é um dos responsáveis pela disponibilização desses documentos na *Internet*.

O Apache é o servidor *Web* utilizado no CACIC. Ele é altamente confiável, configurável, extensível e compatível com diversas tecnologias de conteúdo dinâmico, como a linguagem de programação PHP, por exemplo. Também está disponível para vários sistemas operacionais (Unix, Linux, *Windows*, Netware, entre outros). Além disso, ele é gratuito, até mesmo para uso comercial [34].

De acordo com um levantamento feito pela Netcraft e disponível em [35], mais de 60% dos servidores *Web* ativos na Internet executavam seus sites no Apache em janeiro de 2006. Esta liderança no mercado já dura mais de 10 anos.

No CACIC, o Apache é responsável por tornar disponíveis as páginas *Web* aos administradores da rede. As páginas mostram todos os resultados obtidos no monitoramento dos ativos de redes. Também é nelas que a configuração inicial do módulo gerente é realizada.

3.1.4.4 Linguagem PHP

O PHP (*Hypertext Preprocessor*) é uma linguagem de programação interpretada, livre e bastante utilizada para gerar conteúdo dinâmico na *Web*. Ela é uma linguagem extremamente modularizada, o que a torna ideal para instalação e uso em servidores *Web*. Outra grande vantagem é que por ser executada no lado do servidor, seu código fonte não é exibido ao usuário, que terá acesso apenas ao conteúdo HTML [22].

Além disso, o PHP trabalha com diversos SGBD's, como o MySQL, o Firebird, PostgreSQL, Microsoft SQL Server e Oracle. Com os sistemas operacionais não é diferente; ela opera facilmente na grande maioria deles [25]. Dentre outros motivos, o PHP é a linguagem de programação utilizada pelo CACIC devido ao fato de ser uma linguagem de código aberto e, conseqüentemente, gratuita, por ser eficiente, uma vez que consome poucos recursos do servidor, e por ter um ótimo relacionamento com o MySQL, o SGBD utilizado pelo CACIC.

3.2 A FUNDAJ

A FUNDAJ teve seu inicio no ano de 1948, quando o então deputado federal Gilberto Freyre defendeu a criação de um instituto de pesquisas sociais com o nome de Joaquim Nabuco, homenageando o abolicionista pernambucano.

Em 1º de janeiro de 1949 o Diário de Pernambuco publicou uma matéria expressando um voto de confiança ao instituto que estava prestes a nascer. Naquele mesmo ano, um chalé, datado do ano de 1870, foi alugado na Av. Rui Barbosa, cidade de Recife, onde foi instalada a biblioteca do Instituto Joaquim Nabuco. Alguns pesquisadores foram convidados a compor o que viria a ser, mais tarde, as seções cientificas do Nabuco.

Em 1952, através de uma ação conjunta do sociólogo Gilberto Freyre e do diretor Paulo Maciel, sua sede própria foi inaugurada, que até hoje encontra-se na Av. 17 de Agosto, também na cidade de Recife.

No ano de 1979, o instituto passou à categoria de fundação pública, sendo vinculada então ao Ministério da Educação.

A FUNDAJ tem como missão promover atividades cientificas e culturais; realizar estudos e pesquisas no campo social; preservar e difundir bens patrimoniais representativos da realidade histórica, social e cultural brasileira; e discutir e promover a produção cultural contemporânea, visando dar suporte aos criadores e possibilitar o acesso desse conteúdo à sociedade, prioritariamente a do Norte e do Nordeste do país.

3.2.1 Análise da Infra-estrutura de Rede

Do ponto de vista tecnológico a FUNDAJ conta hoje com um parque computacional de médio porte. A instituição possui 20 servidores, cerca de 350 estações de trabalho e 20 impressoras de rede. Estes ativos de redes estão distribuídos na sede da instituição e em duas filiais, como mostra a Figura 7. A separação física dos dispositivos não interfere no controle do CACIC, uma vez que toda a implantação e o monitoramento são feitos via interface *Web*.

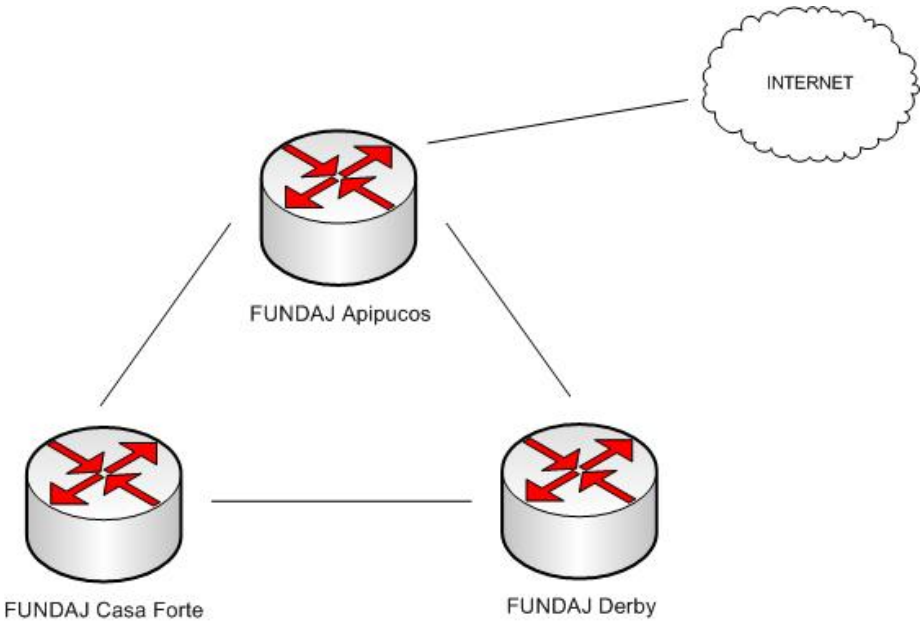


Figura 7. Topologia de rede da FUNDAJ.

3.3 Implantação

O CACIC foi implantando no parque computacional da FUNDAJ tendo como meta o melhoramento do controle dos ativos de redes da instituição. Todo o processo de implantação, da obtenção do sistema à coleta dos primeiros dados, foi realizado em um período de 2 meses.

A implantação do sistema foi motivada pelos diversos requisitos que o *software* oferece tecnicamente, além de ser um *software* livre que não acarreta custos com licenças para a fundação.

3.3.1 Obtenção do CACIC

Para obter o CACIC, é preciso efetuar um cadastro no site do Portal do *Software* Público Brasileiro (SPB), que pode ser acessado pelo endereço www.softwarepublico.gov.br. O SPB é mantido pelo governo federal e define a política de uso e desenvolvimento de *software* pelo setor público no Brasil. Seu objetivo é compartilhar soluções entre as instituições públicas, em particular as instituições de informática. O CACIC foi a primeira ferramenta a ser compartilhada gratuitamente no portal, podendo assim ser distribuída para toda a sociedade [29].

Com a iniciativa do SPB, a implantação de novas ferramentas nos diversos setores da administração pública ficou mais fácil. Através do portal é possível promover a integração entre os estados brasileiros e oferecer um conjunto de serviços públicos entre eles. As ferramentas podem ser acessadas não somente pelas instituições públicas, mas também por qualquer pessoa que tenha interesse em *softwares* livres [29].

Após a realização do cadastro, é possível acessar toda a documentação e realizar o *download* dos pacotes de instalação do CACIC. A comunidade formada pelos criadores e usuários do sistema fornecem suporte ao público em geral através de *e-mail*, fóruns de discussão e tutoriais. Todas estas ferramentas estão disponíveis no portal.

3.3.2 Instalação do Módulo Gerente

Para a instalação do Módulo Gerente foi utilizada uma máquina virtual através do programa VMware. Na virtualização foi criado um computador com as seguintes configurações: 128 MB de memória RAM e HD (*Hard Disk*) de 4 GB. O sistema operacional Linux (distribuição Debian) foi adotado, como recomenda a documentação oficial. A máquina física onde foi hospedada a máquina virtual apresentava as seguintes configurações: Pentium IV 2.4 GHz com 1 GB de memória RAM e HD de 40 GB. Nela estava instalado o sistema operacional *Windows* 2003 *Server – Enterprise Edition.*

A máquina virtual ficou responsável pelo armazenamento das informações coletadas e enviadas pelos agentes instalados nos ativos de redes. A instalação do Módulo Gerente englobou a instalação do banco de dados, do servidor FTP e do servidor *Web* com suporte a PHP. O Apêndice A mostra todo o *script* de instalação do módulo gerente.

3.3.2.1 Banco de Dados

O banco de dados MySQL (versão 5.0) foi instalado utilizando o comando apt-get do Linux, como mostra a Listagem 1. O apt-get trata-se de uma interface simples

de linha de comando capaz de realizar o *download* de pacotes diversos de repositórios na *Internet* e instalá-los.

Listagem 1. Comando para instalar o MySQL.

```
#apt-get install mysql-server-5.0
```

Após a instalação do banco de dados, foi necessário atribuir uma senha de *root* ao servidor para que o acesso ao SGBD pudesse ser controlado. A forma como a senha foi atribuída está exposta na Listagem 2.

Listagem 2. Atribuição de senha para o usuário *root* do MySQL.

```
#/usr/bin/mysqladmin –u root password ‘senha’
```

O MySQL é utilizado para armazenar a base de dados do servidor gerente, que é o responsável pela administração dos agentes. A criação da base de dados foi feita posteriormente, no momento da configuração do Módulo Gerente, que será detalhada mais à frente.

3.3.2.2 Servidor FTP

Necessário para prover acesso aos arquivos de instalação e atualização dos agentes já instalados nos computadores que são monitorados pelo CACIC, o servidor FTP ProFTPd (versão 1.2.9) foi instalado através do comando exibido na Listagem 3.

Listagem 3. Comando para instalar o servidor FTP ProFTPd.

```
#apt-get install proftpd
```

Depois de instalado, algumas configurações precisaram ser ajustadas no ProFTPd por medida de segurança. Como mostra a Listagem 4, o arquivo

proftpd.conf, responsável por armazenar as configurações de FTP, foi acessado para transformar o diretório *home* do usuário no diretório raiz do servidor FTP. Esta transformação foi possível através da inserção da linha de comando exibida na Listagem 5.

Listagem 4. Comando para acessar o arquivo de configuração do ProFTPd.

```
#vi /etc/proftpd/proftpd.conf
```

Listagem 5. Linha de comando que transforma o diretório *home* do usuário em um diretório raiz do servidor FTP.

```
DefaultRoot~
```

Ainda no arquivo proftpd.conf, também foi necessário inserir a linha de comando exibida na Listagem 6. Ela permite que o usuário utilizado pelo CACIC para baixar os pacotes via FTP não possua um *shell* válido no sistema operacional.

Listagem 6. Linha de comando que permite o usuário do CACIC não ter um *shell* válido no sistema operacional.

```
RequireValidShell off
```

Após a configuração, um usuário, que é utilizado pelo CACIC, foi adicionado para que ele pudesse fazer os *downloads* de *updates* dos agentes. A linha de comando responsável por esta operação está exibida na Listagem 7.

Listagem 7. Criação de usuário com acesso a uma pasta do servidor FTP.

```
#adduser –shell /bin/false –home /var/www/ftpcacic ftpcacic
```

Por fim, um diretório chamado ‘agentes’ foi criado dentro do diretório ‘ftpcacic’. Ele é utilizado para armazenar os arquivos executáveis do agente, como mostra o

primeiro comando exibido na Listagem 8. O comando seguinte dá permissão ao usuário ‘ftpcacic’ para que ele acesse o diretório ‘agentes’.

Listagem 8. Comando para criar diretório de FTP e atribuição de permissão a um determinado usuário.

```
#mkdir /var/www/ftpcacic/agentes

#chown ftpcacic.ftpcacic /var/www/ftpcacic/agentes
```

3.3.2.3 Servidor Web com Suporte a PHP

O servidor *Web* é um dos serviços mais importantes para que o Módulo Gerente funcione corretamente. O CACIC utiliza o servidor Apache, que tem suporte à linguagem de programação PHP. Na implantação realizada na FUNDAJ foi utilizada a versão 2.0 do Apache e a versão 5.0 do PHP. A instalação do Apache, bem como do PHP e suas extensões também foi realizada através do comando apt-get, como mostra a Listagem 9.

Listagem 9. Comando para instalar o Apache, o PHP e suas extensões.

```
#apt-get install apache2 php5-dev php5 php5-mysql php5-gd
php5-mcrypt libapache2-mod-php5
```

Após a instalação do Apache e do PHP, algumas configurações precisaram ser alteradas. No Apache foi preciso definir qual o tipo padrão dos caracteres utilizados nas páginas *Web*. Para acessar o arquivo que continha tal configuração, foi utilizado o comando exibido na Listagem 10. Ao acessar o arquivo, bastou apenas descomentar a linha onde estava o tipo padrão utilizado, que estava sendo representado por “AddDefaultCharset ISO-8859-1”.

Listagem 10. Comando para acessar o arquivo de configuração do Apache.

```
#vi /etc/apache2/apache2.conf
```

Já no PHP, foi necessário acessar o arquivo php.ini, como mostra a Listagem 11, para que as configurações exibidas na Listagem 12 pudessem ser alteradas. Estas configurações são referentes a tratamento de erros e definição das extensões utilizadas.

Listagem 11. Comando para acessar o arquivo php.ini.

```
#vi /etc/php5/apache2/php.ini
```

Listagem 12. Configurações alteradas no php.ini.

```
register_globals = On

register_long_arrays = On

error_reporting = E_COMPILE_ERROR | E_ERROR | E_CORE_ERROR

extension=mysql.so

extension=gd.so

extension=mcrypty.so
```

3.3.3 Configuração do Módulo Gerente

Após a instalação e configuração das tecnologias necessárias para o funcionamento do CACIC, foi preciso configurar algumas variáveis do módulo gerente. Essa operação foi realizada através de uma interface *Web*, sendo acessada de uma outra estação de trabalho via rede local.

Para ter acesso a essa interface, um arquivo compactado intitulado cacic2-v222-final.tar.gz foi obtido via *download* diretamente do site do *Software* Público para o servidor que armazenava o módulo gerente, como mostra a Listagem 13.

Listagem 13. Comando para realizar o download dos arquivos da interface *Web.*

```
#wget http://www.softwarepublico.gov.br/dotlrn/clubs/cacic/
file-storage/download/cacic2-v222-final.tar.gz?file%5fid
=186097
```

Em seguida, o arquivo foi descompactado no diretório raiz do servidor *Web*, como mostra a Listagem 14. As propriedades de permissões para o usuário padrão do Apache tiveram que ser alteradas, como exibido na Listagem 15. A partir desse ponto, já era possível acessar a interface *Web* do CACIC de qualquer local da rede da FUNDAJ.

Listagem 14. Comando para descompactar o arquivo cacic2-v222-final.tar.gz.

```
#tar -zxvf cacic2-v222-final.tar.gz –C /var/www
```

Listagem 15. Comando de permissão de acesso ao usuário www-data do Apache.

```
#chown -R www-data /var/www/cacic2
```

3.3.3.1 A Interface Web

A interface *Web* foi desenvolvida com a linguagem de programação PHP. Depois de descompactados, os arquivos ficam em uma pasta chamada cacic2. Para ter acesso às configurações do módulo gerente, o administrador deve acessar o endereço http://ipdoservidor/cacic2/instalador.

Como mostra a Figura 8, a tela inicial de configurações do CACIC faz uma verificação dos requisitos mínimos: PHP (versão 4.2), MySQL (versão 4.1), suporte à criptografia com a biblioteca MCrypt, suporte a imagens com a biblioteca GD (Graphics Draw) e permissão de gravação no arquivo config.php.

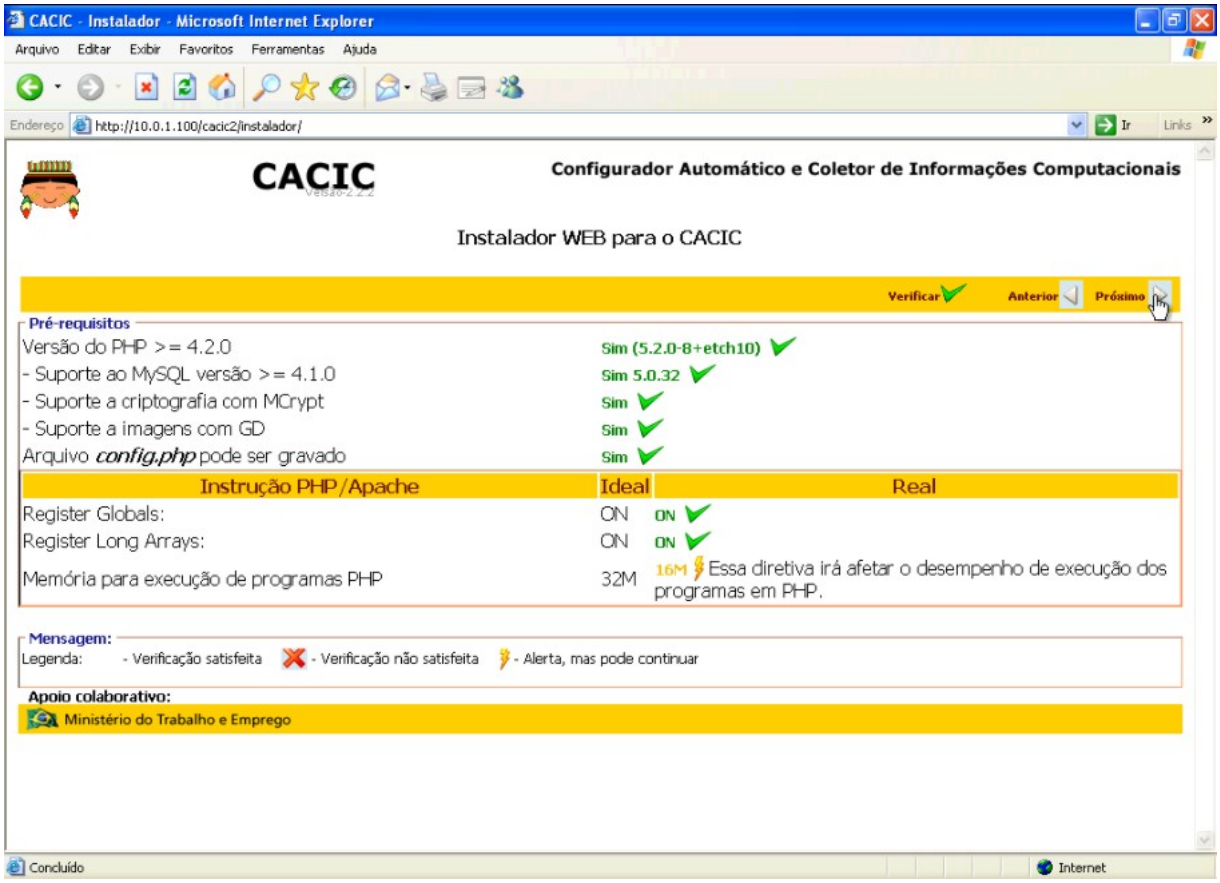


Figura 8. Tela inicial de configurações do CACIC.

Ao avançar nas configurações, o administrador tem acesso à tela responsável pela criação das tabelas do banco de dados onde ficam armazenados os dados sobre os ativos de redes monitorados. Para isso, o administrador deve inserir algumas informações importantes, como: nome do servidor, porta de conexão, nome do banco, nome do usuário e sua respectiva senha. A Figura 9 mostra como é essa tela.

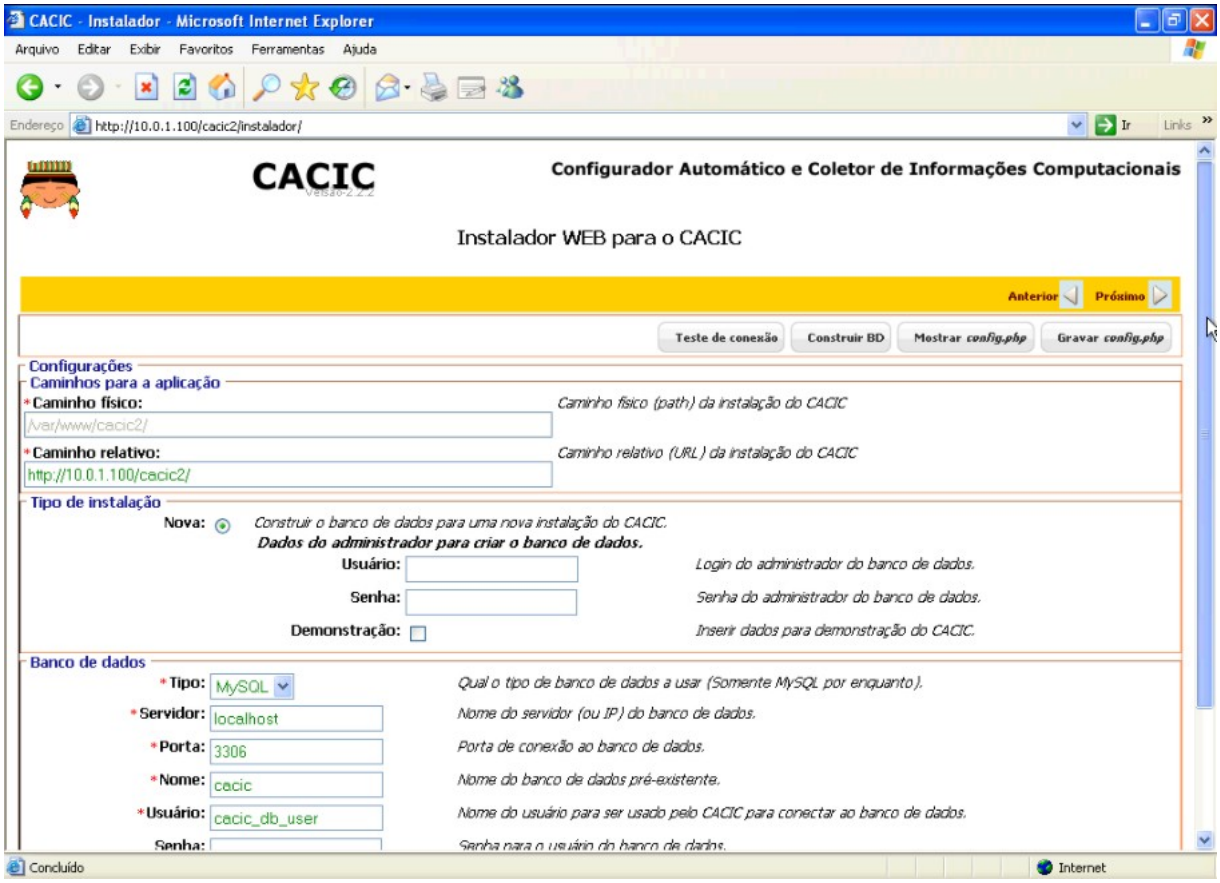


Figura 9. Tela de configuração do banco de dados do CACIC.

Na próxima tela, como exibido na Figura 10, o CACIC solicita que o administrador insira alguns dados sobre a localização onde o sistema está sendo implantado e alguns dados sobre o próprio administrador, como: login, senha, nome, *e-mail* e telefone.

Posteriormente, quando toda a fase de configuração do sistema está concluída, o administrador pode criar novas contas de acesso, às quais serão dadas permissões de administrador ou de usuários comuns com algumas restrições de acesso.

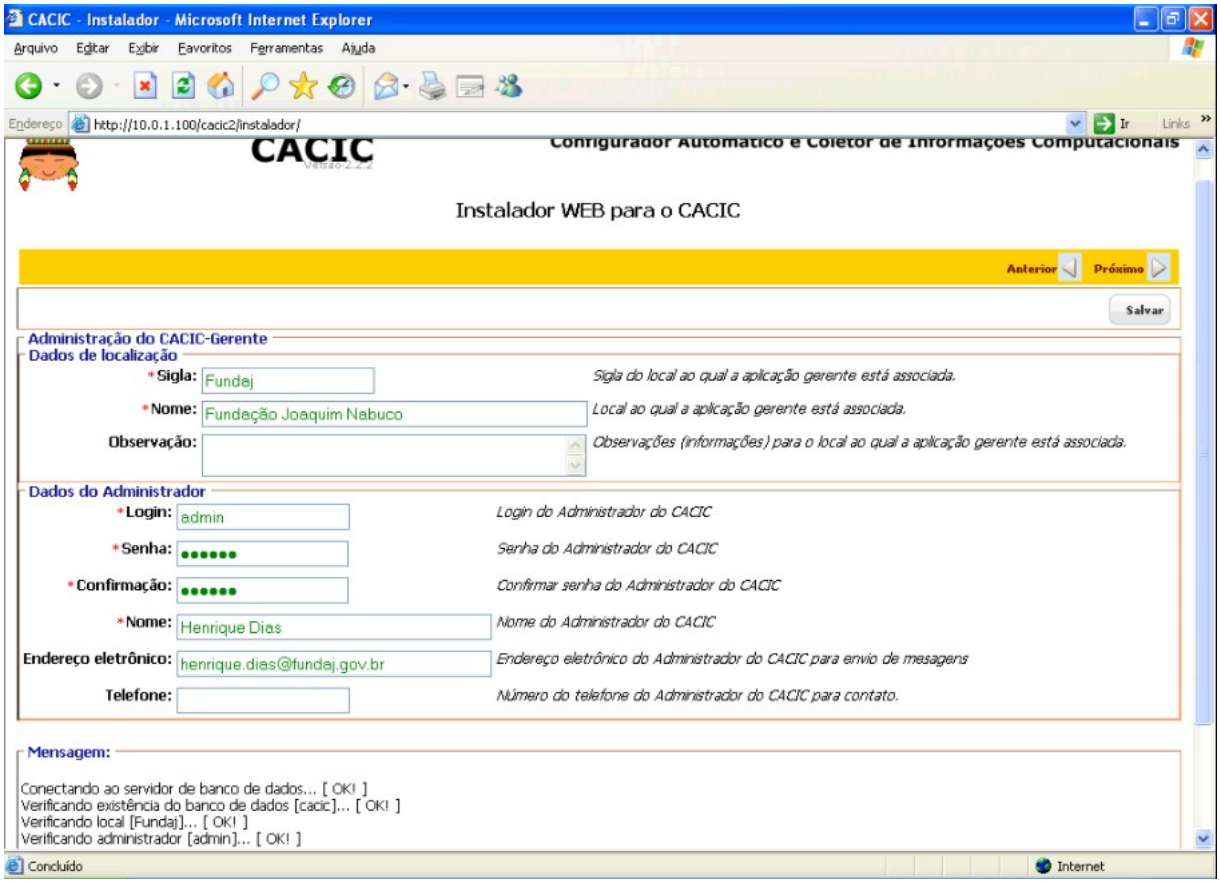


Figura 10. Tela de configuração dos dados do administrador do CACIC.

Por fim, como apresentado na Figura 11, o CACIC exibe na próxima tela uma mensagem de sucesso na configuração do sistema. A tela também sugere que o administrador exclua o diretório ‘instalador’ para que uma nova configuração inicial não corra o risco de ser criada acidentalmente.

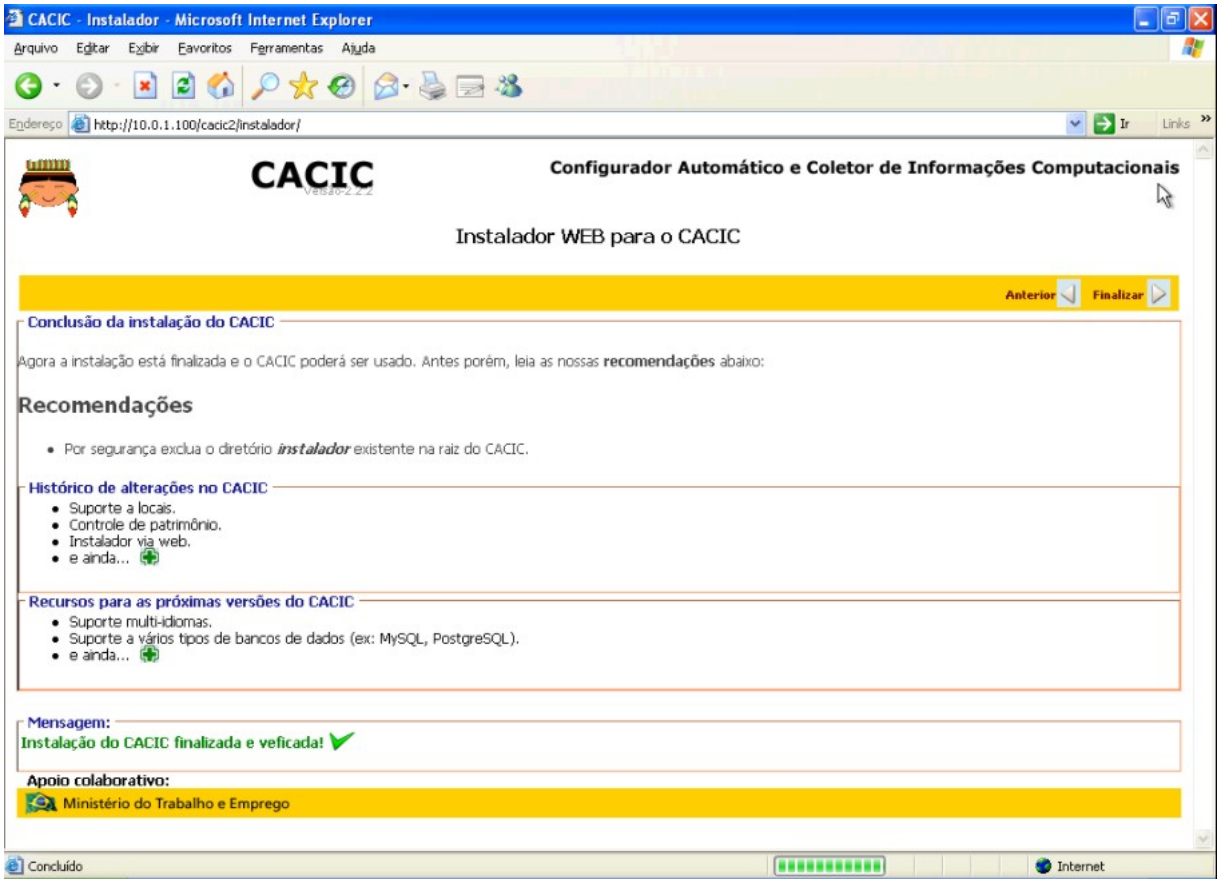


Figura 11. Tela de conclusão da configuração do CACIC.

Finalizada a configuração do CACIC, o administrador já pode acessar a tela inicial de gerenciamento do sistema. Para isso, a partir de qualquer ponto da rede, basta acessar o endereço http://ipdoservidor/cacic2/ via qualquer navegador *Web.*

Como mostra a Figura 12, o CACIC exibe em sua tela inicial um gráfico com a quantidade de equipamentos monitorados. Ao inserir o login e senha, o administrador tem acesso a uma vasta quantidade de informações referentes aos ativos de redes cadastrados. Mais detalhes sobre estas informações serão fornecidos no Capítulo 4.

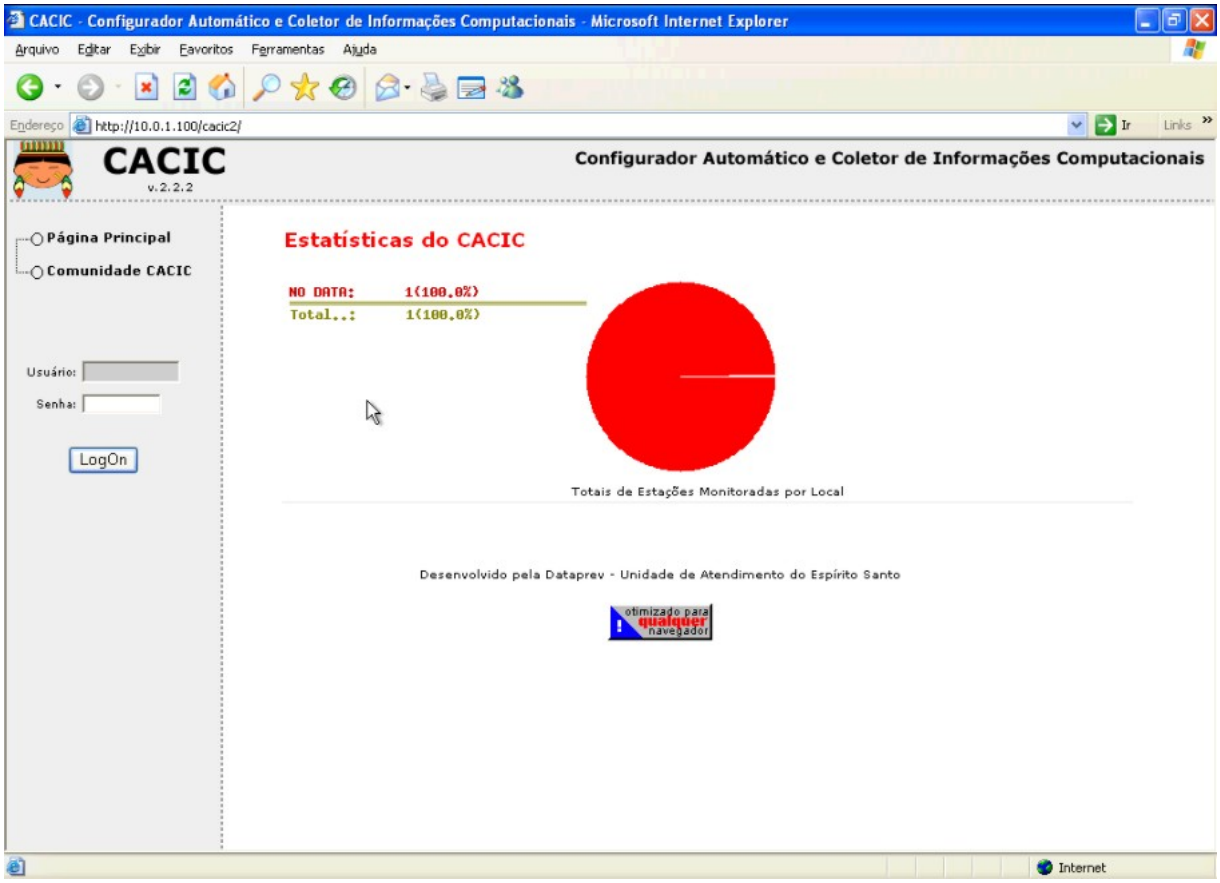


Figura 12. Tela inicial de gerenciamento do CACIC.

3.3.4 Instalação dos Agentes

Quando instalados nos ativos de redes, os agentes servem para que o servidor gerente tenha acesso aos dados de configuração dos respectivos ativos. O módulo agente, quando está em execução, é responsável pela coleta dos dados relativos a *hardware*, *software*, redes e patrimônio, manter o módulo gerente atualizado em relação às informações dos ativos de redes e enviar alertas e notificações para o módulo gerente quando alterações de *hardware* ou patrimônio acontecerem. Os agentes são componentes de *software* compilados que ficam permanentemente ativos. A instalação dos agentes pode ser feita de duas formas. Se utilizarmos redes de pequeno porte, os agentes podem ser instalados manualmente, bastando apenas acessar cada ativo de rede e realizar o *download* dos componentes via FTP diretamente do servidor onde o módulo gerente está localizado e os respectivos componentes estão armazenados. Após o *download*, executa-se o componente e o agente está pronto para ser utilizado. Por outro lado,

caso o parque computacional envolvido seja de médio ou grande porte, é recomendável instalar os agentes automaticamente via *script* de *logon*. No estudo de caso aqui apresentado, a segunda opção foi escolhida, uma vez que mais de 300 ativos de redes estavam sendo monitorados.

Para que o segundo método seja realizado é preciso que a rede seja baseada em servidores de domínio. Dessa forma, um *script* pode ser criado e inicializado no momento que o usuário faz *logon* na rede. Assim, os componentes dos agentes são obtidos do servidor e executados automaticamente, sem que o usuário final tenha conhecimento. No projeto desta monografia, a rede possuía um controlador de domínio *Windows* 2003 *Server – Enterprise Edition*. Uma diretiva de grupo foi criada para que todos os usuários da rede executassem o *script* ao realizarem o *logon* na rede. Essa operação foi possível graças ao *Active Directory*.

3.3.4.1 Script para Instalação Automática

O *script* exibido no Apêndice B foi utilizado neste estudo de caso sendo salvo como um arquivo *batch*, que é um tipo de arquivo utilizado para automatizar tarefas no sistema operacional *Windows*. O arquivo *batch*, também conhecido como arquivo bat ou ponto-bat, nada mais é do que um conjunto de comandos executados seqüencialmente. Ele foi associado a uma diretiva de grupo do *Active Directory* para ser inicializado quando um determinado usuário faz login na rede.

Um problema encontrado foi a negação de permissão aos usuários da rede para instalar qualquer tipo de programa. Esta era uma diretiva de grupo aplicada à grande maioria dos usuários da instituição por questão de segurança. Para sanar esse problema foi preciso utilizar um programa chamado LSrunase, que dá poderes de administrador aos usuários somente para que uma determinada instalação seja feita [19].

O *script* funciona da seguinte forma:

- Um *login* com permissões de administrador, juntamente com sua senha, são reservados para ser utilizados;

- A senha é inserida no LSrunase para que seja criptografada, como mostra a Figura 13 [20];
- O *login*, senha criptografada, domínio e local onde encontra-se o LSrunase são inseridos no *script*;
- O usuário faz *login* no sistema e o *script* é executado;
- Se o agente do CACIC já estiver instalado no ativo de rede, o *script* é finalizado;
- Se o agente ainda não tiver sido instalado, a instalação é iniciada;

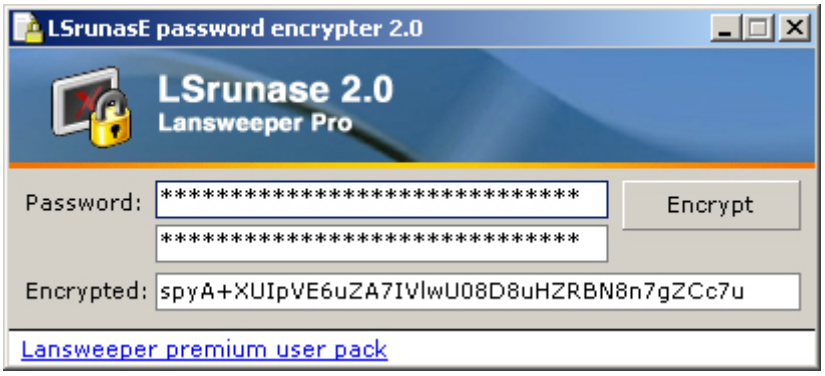


Figura 13. Criptografia da senha do administrador através do programa LSrunase.

O processo de instalação é rápido, eficiente e imperceptível ao usuário, pois nenhuma mensagem referente à instalação é exibida na tela.

Capítulo 4

Obtenção e Análise dos Resultados

Até o momento, a FUNDAJ conta com 325 ativos de redes monitorados pelo CACIC, sendo 5 servidores, 300 estações de trabalho e 20 impressoras de rede. Os demais servidores ainda não foram cadastrados porque operam com o sistema operacional Linux, devendo então aguardar a próxima versão do CACIC. Cerca de 50 estações de trabalho ainda não foram cadastradas por estar em um local fora do domínio. Em breve essas máquinas também farão parte dele.

A Figura 14 exibe a tela inicial do CACIC, a partir de onde é possível obter todas as informações sobre os ativos de redes cadastrados. Dois gráficos foram gerados, sendo o primeiro destinado a quantificar as versões dos sistemas operacionais e o segundo informar quando foram realizadas as últimas coletas.

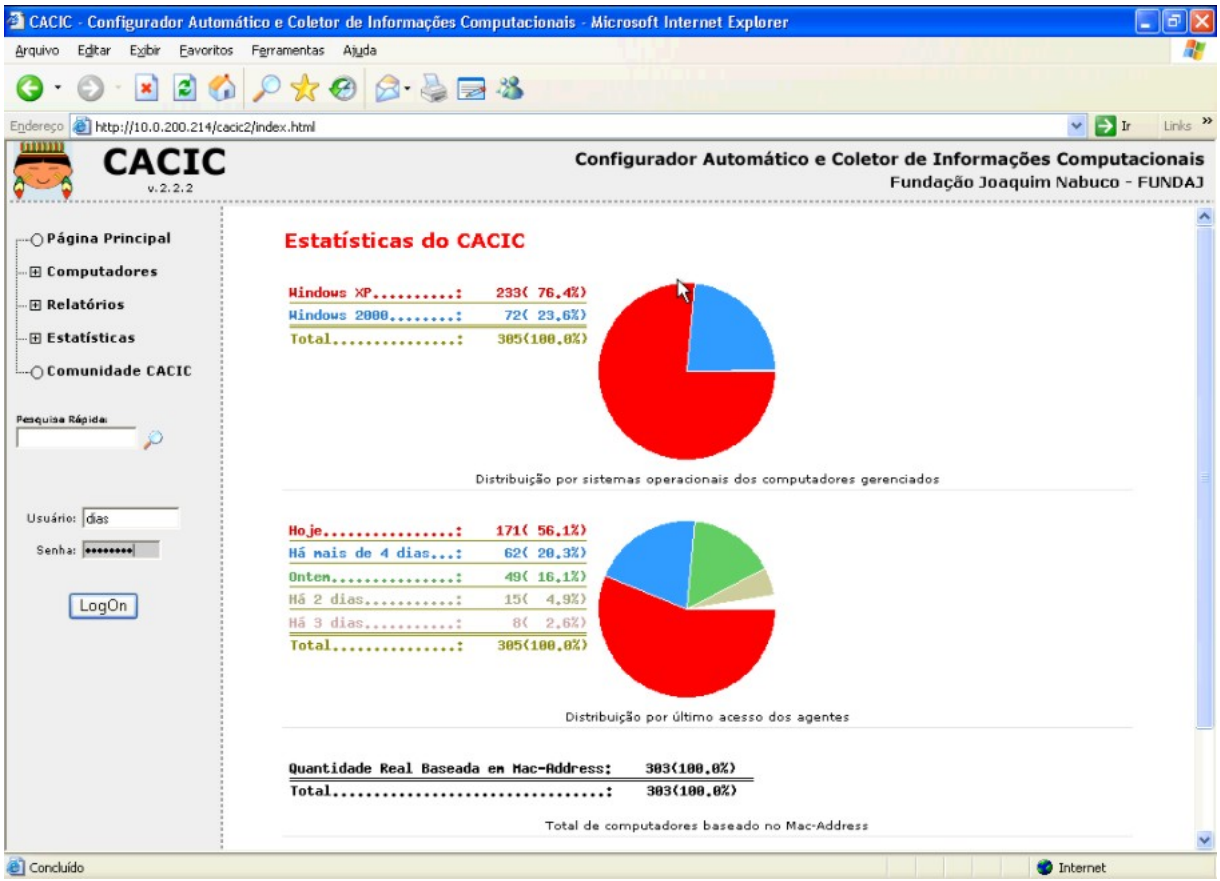


Figura 14. Tela inicial do CACIC.

Com o agente do CACIC operando nesses ativos de redes foi possível obter resultados positivos do sistema. As coletas estão gerando relatórios atualizados de duas em duas horas. Através dessas coletas é possível avaliar as funcionalidades do CACIC de forma prática.

Apesar da freqüência de atualização dos dados ser alta, o tráfego da rede não fica comprometido, uma vez que os dados coletados pelos agentes são passados para o módulo gerente somente quando alguma atualização é feita no ativo de rede.

4.1 Obtenção dos Resultados

Para coletar os dados provenientes dos agente instalados nos ativos de redes, o CACIC possui sete módulos com responsabilidades distintas. Todos eles são listados abaixo:

- Coleta informações de compartilhamento de diretórios e impressoras;
- Coleta informações de *hardware*;
- Coleta informações sobre os sistemas monitorados;
- Coleta informações do antivírus *OfficeScan*;
- Coleta informações de patrimônio;
- Coleta informações de *software*;
- Coleta informações sobre unidades de disco.

A Figura 15 mostra a tela onde é possível ter acesso a configurações específicas de cada um dos módulos. Também é permitida a escolha de quais deles devem estar operantes ou não. Na mesma figura, por exemplo, o módulo ‘Coleta informações de patrimônio’ está desabilitado, pois este não é um dos objetivos principais da FUNDAJ neste momento.

O módulo de coleta de informação de *hardware* tem ajudado bastante na busca de informações sobre o *hardware* instalado nos servidores e estações de

trabalho, tais como: memória, placa de vídeo, placa de rede, discos rígidos, etc. Essas informações são bastantes úteis para saber a característica física de cada ativo de rede. É possível também, através desse módulo, ser informado via *e-mail* sobre qualquer alteração feita no *hardware* dos equipamentos. Esse tipo de informação é muito útil, visto que qualquer alteração de configuração de *hardware* só é permitida pelo setor de manutenção, provendo assim um maior controle para esse setor. Antes da implantação do CACIC, não havia qualquer tipo de controle. A Figura 16 mostra o exemplo de uma coleta de *hardware* realizada em uma determinada estação de trabalho da rede. Um histórico da configuração do *hardware* também é armazenado no banco de dados. Esse tipo de informação é útil para saber quais peças já foram trocadas em cada ativo de rede.

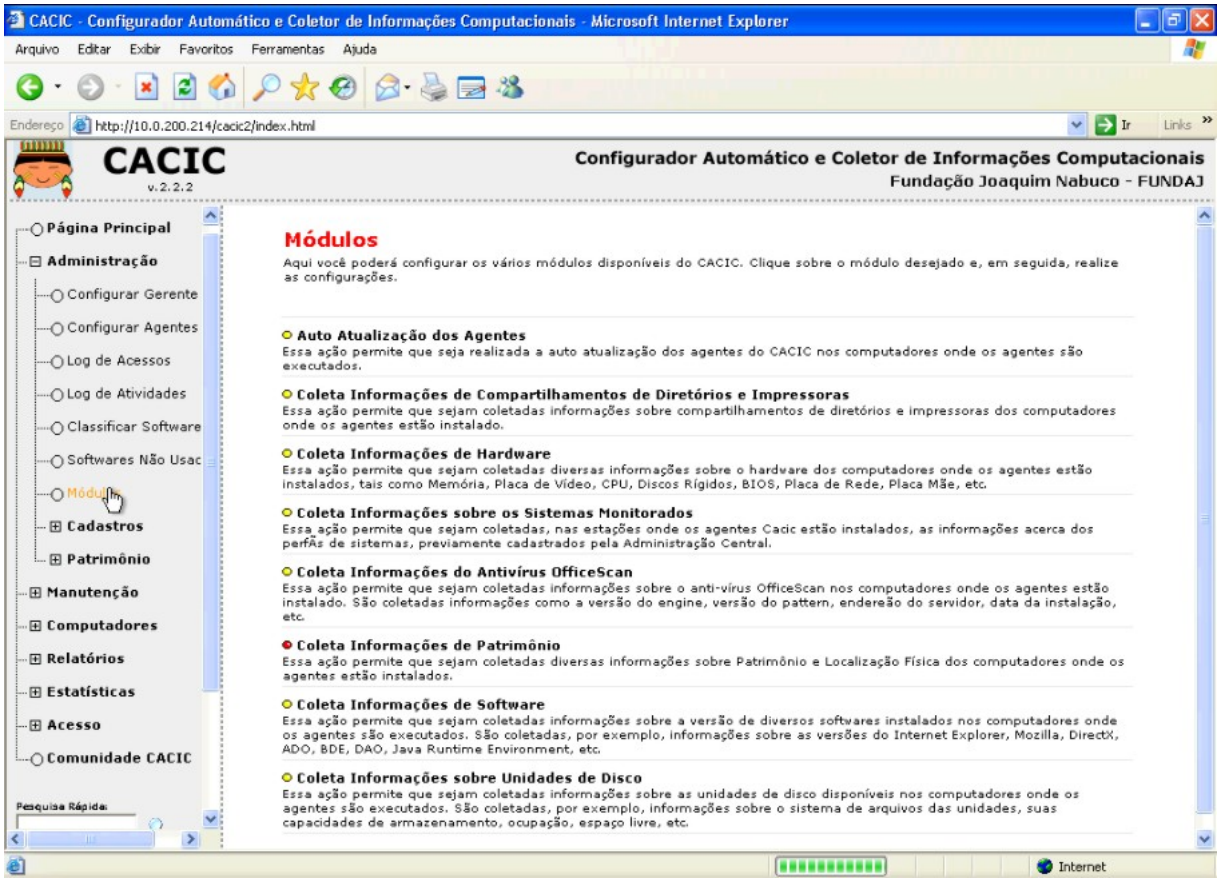


Figura 15. Tela de configuração dos módulos de coleta do CACIC.

O *status* de uso do disco rígido de cada servidor ou estação de trabalho também pode ser acompanhado. Essa informação tem ajudado bastante na prevenção de problemas como insuficiência de espaço de armazenamento de dados para o usuário. A Figura 17 mostra um relatório onde é apresentado o status do

disco com 13% de uso de uma estação de trabalho, onde também é indicado o sistema de arquivos utilizado.

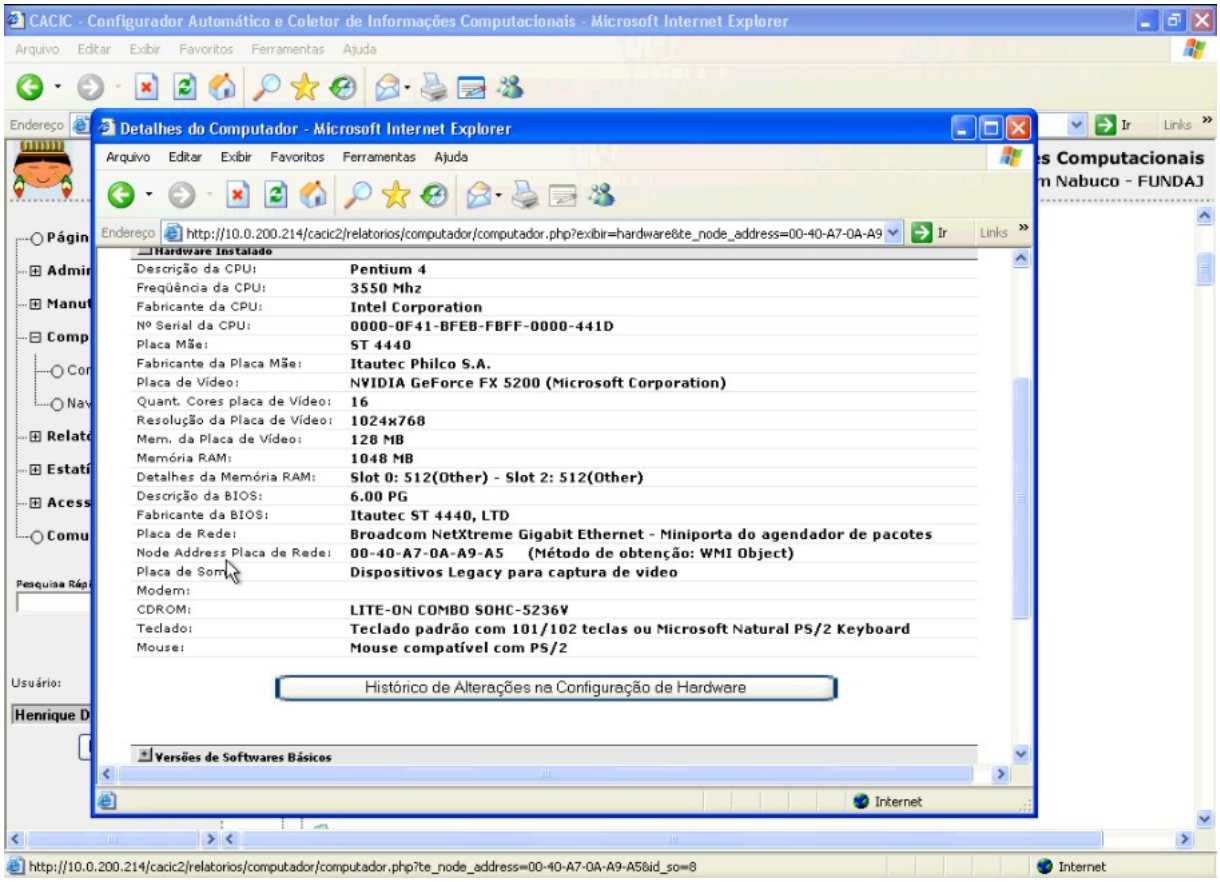


Figura 16. Tela de consulta de *hardware* do CACIC.

O módulo de coleta de informações de *software* permite que sejam obtidas informações sobre a versão de todos os programas instalados nos ativos de redes e também acompanha se estes são licenciados ou não. Isso evita problemas com pirataria de *software* e protege a instituição de sofrer algum tipo de processo judicial. Este módulo também tem ajudado a detectar programas que não são adequados para a FUNDAJ, como jogos e programas de *downloads*, por exemplo.

Além de apresentar um histórico detalhado dos programas instalados em cada ativo de rede, o CACIC também permite que tais programas sejam classificados em categorias, facilitando ainda mais o monitoramento. O administrador também pode criar novas categorias.

O CACIC permite gerar diversos tipos de relatórios sobre as informações coletadas, onde é possível selecionar qual o tipo de informação desejada (ex:

hardware, software ou *rede*) e também aplicar filtros para selecionar quais informações especificas devem ser exibidas. Períodos de datas também podem ser determinados em alguns relatórios, o que torna o monitoramento ainda mais preciso.

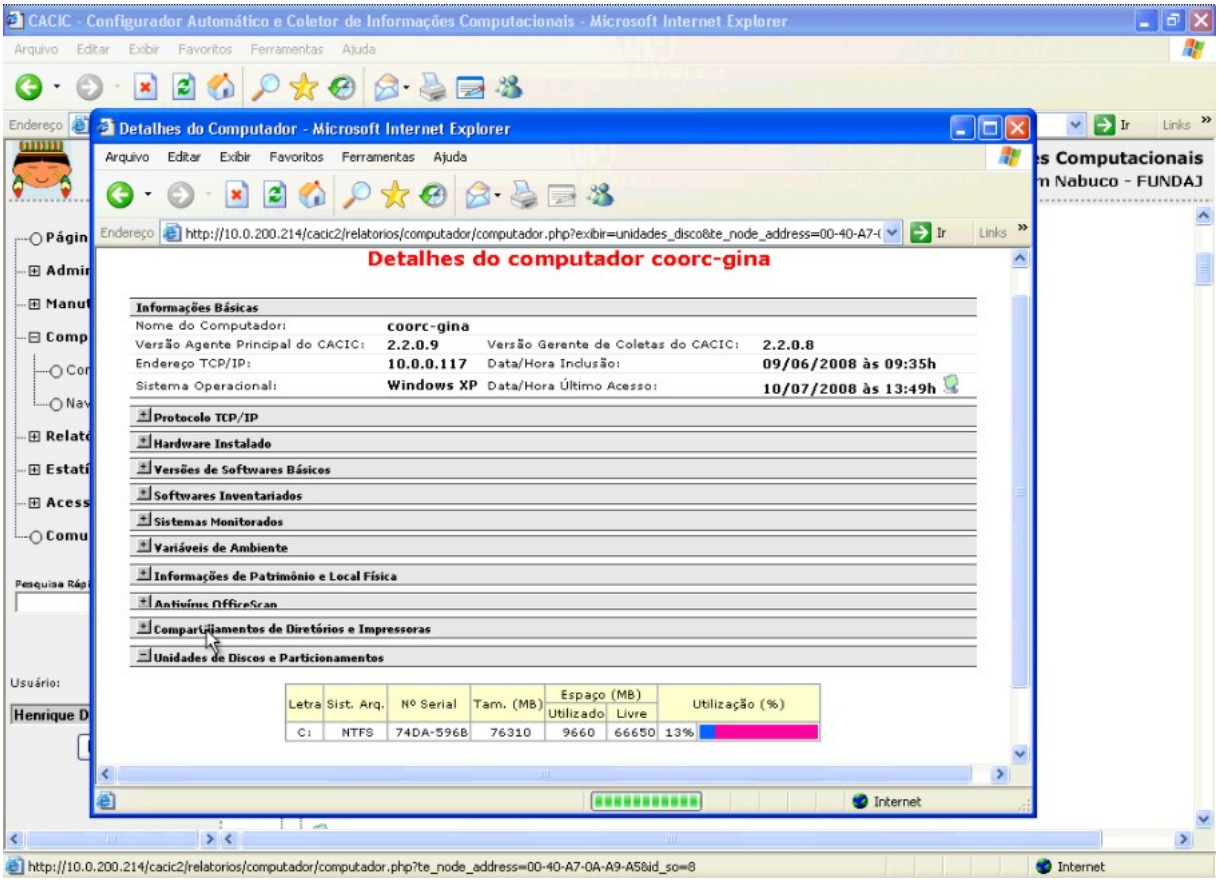
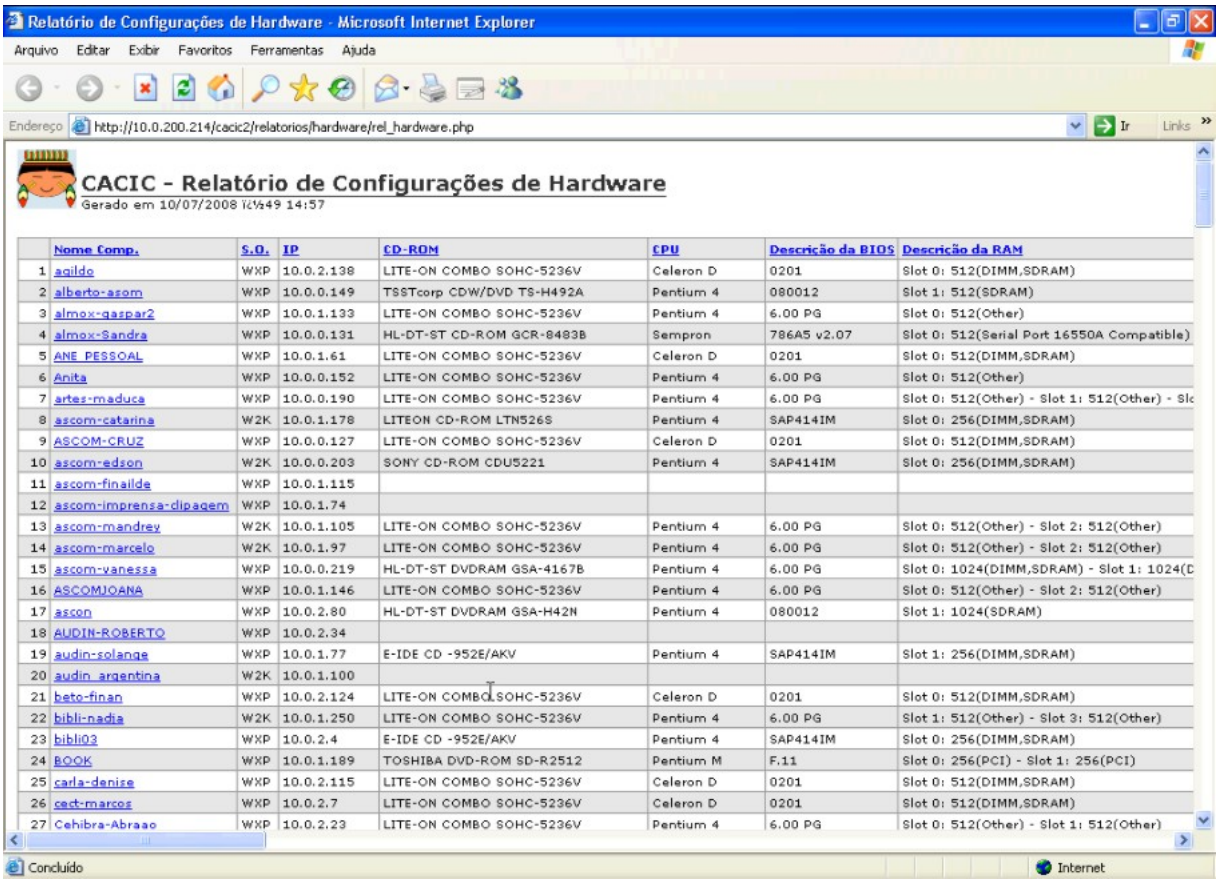


Figura 17. Tela de consulta de utilização de disco e particionamento.

Na Figura 18, por exemplo, um relatório foi gerado contendo informações sobre o *hardware* de todos os servidores e estações de trabalho da rede, tais como: memória, placa de vídeo, CPU (*Central Processing Unit*), discos rígidos (informações sobre o sistema de arquivos, capacidade, utilização), BIOS (*Basic Input/Output System*), placa de rede, placa mãe e periféricos (teclado, mouse). Além dessas informações, também foram disponibilizados os nomes das máquinas, IP's e sistemas operacionais, deixando assim, a consulta mais completa.

Outro relatório bastante utilizado é o referente às configurações de rede dos ativos monitorados. Informações como DNS (*Domain Name System*), *gateway*, IP, máscara, servidor DHCP (*Dynamic Host Configuration Protocol*) e WINS (*Windows Internet Name Services*) podem ser obtidos rapidamente e de forma sucinta.



	Nome Comp.	S.O.	IP	CD-ROM	CPU	Descrição da BIOS	Descrição da RAM
1	agildo	WXP	10.0.2.138	LITE-ON COMBO SOHC-5236V	Celeron D	0201	Slot 0: 512(DIMM,SDRAM)
2	alberto-asom	WXP	10.0.0.149	TSSTcorp CDW/DVD TS-H492A	Pentium 4	080012	Slot 1: 512(SDRAM)
3	almox-gaspar2	WXP	10.0.1.133	LITE-ON COMBO SOHC-5236V	Pentium 4	6.00 PG	Slot 0: 512(Other)
4	almox-Sandra	WXP	10.0.0.131	HL-DT-ST CD-ROM GCR-8483B	Sempron	786A5 v2.07	Slot 0: 512(Serial Port 16550A Compatible)
5	ANE_PESSOAL	WXP	10.0.1.61	LITE-ON COMBO SOHC-5236V	Celeron D	0201	Slot 0: 512(DIMM,SDRAM)
6	Anita	WXP	10.0.0.152	LITE-ON COMBO SOHC-5236V	Pentium 4	6.00 PG	Slot 0: 512(Other)
7	artes-maduca	WXP	10.0.0.190	LITE-ON COMBO SOHC-5236V	Pentium 4	6.00 PG	Slot 0: 512(Other) - Slot 1: 512(Other) - Slo
8	ascom-catarina	W2K	10.0.1.178	LITEON CD-ROM LTN526S	Pentium 4	SAP414IM	Slot 0: 256(DIMM,SDRAM)
9	ASCOM-CRUZ	WXP	10.0.0.127	LITE-ON COMBO SOHC-5236V	Celeron D	0201	Slot 0: 512(DIMM,SDRAM)
10	ascom-edson	W2K	10.0.0.203	SONY CD-ROM CDU5221	Pentium 4	SAP414IM	Slot 0: 256(DIMM,SDRAM)
11	ascom-finailde	WXP	10.0.1.115				
12	ascom-imprensa-dipagem	WXP	10.0.1.74				
13	ascom-mandrev	W2K	10.0.1.105	LITE-ON COMBO SOHC-5236V	Pentium 4	6.00 PG	Slot 0: 512(Other) - Slot 2: 512(Other)
14	ascom-marcelo	W2K	10.0.1.97	LITE-ON COMBO SOHC-5236V	Pentium 4	6.00 PG	Slot 0: 512(Other) - Slot 2: 512(Other)
15	ascom-vanessa	WXP	10.0.0.219	HL-DT-ST DVDRAM GSA-4167B	Pentium 4	6.00 PG	Slot 0: 1024(DIMM,SDRAM) - Slot 1: 1024(D
16	ASCOMJOANA	WXP	10.0.1.146	LITE-ON COMBO SOHC-5236V	Pentium 4	6.00 PG	Slot 0: 512(Other) - Slot 2: 512(Other)
17	ascon	WXP	10.0.2.80	HL-DT-ST DVDRAM GSA-H42N	Pentium 4	080012	Slot 1: 1024(SDRAM)
18	AUDIN-ROBERTO	WXP	10.0.2.34				
19	audin-solange	WXP	10.0.1.77	E-IDE CD -952E/AKV	Pentium 4	SAP414IM	Slot 1: 256(DIMM,SDRAM)
20	audin_argentina	W2K	10.0.1.100				
21	beto-finan	WXP	10.0.2.124	LITE-ON COMBO SOHC-5236V	Celeron D	0201	Slot 0: 512(DIMM,SDRAM)
22	bibli-nadia	W2K	10.0.1.250	LITE-ON COMBO SOHC-5236V	Pentium 4	6.00 PG	Slot 1: 512(Other) - Slot 3: 512(Other)
23	bibli03	WXP	10.0.2.4	E-IDE CD -952E/AKV	Pentium 4	SAP414IM	Slot 0: 256(DIMM,SDRAM)
24	BOOK	WXP	10.0.1.189	TOSHIBA DVD-ROM SD-R2512	Pentium M	F.11	Slot 0: 256(PCI) - Slot 1: 256(PCI)
25	carla-denise	WXP	10.0.2.115	LITE-ON COMBO SOHC-5236V	Celeron D	0201	Slot 0: 512(DIMM,SDRAM)
26	cect-marcos	WXP	10.0.2.7	LITE-ON COMBO SOHC-5236V	Celeron D	0201	Slot 0: 512(DIMM,SDRAM)
27	Cehibra-Abraao	WXP	10.0.2.23	LITE-ON COMBO SOHC-5236V	Pentium 4	6.00 PG	Slot 0: 512(Other) - Slot 1: 512(Other)

Figura 18. Relatório de configurações de *hardware.*

4.2 Análise dos Resultados

A escolha do CACIC para ser implementado em toda a Administração Pública Federal foi motivada principalmente pelas diversas funcionalidades que ele possui. Outro fator importante foi sua condição de *software* livre. A compra de um *software* proprietário demandaria recursos extras. A vasta documentação encontrada facilitou a implantação do CACIC, contribuindo para um maior aprofundamento no estudo e configuração das tecnologias utilizadas. Até o presente momento há uma grande satisfação com o desempenho do CACIC. Apesar de ainda não contemplar todo o parque computacional da FUNDAJ, ele já tem atendido positivamente com os resultados descritos anteriormente.

4.2.1 Problemas Encontrados

A implantação dos agentes foi uma das partes mais trabalhosas do projeto, uma vez que a documentação oficial do CACIC não aborda muitos detalhes sobre esse tema. As dúvidas foram sanadas através do fórum de discussão da comunidade CACIC.

Foi possível perceber que o agente só coleta os dados corretamente se a rede onde ele estiver atuando estiver cadastrada no banco de dados do módulo gerente.

O funcionamento do agente no *Windows* 98 também não foi satisfatório, uma vez que o usuário poderia interromper o processo de coleta do agente quando quisesse, prejudicando a atualização dos dados. Um paliativo para isso foi aguardar a atualização gradativa das poucas estações de trabalho que ainda estavam com esse sistema operacional, uma vez que esse projeto já estava sendo planejado para ser executado em breve.

Capítulo 5

Conclusão e Trabalhos Futuros

Este trabalho procurou analisar de forma sintética a importância do monitoramento de ativos de redes em parques computacionais, principalmente os de médio e grande porte. Em busca desse objetivo, um estudo de caso foi proposto e executado em tempo hábil, podendo assim gerar resultados que comprovem a eficiência dos sistemas de monitoramento.

No estudo de caso foi utilizado o sistema CACIC, mas certamente o que foi aqui analisado pode servir como base para estudos futuros sobre qualquer outro sistema de monitoramento, sempre levando em consideração as suas funcionalidades existentes.

5.1 Contribuições e Conclusões

Nesta monografia constatou-se que a utilização de sistemas de monitoramento de ativos de redes podem gerar grande impacto na melhoria da gestão de recursos de TI. Entretanto, dependendo da arquitetura utilizada, limitações de escalabilidade podem dificultar a adoção destes sistemas nas empresas.

Um estudo de caso sobre o sistema CACIC pôde proporcionar um bom levantamento de dados, tornando possível analisar a arquitetura de um sistema de monitoramento. Foi constatado com isso, que um dos principais limitadores de tais sistemas é a baixa escalabilidade que limita o crescimento de uma implantação de monitoramento, refletindo no desempenho do sistema como um todo.

Com a implantação do CACIC na rede da FUNDAJ foi possível visualizar sua contribuição para o gerenciamento da mesma. Os ativos de redes onde já se encontram instalados os agentes estão constantemente atualizando suas informações depositadas na base de dados do módulo gerente. Pode-se concluir também que esse trabalho irá contribuir fundamentalmente, não só para o setor de

informática da FUNDAJ, mas também com o setor de patrimônio, que poderá contar com todas as informações de inventário quando um projeto nesta área for implantado.

A realização deste trabalho foi um desafio muito gratificante, onde foi possível empregar os conhecimentos adquiridos no curso de Engenharia da Computação. Temas como engenharia de *software*, banco de dados, sistemas operacionais e redes de computadores puderam ser vistos de forma prática, ajudando a ampliar estes conhecimentos. Os resultados obtidos também atenderam as necessidades e expectativas do projeto, ou seja, implementar o CACIC em mais uma Unidade da Administração Pública Federal, atendendo aos objetivos de sua implantação e dando espaço para melhorias e projetos futuros.

5.2 Trabalhos Futuros

Foram identificados trabalhos que podem ser implementados em um futuro próximo e que são relacionados não somente ao sistema CACIC, mas também à sua arquitetura, baseada no conceito de agente e gerente. Dentre eles, é possível destacar os seguintes:

- Realização de uma coleta de dados mais detalhada para elaborar uma análise mais aprofundada sobre a segurança e robustez do CACIC, que não foram discutidas neste trabalho;

- Aprimoramento da documentação da nova versão (2.4) do CACIC lançada neste ano e que ainda não tem referências suficientes para uma boa compreensão;

- Integração do CACIC com outros sistemas de monitoramento. Por ser uma ferramenta de código aberto, a sua interação com outras tecnologias é possível e viável.

Do ponto de vista de monitoramento, sugere-se ainda o estudo de sistemas que trabalhem com áreas afins de redes de computadores, como gerência de desempenho, gerência de falhas, gerência de configurações, etc.

Bibliografia

[1] **3Com Network Supervisor – Recursos e Benefícios**. Disponível em: <http://www.3com.com/prod/pt_la_amer/detail.jsp?tab=features&sku=3C15100E>. Acesso em: 9 de outubro de 2008.

[2] ABDALA, E. A.; OLIVEIRA, M. **Tecnologias da Internet: Casos Práticos em Empresas**, 1ª edição, Porto Alegre: EDIPUCRS, 2003.

[3] **Arquitetura CACIC UNB**. Disponível em: <http://svn.softwarepublico.gov.br/trac/cacic/wiki/ArquiteturaCacicUNB>. Acesso em: 12 de outubro de 2008.

[4] BACIC, N. M. **O Software Livre como Alternativa ao Aprisionamento Tecnológico Imposto pelo Software Proprietário**, Trabalho de Conclusão de Curso de Ciência da Computação, Universidade Estadual de Campinas, 2003.

[5] BRAGA, B. F.; KINOSHITA, C. **Uma Proposta de Arquitetura Adaptada do Modelo JMX para o Sistema CACIC**, Trabalho de Conclusão de Curso de Ciência da Computação, Universidade de Brasília, 2005.

[6] **CACIC**. Disponível em: <http://www.softwarepublico.gov.br/dotlrn/clubs/cacic/onecommunity?page_num=0>. Acesso em: 19 de setembro de 2008.

[7] **Cacti – O Tutorial Fácil – O que é o Cacti?**. Disponível em: <http://openmaniak.com/pt/cacti.php>. Acesso em: 29 de outubro de 2008.

[8] **Cacti: The Complete RRDTool based Graphing Solution**. Disponível em: <www.cacti.net>. Acesso em: 28 de outubro de 2008.

[9] **Cartilha de Segurança**. Disponível em: <http://cartilha.cert.br/glossario/>. Acesso em: 15 de outubro de 2008.

[10] CARVILHE, J. L. V. **A Utilização de Tecnologias Web em Sistemas de Gerência Corporativa**, Especialização em Sistemas Distribuídos, Pontifícia Universidade Católica do Paraná, 2000.

[11] CASE, J.; FEDOR, M.; SCHOFFSTALL, M.; DAVIN, J. **A Simple Network Management Protocol (SNMP)**, Request for Comments 1157, Internet Engineering Task Force, 1990.

[12] **DATAPREV**. Disponível em: <http://www.dataprev.gov.br/produtos/cacic.htm>. Acesso em: 20 de agosto de 2008.

[13] DATAPREV. **Manual de Implantação Sistema de Inventário CACIC – Parte I – Introdução ao Sistema**, Espírito Santo, DATAPREV, 2007.

[14] DATAPREV. **Manual de Implantação Sistema de Inventário CACIC – Parte II – Intalação para o Sistema Operacional Debian,** Espírito Santo, DATAPREV, 2007.

[15] **EsCCap31 – CACIC – Trac**. Disponível em: <http://svn.softwarepublico.gov.br/trac/cacic/wiki/EsCCap31>. Acesso em: 9 de outubro de 2008.

[16] FERRARI, F. A. **Crie banco de dados em MySQL**, 1ª edição, São Paulo, Digerati Books, 2007.

[17] **INFOWESTER. Banco de dados MySQL e PostgreSQL [on-line]**. Disponível em: <http://www.infowester.com/postgremysql.php>. Acesso em: 25 de setembro de 2008.

[18] JUNIOR, I. D. M.; JUNIOR, J. C. **Descoberta e Monitoramento de Recursos em Redes de Computadores usando Agentes Móveis**, In: WORKCOMP SUL 2004, Florianópolis, 2004.

[19] **LSrunas [Comunidade Cacic]**. Disponível em: <http://cetico.org/cacic/lsrunas?do=show>. Acesso em: 1 de novembro de 2008.

[20] **LSrunas: runas and passing the password (sanur replacement)**. Disponível em: <http://www.moernaut.com/default.aspx?item=lsrunas>. Acesso em: 1 de novembro de 2008.

[21] MAGRIN, M. H. **Guia do Profissional Linux**, 2ª edição, São Paulo: Digerati, 2006.

[22] MELO, A. A.; NASCIMENTO, M. G. F. **PHP Profissional**, 1ª edição, São Paulo: Novatec, 2007.

[23] MOURA, J. M. **Gerência de Sistemas Baseada em Redes Ativas**, Trabalho de Conclusão de Curso de Ciência da Computação, Universidade Tiradentes, 2003.

[24] **Network security scanner, vulnerability and patch management, port scanner and network auditing**. Disponível em: <http://www.gfi.com/lannetscan/?adv=69&loc=535>. Acesso em: 9 de outubro de 2008.

[25] NIEDERAUER, J. **PHP 5 – Guia de Consulta Rápida**, 3ª edição, São Paulo: Novatec, 2008.

[26] BOUTABA, R.; GUEMHIOUI, K.; DINI, P. **An Outlook on Intranet Management**. IEEE Communications Magazine. v. 35, n. 10, p. 92-99, out. 1997.

[27] RIBEIRO, D. D. C. **Software Livre na Administração Pública: Estudo de Caso Sobre Adoção do SAMBA na Auditoria Geral do Estado de Minas Gerais.** Especialização em Administração de Redes Linux, Universidade Federal de Lavras, 2004.

[28] PEREIRA, M. C. **Administração e Gerência de Redes de Computadores**, Trabalho de Conclusão de Curso de Ciência da Computação, Universidade Federal de Santa Catarina, 2001.

[29] **Portal do Software Público Brasileiro.** Disponível em: <http://www.softwarepublico.gov.br/O_que_e_o_SPB>. Acesso em: 12 de agosto de 2008.

[30] STALLINGS, W. **SNMP, SNMP v2, SNMP v3 and RMON 1 and 2**, 3ª edição, Addison-Wesley, 1999.

[31] TANENBAUM, A. S. **Redes de Computadores**, 4ª edição, Rio de Janeiro: Campus, 2003.

[32] **The Proftpd Project: Features & Platforms.** Disponível em: <http://www.proftpd.org/features.html>. Acesso em: 1 de novembro de 2008.

[33] THOTTAN M., J. C. **Anomaly Detection in IP Networks**, IEEE Transactions in Signal Processing, v. 51, n. 8, p. 2191-2204, ago. 2003.

[34] VEIGA, R. G. A. **Apache – Guia de Consulta Rápida**, 1ª edição, São Paulo: Novatec, 2006.

[35] **Web Server Survey Archives – Netcraft.** Disponível em: <http://news.netcraft.com/archives/web_server_survey.html>. Acesso em: 3 de novembro de 2008.

[36] ZARPELÃO, B. B. **Detecção de Anomalias e Geração de Alarmes em Redes de Computadores**, Trabalho de Conclusão de Curso de Ciência da Computação, Universidade Estadual de Londrina, 2004.

Apêndice A

Script para a Instalação do Módulo Gerente

```
#apt-get install mysql-server-5.0

#/usr/bin/mysqladmin -u root password 'senha'

#apt-get install proftpd

#vi /etc/proftpd/proftpd.conf

#adduser --shell /bin/false --home /var/www/ftpcacic ftpcacic

#mkdir /var/www/ftpcacic/agentes

#chown ftpcacic.ftpcacic /var/www/ftpcacic/agentes

#apt-get install apache2 php5-dev php5 php5-mysql php5-gd
php5-mcrypt libapache2-mod-php5

#vi /etc/apache2/apache2.conf

#vi /etc/php5/apache2/php.ini

#wget http://www.softwarepublico.gov.br/dotlrn/clubs/cacic/
file-storage/download/cacic2-v222-final.tar.gz?file%5fid
=186097

#tar -zxvf cacic2-v222-final.tar.gz -C /var/www/

#chown -R www-data /var/www/cacic2
```

Apêndice B

Script para a Instalação do Módulo Agente

```
@echo off

SET LOGIN=login

SET DOMAIN=dominio

SET SERVER="\\InstallCacic\"

SET SENHA=senha

SET CHKSISEXE=%WINDIR%\chksis.exe

if exist %CHKSISEXE% goto end else goto instalar

:instalar

%SERVER%\lsrunase.exe /user:%LOGIN% /password:%SENHA%
/domain:%DOMAIN% /command:"chkcacic.exe" /runpath:"%SERVER%"

goto end

:end
```