

Universidade Federal do Estado do Rio De Janeiro  
Escola de Informática Aplicada  
Curso de Bacharelado em Sistemas de Informação

**Uma Solução de Monitoramento para Infraestrutura  
Corporativa de Serviços de TI**

André Vieira Pinto

**Orientador**  
Sidney Cunha de Lucena

Janeiro de 2014

# **Uma Solução de Monitoramento para Infraestrutura Corporativa de Serviços de TI**

André Vieira Pinto

Projeto de Graduação apresentado à Escola de Informática Aplicada da Universidade Federal do Estado do Rio de Janeiro (UNIRIO) para obtenção do título de Bacharel em Sistemas de Informação.

Aprovada por:

---

Sidney Cunha de Lucena (UNIRIO)

---

Carlos Alberto Vieira Campos (UNIRIO)

---

Alex Soares de Moura (RNP)

Janeiro de 2014

## **Agradecimentos**

Agradeço ao professor Sidney Lucena por me orientar, não apenas nesse projeto, mas ao longo de todo o curso, que sempre ofereceu oportunidades para expandir meus horizontes quando o tema envolvia Redes de Computadores. Foi um prazer ser seu aluno e monitor.

Devo agradecer também aos meus colegas de trabalho no Sesc Departamento Nacional, em especial ao meu supervisor Ronaldo Neves, que esteve sempre ao meu lado durante essa experiência profissional e sem o qual a ideia deste projeto sequer teria nascido.

O apoio da minha família e dos meus amigos da UNIRIO também foram essenciais para que eu não esquecesse dos meus objetivos e pudesse lutar para alcançá-los.

## **Resumo**

Com o avanço da tecnologia e a crescente dependência das instituições por seus serviços, torna-se necessário encontrar uma forma de permitir o gerenciamento de toda a infraestrutura de Tecnologia da Informação, essencial ao negócio da empresa. O gerenciamento eficiente de uma rede de computadores permite que falhas possam ser prevenidas e identificadas rapidamente, com o intuito de minimizar o impacto sobre os usuários e diminuir os prejuízos da corporação. Com base nisto, surgiu a oportunidade de realizar o estudo de um cenário real, no Departamento Nacional do Sesc (Serviço Social do Comércio). O projeto envolveu um ciclo de levantamento de necessidades no qual os aspectos da infraestrutura foram analisados, e foi determinada a maneira mais eficaz de realizar o monitoramento de cada dispositivo e serviço. Diversas ferramentas de gerência de TI foram estudadas a fim de identificar aquela que melhor se adaptaria ao cenário da instituição. É demonstrada a implementação do Zabbix como sistema de monitoramento de TI através da configuração de dispositivos, alertas, mapas, diagramas, gráficos e monitores em um ambiente corporativo. Ocorre também a validação da implementação, por meio de testes e simulações, com a intenção de assegurar que a ferramenta estivesse cumprindo seu papel de forma eficaz. Além da adaptação da solução ao ambiente da empresa, o projeto também permitiu observar o impacto positivo gerado sobre a equipe de TI responsável pelo gerenciamento da rede, e consequentemente sobre a empresa como um todo.

**Palavras-chave:** infraestrutura de TI, gerenciamento de TI, rede de computadores, monitoramento, Zabbix, FCAPS, SNMP.

## **Abstract**

The evolution of technology along the increasing dependency on its services by the corporations, made necessary finding a way to manage the IT infrastructure, vital to every company business. Efficient management of a computer network allows potential failures to be predicted and quickly detected, thus reducing the impact on end-users and decreasing the risk of loss by the corporation. Based on this, emerged the opportunity of conducting a study on a real scenario, the National Department of Sesc (Social Service of Commerce). The project involved developing an assessment of needs, in which aspects of the infrastructure were analyzed and the most effective way to perform the monitoring of each device and service was determined. Several IT management tools were studied in order to identify which one would best adapt to the scenario found. This document demonstrates the implementation of Zabbix as an IT monitoring system through the configuration of devices, alerts, maps, diagrams and graphs in a corporate environment. Based on the intention of validating the implementation of the system, a series of tests and simulations were performed in order to ensure its job would be done efficiently. Besides the adjustment of the solution to the company's environment, the project also allowed the positive impact on the IT staff to be noticed, and consequently on the company as a whole.

**Keywords:** IT infrastructure, IT management, computer networks, monitoring, Zabbix, FCAPS, SNMP.

## **Índice de Siglas**

API – Application Programming Interface

CPU – Central Processing Unit

DN – Departamento Nacional

DNS – Domain Name System

DR – Departamento Regional

E/S – Entrada/Saída

FCAPS – Fault, Configuration, Accounting, Performance and Security

FTP – File Transfer Protocol

HTTP – Hypertext Transfer Protocol

HTTPS – HyperText Transfer Protocol Secure

ICMP – Internet Control Message Protocol

IEC – International Electrotechnical Commission

IETF – Internet Engineering Task Force

IMAP – Internet Message Access Protocol

IP – Internet Protocol

ISO – International Organization for Standardization

ITIL – Information Technology Infrastructure Library

JMX – Java Management Extensions

LDAP – Lightweight Directory Access Protocol

MD5 – Message-Digest algorithm 5

MPLS – Multi Protocol Label Switching

Netconf – Network Configuration Protocol

NNTP – Network News Transfer Protocol

ODBC – Open Database Connectivity

OSI – Open Systems Interconnection  
POP – Post Office Protocol  
QoS – Quality of Service  
RFC – Request for Comments  
RPC – Remote Procedure Call  
RTT – Round-trip Time  
Senac – Serviço Nacional de Aprendizagem Comercial  
Sesc – Serviço Social do Comércio  
SLA – Service Level Agreement  
SNMP – Simple Network Management Protocol  
SSH – Secure Shell  
TCP – Transmission Control Protocol  
TI – Tecnologia da Informação  
TMN – Telecommunications Management Network  
TTL – Time to Live  
VoIP – Voice over Internet Protocol  
VPN – Virtual Private Network  
XML – Extensible Markup Language

# Índice

<b>1</b>	<b>Introdução</b>	<b>12</b>
1.1	Objetivos do trabalho	12
1.2	Estrutura organizacional do texto	13
<b>2</b>	<b>Fundamentos de Gerenciamento de TI</b>	<b>15</b>
2.1	Modelos de referência de gerenciamento	15
2.1.1	FCAPS	15
2.1.2	TMN	17
2.1.3	ITIL	18
2.2	Arquiteturas para gerenciamento de TI	19
2.2.1	SNMP	19
2.2.2	ICMP	20
2.2.3	NetFlow	22
2.2.4	Netconf	23
2.3	Ferramentas de gerência	24
2.3.1	Cacti	24
2.3.2	Icinga	24
2.3.3	InterMapper	25
2.3.4	Nagios	25
2.3.5	Opsview	26
2.3.6	Pandora FMS	26
2.3.7	SolarWinds	27
2.3.8	Zabbix	27
2.3.9	Comparação das ferramentas de gerência	28
<b>3</b>	<b>Cenário de Aplicação da Solução de Gerenciamento de TI</b>	<b>29</b>
3.1	Sobre a empresa	29
3.2	Números e estatísticas	29
3.3	Estrutura da rede	29
3.4	Requisitos de monitoramento	35
3.4.1	Coneção com a Internet	36
3.4.2	Coneção com a Intranet	36
3.4.3	Coneção com o satélite de videoconferência	36
3.4.4	Coneção com o serviço de telefonia	36
3.4.5	Estado dos switches locais	36
3.4.6	Equipamentos de energia	37
3.4.7	Servidores e sistemas internos	37
3.5	Solução antiga	37
<b>4</b>	<b>Zabbix</b>	<b>40</b>
4.1	Recursos de monitoramento	41
4.1.1	Agente Zabbix de monitoramento	41
4.1.2	Agente SNMP	43
4.1.3	Monitoramento sem agente	43
4.1.4	Monitoramento web	44
4.1.5	Monitoramento de máquina virtuais	45
4.1.6	Outros métodos de monitoramento	45
4.1.7	Monitoramento de serviços de TI – SLA	46
<b>5</b>	<b>Implementação do Sistema</b>	<b>47</b>
5.1	Testes com Appliance	47
5.2	Escolha do sistema operacional	48
5.3	Instalação do Zabbix	48

<b>5.4 Configuração de hosts</b>	<b>49</b>
5.4.1 Servidores	50
5.4.2 Roteadores	51
5.4.3 Switches	51
5.4.4 Outros dispositivos	52
<b>5.5 Configuração de gráficos</b>	<b>53</b>
<b>5.6 Configuração de mapas</b>	<b>54</b>
<b>5.7 Configuração de telas personalizadas</b>	<b>54</b>
<b>5.8 Integração com sistema de autenticação corporativo</b>	<b>55</b>
<b>5.9 Configuração de avisos por e-mail</b>	<b>56</b>
<b>6 Validação da Implementação</b>	<b>58</b>
6.1 Demonstração de falha em um dos links de voz	59
6.2 Demonstração de falha em um dos links de Internet	60
6.3 Demonstração de aumento excessivo de temperatura em um nobreak	62
<b>7 Impacto na Equipe de TI</b>	<b>64</b>
7.1 Facilitação da identificação dos problemas da rede	64
7.2 Diminuição do tempo de resposta	64
7.3 Priorização de investimentos	66
<b>8 Conclusões</b>	<b>67</b>
8.1 Trabalhos futuros	67
<b>9 Referências</b>	<b>69</b>

## **Índice de Tabelas**

<b>Tabela 1 - Principais tipos de mensagens do ICMP .....</b>	<b>21</b>
<b>Tabela 2 - Comparação de algumas das principais características dos sistemas testados .</b>	<b>28</b>
<b>Tabela 3 - Funções de monitoramento do agente Zabbix .....</b>	<b>43</b>
<b>Tabela 4 - Funções do monitoramento sem agente .....</b>	<b>43</b>

## Índice de Figuras

<b>Figura 1 - Áreas conceituais do modelo FCAPS</b>	<b>15</b>
<b>Figura 2 - Diagrama de camadas do Netconf</b>	<b>23</b>
<b>Figura 3 - Diagrama de blocos do Sesc Departamento Nacional (azuis e brancos)</b>	<b>30</b>
<b>Figura 4 - Interior de uma das salas de Teleinfo do Sesc DN</b>	<b>31</b>
<b>Figura 5 - Servidores virtualizados no datacenter principal do Sesc DN</b>	<b>32</b>
<b>Figura 6 - Switch core no datacenter principal do Sesc DN</b>	<b>32</b>
<b>Figura 7 - Servidores de contingência no datacenter secundário do Sesc DN</b>	<b>33</b>
<b>Figura 8 - Mapa do estado dos roteadores de Intranet do Sesc DN</b>	<b>34</b>
<b>Figura 9 - Diagrama da infraestrutura de TI do Sesc DN</b>	<b>35</b>
<b>Figura 10 - Interface principal do Nagios utilizado anteriormente</b>	<b>38</b>
<b>Figura 11 - Consumo de recursos do agente em um dos servidores do Sesc DN</b>	<b>41</b>
<b>Figura 12 - Verificações passivas (comunicação começa do servidor Zabbix)</b>	<b>42</b>
<b>Figura 13 - Verificações ativas (comunicação começa do agente Zabbix)</b>	<b>42</b>
<b>Figura 14 - Gráfico do tempo de resposta de um sistema web do Sesc DN</b>	<b>45</b>
<b>Figura 15 - Opção de download de Appliance na Homepage do Zabbix</b>	<b>47</b>
<b>Figura 16 - Atualizando o Zabbix por linha de comando</b>	<b>49</b>
<b>Figura 17 - Configuração de monitoramento de um servidor</b>	<b>50</b>
<b>Figura 18 - Configuração de monitoramento de um roteador</b>	<b>51</b>
<b>Figura 19 - Templates associados à um switch</b>	<b>52</b>
<b>Figura 20 - Tela de monitoramento de nobreaks</b>	<b>52</b>
<b>Figura 21 - Tráfego de dados em um dos roteadores de Internet</b>	<b>53</b>
<b>Figura 22 - Tela de monitoramento do servidor de e-mail do Sesc DN</b>	<b>54</b>
<b>Figura 23 - Monitores da infraestrutura na Coordenadoria de TI do Sesc DN</b>	<b>55</b>
<b>Figura 24 - Modos de autenticação de usuários no Zabbix</b>	<b>56</b>
<b>Figura 25 - Tela de configuração de servidor de e-mail no Zabbix</b>	<b>56</b>
<b>Figura 26 - Tela de configuração do endereço de e-mail de um usuário no Zabbix</b>	<b>57</b>
<b>Figura 27 - Dashboard principal do Zabbix com nenhum alerta ativo</b>	<b>58</b>
<b>Figura 28 - Tela do estado dos serviços principais da infraestrutura com nenhum alerta ativo</b>	<b>58</b>
<b>Figura 29 - Diagrama simplificado da rede do Sesc DN com nenhum alerta ativo</b>	<b>59</b>
<b>Figura 30 - Dashboard principal do Zabbix com alerta de falha em link de voz</b>	<b>59</b>
<b>Figura 31 - Tela do estado dos serviços principais com alerta na parte de Telefonía</b>	<b>60</b>
<b>Figura 32 - Tela personalizada de informações do Gateway de Voz com alerta ativo em um dos links</b>	<b>60</b>
<b>Figura 33 - Dashboard principal do Zabbix com alerta de falha em um link de Internet</b>	<b>61</b>
<b>Figura 34 - Tela do estado dos serviços principais com alerta na conexão principal com a Internet</b>	<b>61</b>
<b>Figura 35 - Diagrama simplificado da rede do Sesc DN com alerta ativo no roteador principal de Internet</b>	<b>62</b>
<b>Figura 36 - Dashboard principal do Zabbix com alerta de temperatura em um nobreak</b>	<b>62</b>
<b>Figura 37 - Tela do estado principal dos serviços da rede com alerta na parte de Infraestrutura</b>	<b>63</b>
<b>Figura 38 - Diagrama simplificado da rede do Sesc DN com alerta ativo em um dos nobreaks</b>	<b>63</b>
<b>Figura 39 - Monitor do estado dos principais serviços de TI do Sesc DN</b>	<b>64</b>
<b>Figura 40 - Diagrama de atividades em uma eventual falha na rede</b>	<b>65</b>

# **1     Introdução**

Em uma empresa de médio ou grande porte, a infraestrutura de TI é um elemento fundamental em seu processo produtivo. Acesso à rede interna e à Internet, e-mails e telefonia são alguns exemplos de serviços que a infraestrutura de TI fornece para seus usuários.

Com a oportunidade de analisar uma empresa com infraestrutura de TI em um nível elevado de maturidade, foi possível identificar que apesar dos esforços e da experiência da equipe de administradores, a rede possuía um aspecto que merecia especial atenção: o monitoramento da infraestrutura em si.

Várias questões cotidianas começaram a motivar este trabalho. Algumas delas:

- Como garantir uma infraestrutura confiável se não é possível saber o que está acontecendo?
- Como saber se houve algum problema em um dispositivo?
- Como saber as áreas da infraestrutura que necessitam de mais investimentos?
- Como saber se as concessionárias estão oferecendo os serviços prometidos?
- Como obter um histórico de eventos para auditar problemas na infraestrutura?

Apesar de existirem várias técnicas e sistemas que auxiliem no gerenciamento de uma rede, esta não é uma tarefa trivial, principalmente quando levamos em consideração a complexidade da infraestrutura de TI de uma empresa.

## **1.1   Objetivos do trabalho**

O objetivo desse projeto foi, através de um levantamento de requisitos de monitoramento e análise de ferramentas disponíveis no mercado, implementar um sistema de monitoramento de TI que atendesse as necessidades e se encaixasse melhor no cenário da empresa estudada.

Para isso, várias outras tarefas , ou sub-objetivos estavam presentes:

- Analisar o ambiente da empresa e levantar requisitos de monitoramento
- Pesquisar as ferramentas de monitoramento existentes no mercado
- Verificar os principais recursos de cada ferramenta
- Testar as ferramentas mais relevantes
- Implementar a ferramenta escolhida em ambiente de produção
- Configurar a ferramenta para abranger toda a infraestrutura do ambiente
- Encontrar maneiras de realizar a exibição dos dados de forma amigável
- Configurar alertas de prevenção contra problemas
- Validar a implementação do sistema
- Realizar documentação para que a equipe de TI possa atualizar e manter a ferramenta em utilização

## **1.2 Estrutura organizacional do texto**

O documento está organizado de acordo com os seguintes capítulos:

O capítulo 2 começa com uma breve descrição dos principais modelos de referência de gerenciamento de TI. São apresentadas também algumas das ferramentas de gerenciamento estudadas neste projeto.

O capítulo 3 apresenta informações e estatísticas sobre a empresa na qual o projeto se baseou. São definidos os requisitos de monitoramento da infraestrutura de TI da instituição, e também é mencionada a solução utilizada anteriormente.

O capítulo 4 descreve o sistema de monitoramento escolhido para ser implementado na empresa, assim como seus recursos, diferenciais e vantagens em relação às outras ferramentas disponíveis no mercado.

O capítulo 5 faz a análise da implementação do sistema no cenário da empresa estudada. A análise engloba a parte de testes, tomada de decisões, instalação, integração e configuração do sistema.

O capítulo 6 trata da validação da implementação da ferramenta de monitoramento através de testes e simulações, de forma a garantir sua eficácia.

O capítulo 7 relata o impacto que a nova ferramenta provocou da equipe de infraestrutura de TI e descreve alguns exemplos.

O capítulo 8 por fim apresenta as conclusões que foram obtidas com a execução deste projeto e possíveis trabalhos futuros.

## 2 Fundamentos de Gerenciamento de TI

### 2.1 Modelos de referência de gerenciamento

#### 2.1.1 FCAPS

FCAPS é um modelo de gerência de rede criado pela ISO (International Organization for Standardization) para auxiliar no entendimento das principais funções de sistemas de gerenciamento de redes. São elas [1]:

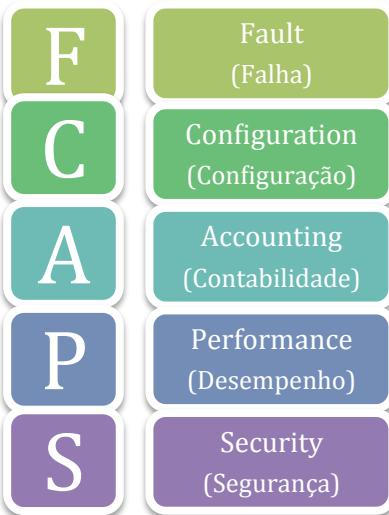


Figura 1 - Áreas conceituais do modelo FCAPS

Através do Modelo Básico de Referência do Modelo OSI (ISO/IEC 7498-4) [2], podemos fazer a definição destas cinco áreas:

##### 2.1.1.1 *Gerenciamento de falha*

O gerenciamento de falha engloba: detecção da falha, isolamento e correção de operações anormais do ambiente OSI. Falhas causam sistemas abertos a não conseguirem atingir seus objetivos operacionais, e elas podem ser constantes ou momentâneas. Falhas se manifestam em eventos particulares, como erros, na operação de um sistema aberto. A detecção de erros fornece a capacidade de identificar falhas. Funções do gerenciamento de falhas incluem [2]:

- Manter e examinar logs de erros
- Agir de acordo com notificações de detecção de erros
- Rastrear e identificar falhas

- Realizar sequências de testes de diagnóstico
- Corrigir falhas

#### ***2.1.1.2 Gerenciamento de configuração***

O gerenciamento de configuração identifica, exerce controle, coleta e fornece dados para sistema abertos com o objetivo de preparar, inicializar, prover a contínua operação e terminar serviços de interconexão. Funções do gerenciamento de configuração incluem [2]:

- Definir os parâmetros que controlam a operação cotidiana do sistema aberto
- Associar nomes com objetos gerenciados e conjuntos de objetos gerenciados
- Inicializar e encerrar objetos gerenciados
- Coletar informações da demanda sobre o estado atual do sistema aberto
- Obter informações sobre mudanças significativas no estado do sistema aberto
- Alterar a configuração do sistema aberto

#### ***2.1.1.3 Gerenciamento de contabilidade***

O gerenciamento de contabilidade possibilita que sejam estabelecidas cobranças pelo uso dos recursos no ambiente OSI, e que os custos sejam identificados. Funções do gerenciamento de contabilidade incluem [2]:

- Informar aos usuários sobre custos gerados ou recursos consumidos
- Possibilitar que sejam estabelecidos limites de contabilidade e tarifas diferenciadas associadas ao uso dos recursos
- Permitir que os custos sejam combinados quando múltiplos recursos forem requisitados para alcançar um determinado objetivo de comunicação

#### **2.1.1.4 Gerenciamento de desempenho**

Para permitir a avaliação do comportamento dos recursos no ambiente OSI, assim como a eficácia nas atividades de comunicação, existe o gerenciamento de desempenho. Suas funções incluem [2]:

- Coletar informações estatísticas
- Manter e examinar logs dos estados do sistema
- Determinar o desempenho do sistema sob condições naturais e artificiais
- Modificar os modos de operação do sistema com o objetivo de conduzir atividades de gerenciamento de desempenho

#### **2.1.1.5 Gerenciamento de segurança**

O objetivo do gerenciamento de segurança é apoiar a aplicação de políticas de segurança através de funções que incluem [2]:

- A criação, deleção e controle de serviços e mecanismos de segurança
- A distribuição de informações de segurança
- A descrição de eventos relacionados à segurança

### **2.1.2 TMN**

Os princípios de uma TMN (Telecommunications Management Network) foram criados para atender diversos dos problemas fundamentais que envolviam o gerenciamento de redes de telecomunicações.

Ela fornece uma estrutura para categorizar a rede gerenciada de acordo com entidades físicas ou funcionais, e de acordo com interfaces e pontos de referência [3].

O conceito básico por trás de uma TMN é fornecer uma arquitetura organizada para alcançar a interconexão entre os vários tipos de sistemas operacionais e equipamentos de telecomunicações para a troca de informações de gerenciamento usando uma arquitetura pré-estabelecida com interfaces padronizadas, incluindo protocolos e mensagens [4] .

A introdução das TMNs fornece aos operadores de telecomunicações a possibilidade de alcançar uma série de metas de gerenciamento, incluindo a capacidade de [4]:

- Diminuir o tempo de reação à eventos na rede
- Diminuir a sobrecarga causada pelo gerenciamento de tráfego onde a rede de telecomunicações é usada para transmiti-lo
- Permitir a dispersão geográfica do controle sobre aspectos da operação da rede
- Fornecer mecanismos de isolamento para minimizar riscos de segurança
- Fornecer mecanismos de isolamento para localizar e conter problemas da rede
- Melhorar a assistência ao serviço e a interação com os clientes

A implementação dos princípios porém, se tornou muito lenta principalmente por causa da complexidade dos sistemas legados. Conforme a área das telecomunicações segue evoluindo, estas dificuldades começam a ser superadas [3].

### **2.1.3 ITIL**

Durante a década de 1980, para responder à crescente dependência em TI, o governo do Reino Unido desenvolveu um conjunto de recomendações. Sem práticas padrões, empresas privadas e agências do governo haviam começado a desenvolver suas próprias práticas de gerenciamento de TI independentemente [5].

No início dos anos 1990 já haviam sido produzidos uma série de livros documentando a postura que o gerenciamento de TI precisava ter para atender os usuários corporativos. Esta biblioteca de práticas foi intitulada de IT Infrastructure Library (ITIL).

A intenção do ITIL é entregar valor ao negócio. Isto se torna possível através de sua composição – uma postura de senso comum ao gerenciamento de serviços.

A seguir estão algumas das características que contribuem para que o ITIL seja um sucesso mundial [5]:

- Não-proprietário: As práticas de gerenciamento de serviços do ITIL são aplicáveis à qualquer empresa pois não se baseiam em uma plataforma de tecnologia particular, nem em um tipo de indústria específica. O ITIL pertence ao governo do Reino Unido e não está vinculado a qualquer prática proprietária comercial.
- Não-prescritivo: O ITIL oferece práticas robustas e maduras que têm aplicabilidade para todos os tipos de instituições. Ele continua a ser útil e importante nos setores públicos e privados, e empresas de pequeno, médio e grande porte, em qualquer ambiente técnico.
- Melhor prática: As práticas do ITIL representam as experiências de aprendizagem e de lideranças de pensamento dos principais provedores de serviços do mundo.
- Boa prática: Nem toda prática no ITIL pode ser considerada como melhor prática. Muitos consideram que uma mistura entre práticas comuns, boas e melhores é o que dá significado ao gerenciamento de serviços de TI.

## 2.2 Arquiteturas para gerenciamento de TI

### 2.2.1 SNMP

O SNMP (Simple Network Management Protocol) foi apresentado em 1988 para atender a crescente demanda por um protocolo que pudesse gerenciar dispositivos IP. Ele fornece aos seus usuários um conjunto de operações simples que permite que estes dispositivos possam ser administrados remotamente [1].

O essência do SNMP é um simples conjunto de operações que dá aos administradores o poder de alterar o estado de algum dispositivo que suporte o protocolo. É possível utilizar o SNMP para verificar a velocidade do tráfego em uma determinada porta de um switch, ou monitorar a temperatura de um roteador, por exemplo.

É importante entender que o SNMP pode ser utilizado para administrar diversos tipos de equipamentos, e não apenas roteadores como normalmente se pensa. O protocolo pode gerenciar sistemas Unix, Windows, impressoras, roteadores, switches, nobreaks, modems, entre outros.

A IETF (Internet Engineering Task Force) é a responsável por definir os protocolos que regem o tráfego da Internet, inclusive o SNMP. Ela regularmente publica RFCs (Requests for Comments), que são especificações para muitos protocolos que existem na área de redes. Existem hoje três versões do SNMP definidas pela IETF:

- SNMPv1: é a versão inicial do protocolo SNMP. A segurança é baseada em communities, que não passam de simples senhas em texto puro, e que permitem acesso à qualquer aplicação baseada em SNMP e assim ao gerenciamento de informação do dispositivo. Nesta primeira versão do SNMP existem três communities: read-only (somente leitura), read-write (leitura e escrita), e trap. Embora esta versão seja histórica, muitas vezes é a única implementação de SNMP que vários fornecedores oferecem.
- SNMPv2: também conhecida como SNMPv2c ou community-string-based.
- SNMPv3: é a última versão do SNMP. Traz vários avanços nas partes de segurança em gerenciamento de redes. Oferece autenticação segura e comunicação privada entre entidades administradas. Em 2002 deixou de ser um 'draft' (protocolo em rascunho) e passou a ser uma versão de fato estabelecida.

### 2.2.2 ICMP

ICMP (Internet Control Message Protocol) é um protocolo de controle que faz parte do protocolo IP. Quando algo não esperado ocorre durante o processamento de um pacote em um roteador qualquer, o remetente recebe um aviso por ICMP.

Existem vários tipos de mensagens ICMP e cada uma é encapsulada em um pacote IP. As mais importantes [6] estão listadas na Tabela 1:

Tipo de Mensagem	Descrição
<b>Destination unreachable</b>	Não foi possível entregar um pacote IP ao destino
<b>Time exceeded</b>	O TTL do pacote expirou e ele foi descartado
<b>Parameter problem</b>	Pacote descartado por erro no cabeçalho
<b>Source quench</b>	Falta de espaço no buffer de recepção que causa o descarte do pacote e gera uma mensagem de aviso ao remetente
<b>Redirect</b>	Pacote é redirecionado quando surge uma rota melhor
<b>Echo request/reply</b>	Mensagens geradas pelo comando ping
<b>Timestamp request/reply</b>	Requisição/resposta sobre o horário atual em outro sistema

Tabela 1 - Principais tipos de mensagens do ICMP

Existem algumas utilitários de administração de redes tal como o “ping” que é utilizado para testar o alcance à um host em uma rede IP e para medir o atraso (RTT) na comunicação. Isto é feito enviando pacotes “echo request” para o alvo e aguardando uma resposta ICMP.

Podemos ver o resultado de um simples comando “ping” para o site da RedeRio:

```

PING www.rederio.br (152.84.253.9): 56 data bytes
64 bytes from 152.84.253.9: icmp_seq=0 ttl=54 time=7.891 ms
64 bytes from 152.84.253.9: icmp_seq=1 ttl=54 time=10.336 ms
64 bytes from 152.84.253.9: icmp_seq=2 ttl=54 time=10.093 ms
64 bytes from 152.84.253.9: icmp_seq=3 ttl=54 time=7.177 ms
64 bytes from 152.84.253.9: icmp_seq=4 ttl=54 time=9.688 ms
^C
--- www.rederio.br ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 7.177/9.037/10.336/1.265 ms

```

Outro utilitário que faz uso de mensagens ICMP é o “traceroute”. Ele serve para diagnosticar a rota e o atraso dos pacotes em uma rede IP. O caminho da rota é registrado e o RTT dos pacotes é recebido para cada nó do caminho.

A seguir temos o resultado da execução de um comando traceroute ao site da RedeRio:

```
traceroute to www.rederio.br (152.84.253.9), 64 hops max, 52 byte
packets
 1  192.168.1.1 (192.168.1.1)  3.878 ms  0.826 ms  0.685 ms
 2  173.251.40.189.isp.timbrasil.com.br (189.40.251.173)  5.935 ms
 155.760 ms  6.180 ms
 3  10.223.239.161 (10.223.239.161)  6.647 ms
    10.223.239.193 (10.223.239.193)  6.509 ms  6.494 ms
 4  10.223.229.33 (10.223.229.33)  13.647 ms  10.244 ms
    10.223.238.145 (10.223.238.145)  7.715 ms
 5  10.223.255.201 (10.223.255.201)  10.056 ms  7.681 ms  7.672 ms
 6  10.223.238.237 (10.223.238.237)  12.998 ms  7.779 ms  8.023 ms
 7  as1916.rj.ptt.br (200.219.138.101)  7.511 ms  14.604 ms  17.262 ms
 8  mxrj-rederio-1g-int.bkb.rnp.br (200.143.254.137)  140.602 ms
 8.299 ms  7.879 ms
 9  200.20.92.182 (200.20.92.182)  9.066 ms  7.767 ms  7.869 ms
10  152.84.49.1 (152.84.49.1)  8.170 ms  7.912 ms  7.835 ms
11  cbpfsu6.cat.cbpf.br (152.84.253.9)  7.589 ms  7.483 ms  7.445 ms
```

### 2.2.3 NetFlow

NetFlow é um recurso que foi introduzido nos roteadores da Cisco com a função de possibilitar a coleta de informações sobre o tráfego IP conforme ele passa por uma interface [7].

Ele pode ser utilizado por profissionais de TI para analisar o fluxo e o volume de tráfego da rede e determinar de onde o tráfego vem, seu destino, e a quantidade de tráfego sendo gerado. Roteadores e switches que suportam o NetFlow exportam as estatísticas de tráfego que então são recuperadas por um coletor NetFlow. É o coletor que de fato faz a análise do fluxo de tráfego e apresenta as informações obtidas.

O NetFlow fornece aos administradores da rede os seguintes principais recursos [8].

- Monitoramento da banda
- Análise do tráfego
- Gerência de segurança da rede
- Validação de QoS
- Previsão e planejamento de capacidade
- Identificação de ameaças (vírus, malwares)
- Análise de tráfego remoto (VPN)

Com as informações obtidas pelo NetFlow, um administrador consegue entender do que é composto o tráfego de sua rede, e assim se torna mais fácil a identificação de aplicativos ou usuários que estejam abusando do consumo de banda, os principais protocolos em uso, e os usos para o tráfego de saída e para o tráfego de entrada.

#### 2.2.4 Netconf

O protocolo Netconf (Network Configuration Protocol) define um simples mecanismo pelo qual um dispositivo de rede pode ser gerenciado, informações de configuração podem ser obtidos, e novas configurações podem ser enviadas e manipuladas [9].

O protocolo utiliza um paradigma RPC (Remote Procedure Call). Um cliente codifica uma RPC em XML e a envia utilizando uma sessão segura. O servidor envia uma resposta também codificada em XML.

Um ponto principal do Netconf é que ele possibilita que a funcionalidade do protocolo de gerenciamento seja muito próxima da funcionalidade nativa do dispositivo. Isto reduz os custos de implementação e permite acesso rápido aos novos recursos.

Na Figura 2, temos um diagrama da divisão conceitual do Netconf em quatro camadas [9]:

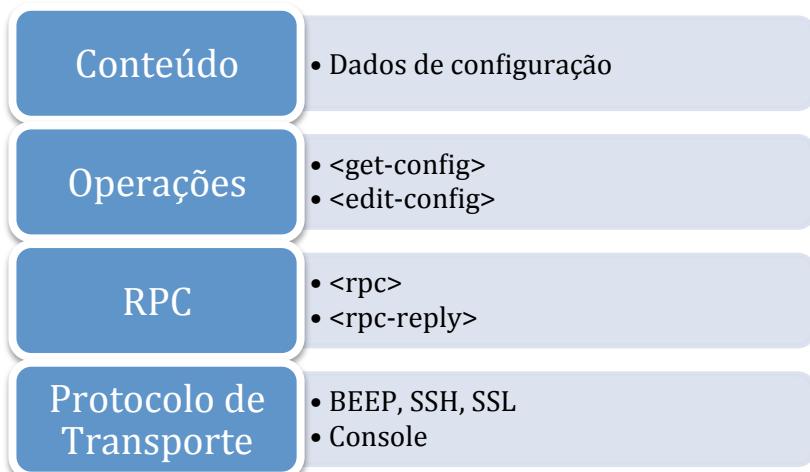


Figura 2 - Diagrama de camadas do Netconf

O protocolo de transporte fornece um caminho de comunicação entre o cliente e o servidor. A camada RPC provê um simples mecanismo de

encapsulamento para codificar RPCs. A camada de operações define um conjunto de operações-base que são chamadas com parâmetros codificados em XML. E por último, a camada de conteúdo, que consiste em dados de configuração e de notificação.

## 2.3 Ferramentas de gerência

Existem diversos sistemas de monitoramento de dispositivos, serviços e de análise de tráfego que ajudam que os administradores de TI tenham um controle maior sobre a rede.

A seguir estão listadas algumas das ferramentas mais populares, que foram pesquisadas e avaliadas para a execução deste projeto, e que se baseiam no modelo FCAPS de gerência de rede [10], modelo este que se destacou como mais relevante ao cenário da empresa analisada neste trabalho.

### 2.3.1 Cacti

O Cacti é um sistema open-source para monitoramento de rede. Sua interface web permite a utilização por múltiplos usuários, cada um com seu próprio conjuntos de permissões.

Dentre os principais recursos da ferramenta estão:

- Manipulação de dados em gráficos
- Suporte à SNMP
- Templates para gráficos
- Templates para fontes de dados
- Templates para dispositivos
- Autenticação através de outros sistemas como Active Directory ou LDAP

### 2.3.2 Icinga

O Icinga também é um sistema open-source para monitoramento da infraestrutura. Conta com uma interface avançada ao usuário baseada em Web 2.0, e permite a integração com diversos tipos de banco de dados, tais como PostgreSQL, MySQL e Oracle). O Icinga é um fork do Nagios, outro sistema de

monitoramento, e possui retrocompatibilidade com seus plug-ins, configurações e add-ons.

Suas principais características incluem:

- Monitoramento de serviços de rede
- Monitoramento de recursos de dispositivos
- Monitoramento de componentes de servidores
- Notificação de usuários sobre falhas por vários métodos
- Criação de relatórios
- Criação de gráficos de performance através de plug-ins

### **2.3.3 InterMapper**

Outro sistema de monitoramento da infraestrutura de TI é o InterMapper. É um programa multiplataforma que tem a capacidade de realizar diversas verificações de rede baseadas em ICMP, SNMP, HTTP e outros protocolos. No entanto, não se trata de um software gratuito.

O software conta com os seguintes recursos:

- Mapeamento em tempo real da rede
- Autodescoberta de dispositivos
- Monitoramento de banda
- Suporta o monitoramento de até 1000 dispositivos
- Criação de alertas
- Análise de tendências

### **2.3.4 Nagios**

Um dos mais famosos e tradicionais sistemas de monitoramento de TI é o Nagios. É uma solução gratuita e de código aberto, desenvolvida para ser executada em Linux. Um dos pontos negativos é sua interface web, que com o passar dos anos se tornou desatualizada e pouco amigável, principalmente para a configuração do sistema.

Suas características principais são:

- Monitoramento de serviços de rede
- Monitoramento de recursos de dispositivos
- Monitoramento de sensores
- Diversos plug-ins criados pela comunidade
- Notificação de usuários sobre falhas por vários métodos
- Possibilidade de armazenar dados em arquivos de texto ao invés de banco de dados

### **2.3.5 Opsview**

O Opsview é um outro sistema de gerência de TI para infraestrutura física, virtual e baseada na nuvem. Apesar do software ser pago, a empresa oferece uma versão gratuita de código aberto direcionada à desenvolvedores.

Seus principais recursos incluem:

- Painéis para facilitar a visualização de informações da rede
- Autodescoberta de dispositivos
- Geração de relatórios
- Monitoramento de serviços de rede

### **2.3.6 Pandora FMS**

Inicialmente lançado em 2004, o Pandora FMS é mais uma solução de monitoramento de redes de computadores. Assim como o OpsView, possui uma versão gratuita e open-source, porém mais básica.

Dentre suas principais características estão:

- Alta escalabilidade através de instalações independentes
- Testes de disponibilidade através de ICMP, SNMP, HTTP e outros
- Monitoramento de tráfego
- Autenticação através de outros sistemas como Active Directory ou LDAP

- Armazenamento de dados históricos para análise
- Geração de relatórios personalizados

### **2.3.7 SolarWinds**

A SolarWinds é uma empresa que desenvolve diversos softwares para gerenciamento da infraestrutura de TI. As ferramentas são proprietárias e seus preços iniciais giram em torno de 3000 dólares.

Uma das ferramentas mais interessantes é o Network Performance Monitor, e seus principais recursos são:

- Detecção automática de dispositivos
- Suporte nativo à diferentes tipos de marcas de dispositivos
- Monitoramento do estado geral da saúde da rede
- Alertas em tempo real
- Geração de relatórios
- Monitoramento de sensores
- Suporte à SNMP

### **2.3.8 Zabbix**

Lançado inicialmente ao público em 2001, o Zabbix se tornou referência entre as ferramentas de gerência de TI existentes no mercado. O sistema é gratuito e conta com as seguintes características:

- Capacidade de monitorar milhares de dispositivos
- Autodescoberta de servidores e dispositivos de rede
- Administração web centralizada
- Agentes de monitoramento para diversas plataformas
- Monitoramento sem agente
- Monitoramento web
- Monitoramento SNMP
- Monitoramento de banco de dados

- Monitoramento de máquinas virtuais
- Criação de mapas, gráficos e telas personalizadas
- Autenticação através de outros sistemas como Active Directory ou LDAP
- Estipulação de métricas
- Notificação de usuários sobre falhas por vários métodos

### 2.3.9 Comparação das ferramentas de gerência

Na Tabela 2, é feita a comparação de algumas das principais características dos sistemas de gerenciamento de TI testados. É importante ressaltar que apesar de um sistema possuir determinado recurso, sua facilidade de uso e eficiência variam significativamente de um para o outro.

	Gratuito	SLA	Autodescoberta	Agentless	SNMP	Plug-ins	Alertas	Mapas	LDAP
<b>Cacti</b>	Sim	Sim	Plug-in	Sim	Sim	Sim	Sim	Plug-in	Sim
<b>Icinga</b>	Sim	Plug-in	Plug-in	Sim	Plug-in	Sim	Sim	Sim	Sim
<b>Intermapper</b>	Não	Sim	Sim	Não	Sim	Sim	Sim	Sim	Sim
<b>Nagios</b>	Sim	Plug-in	Plug-in	Sim	Plug-in	Sim	Sim	Sim	Não
<b>Opsview</b>	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
<b>PandoraFMS</b>	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
<b>SolarWinds</b>	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
<b>Zabbix</b>	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tabela 2 - Comparação de algumas das principais características dos sistemas testados

### **3 Cenário de Aplicação da Solução de Gerenciamento de TI**

#### **3.1 Sobre a empresa**

O Sesc (Serviço Social do Comércio) é uma instituição privada, sem fins lucrativos, mantida pelos empresários do comércio de bens e serviços. Com o auxílio de recursos públicos, atua em todo o território nacional nas áreas da educação, saúde, cultura e lazer através de seus vários Departamentos Regionais distribuídos pelos estados do país [11].

O Departamento Nacional (DN) do Sesc por sua vez, é um órgão normativo que elabora as diretrizes gerais da entidade e suas políticas de ações para os programas institucionais. Ele também é responsável por prestar apoio aos Departamentos Regionais, inclusive na área de Tecnologia da Informação.

O campus do DN está localizado na Barra da Tijuca - Rio de Janeiro e opera em horário comercial. Porém alguns setores possuem esquema de plantão (como é o caso da Coordenadoria de TI) por serem responsáveis por serviços críticos.

#### **3.2 Números e estatísticas**

O Sesc Departamento Nacional conta com 480 funcionários. Na Coordenadoria de TI da empresa estão 30 pessoas, entre desenvolvedores, analistas de banco de dados, analistas de infraestrutura e analistas de suporte. Na equipe de infraestrutura especificamente estão alocadas 10 pessoas.

A empresa conta com aproximadamente 400 computadores e notebooks utilizados por seus funcionários, 400 ramais distribuídos entre telefones IP e softphones, e 100 servidores de aplicações que hospedam os sistemas da instituição.

#### **3.3 Estrutura da rede**

A infraestrutura física do complexo onde a instituição se encontra pode ser considerada como nova, principalmente se comparada com a realidade da maioria das outras empresas da cidade. São construções recentes, concluídas por volta de 2006 e planejadas para receber uma infraestrutura de TI.

O complexo é dividido em vários blocos, identificados por letras. Cada bloco tem seu próprio prédio e vários andares. Na Figura 3 temos um diagrama da divisão física do espaço da empresa:



**Figura 3 - Diagrama de blocos do Sesc Departamento Nacional (azuis e brancos)**

A maioria dos andares de cada bloco possui uma sala chamada de “Teleinfo” com equipamentos de rede, geralmente apenas switches, que ligam os computadores e outros dispositivos das salas próximas à ela até o Datacenter.

A seguir temos um exemplo de sala de Teleinfo. Note que do lado direito encontram-se os equipamentos do Sesc DN: alguns switches e patch panels.

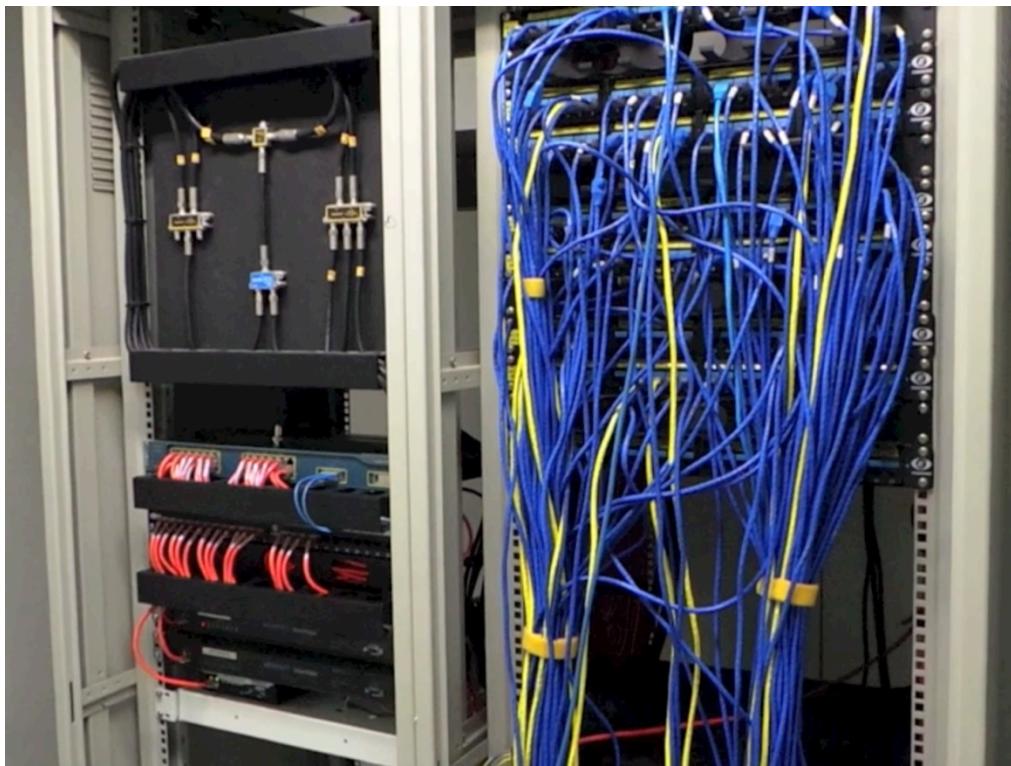


Figura 4 – Interior de uma das salas de Teleinfo do Sesc DN

O datacenter principal se localiza no subsolo do bloco K. Nele temos um switch core que liga todas as salas de Teleinfo à rede, roteadores de Internet e Intranet com links fornecidos pela Embratel, um roteador de Videoconferência que permite a transmissão por um link de satélite fornecido pela Telespazio, três links E1 de telefonia fornecidos pela Embratel, servidores para virtualização com a solução BladeCenter da IBM (utilizados em sua maioria para aplicações web, e-mail, serviços internos), servidores de armazenamento, e servidores de telefonia da Cisco.

Na Figura 5 podemos visualizar a solução de virtualização de servidores da IBM. Com ela, em um pequeno espaço físico, a empresa administra dezenas de servidores virtualizados. Na Figura 6 temos uma imagem do switch principal da empresa, também localizado no datacenter principal.



Figura 5 – Servidores virtualizados no datacenter principal do Sesc DN

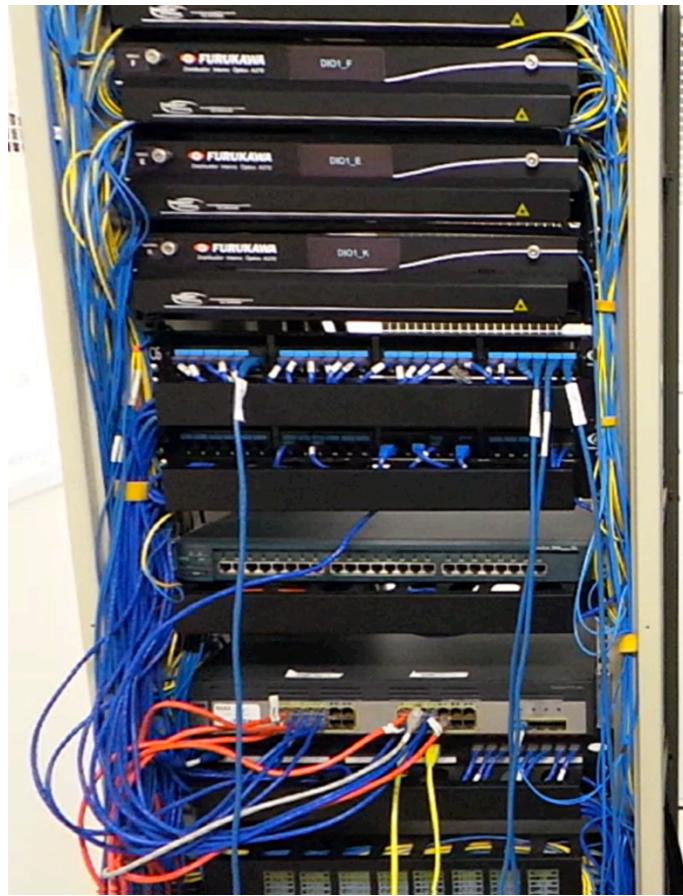


Figura 6 - Switch core no datacenter principal do Sesc DN

A empresa valoriza a questão da redundância. Existe em um local físico separado, um datacenter secundário. Nele está um espelho dos servidores virtualizados, e um roteador secundário de Internet. Caso alguma falha ocorra no datacenter principal, é possível ativar os servidores de contingência, assim como redirecionar o tráfego de Internet para o roteador secundário. A Figura 7 mostra o ambiente do datacenter secundário.

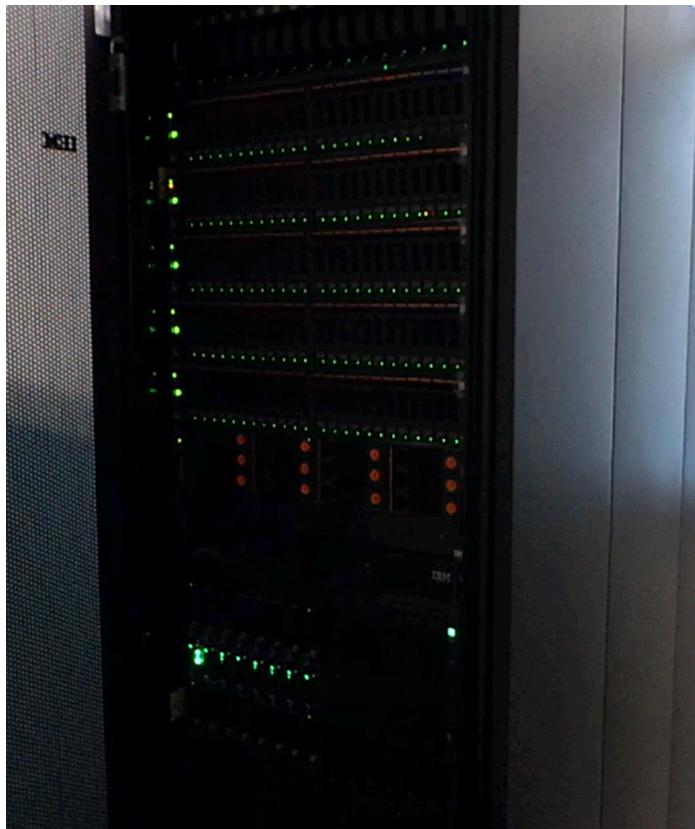
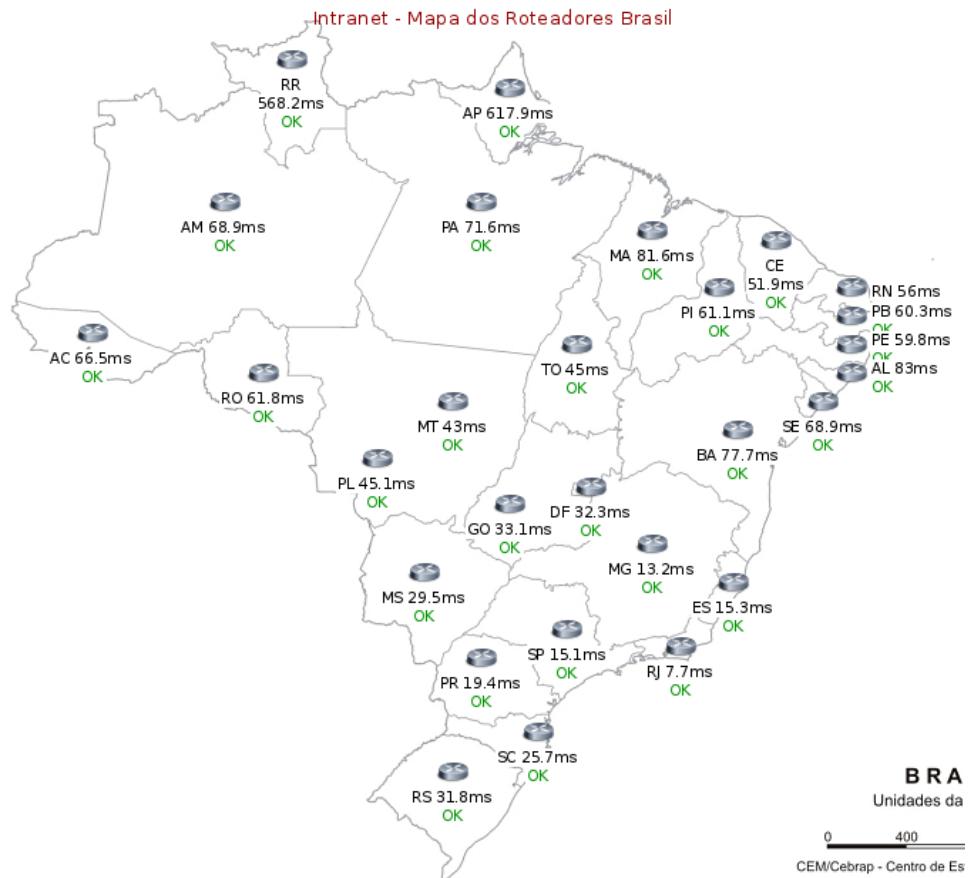


Figura 7 - Servidores de contingência no datacenter secundário do Sesc DN

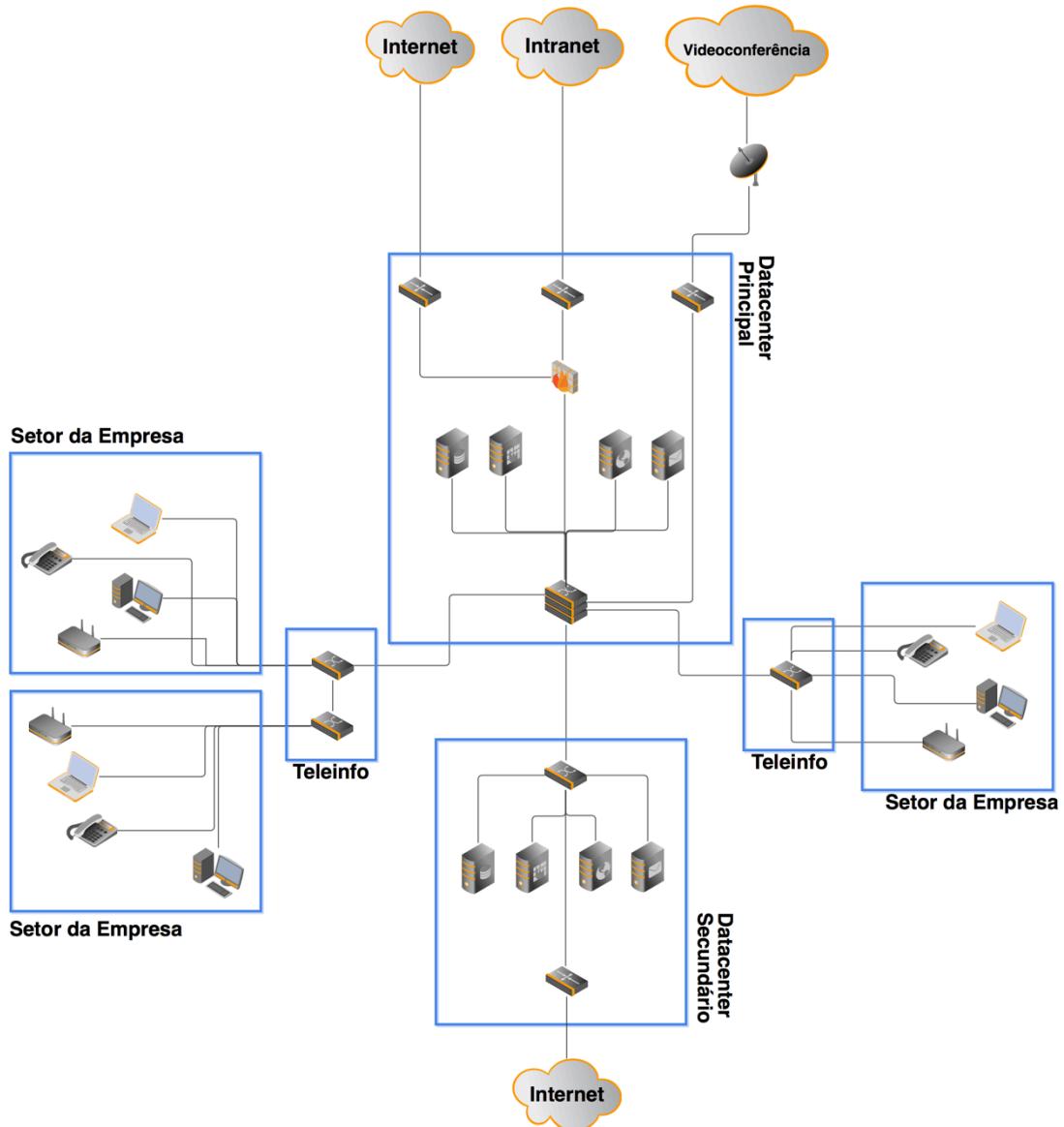
Em cada estado do Brasil existe um Departamento Regional (DR) do Sesc, cada um com um Roteador de Intranet, que interliga todos os DRs com o Departamento Nacional. Essa rede é muito utilizada para troca de e-mails corporativos, troca de arquivos (principalmente via FTP), e videoconferência.

Na Figura 8, podemos ver um mapa de monitoramento em tempo real gerado pelo Zabbix (ferramenta de gerência de TI que será detalhada no próximo capítulo) com os roteadores de Intranet dos Departamentos Regionais no Brasil.



**Figura 8 - Mapa do estado dos roteadores de Intranet do Sesc DN**

É possível afirmar que não se trata de uma empresa com uma infraestrutura de TI trivial, e isto aumenta ainda mais a necessidade por uma solução de gerenciamento eficaz. Na Figura 9 temos um simples esquema da infraestrutura de TI da empresa:



**Figura 9 - Diagrama da infraestrutura de TI do Sesc DN**

A ferramenta de gerência de TI se localizaria no datacenter principal, entre o firewall e o switch core, junto com os outros servidores virtualizados da empresa.

### 3.4 Requisitos de monitoramento

As necessidades de gerenciamento da infraestrutura na empresa eram diversas. A seguir estão os principais requisitos de monitoramento do cenário da instituição.

### **3.4.1 Conexão com a Internet**

A empresa depende da Internet para diversas tarefas. O envio e recebimento de e-mail, a disponibilidade de sistemas para o público, o acesso à páginas web, a comunicação através de mensagens instantâneas, e a hospedagem do site da empresa são exemplos de atividades diárias dependentes da Internet.

Existem dois roteadores de Internet com link oriundos de lugares diferentes para garantir a disponibilidade do serviço. Para garantir que a conexão da rede com a Internet não seja afetada, é preciso monitorar ambos os roteadores.

### **3.4.2 Conexão com a Intranet**

A instituição possui uma rede MPLS de Intranet que engloba os Departamentos Regionais. Essa rede é essencial para a troca de e-mails corporativos, transferência de arquivos e videoconferência.

É necessário monitorar o roteador de Intranet para garantir que todos os DRs estejam conectados sem problemas à rede, e verificar se a concessionária está fornecendo o serviço prometido.

### **3.4.3 Conexão com o satélite de videoconferência**

Existe um link de satélite contratado pela empresa que é utilizado para a transmissão de eventos da instituição, assim como videoconferências nacionais. Para garantir que o serviço está disponível mesmo quando não está em uso, é importante monitorá-lo.

### **3.4.4 Conexão com o serviço de telefonia**

Todo o sistema de telefonia da empresa é baseado em uma solução VoIP da Cisco. Além de todo os servidores que compõem o sistema, é preciso garantir que os três links de voz fornecidos pela concessionária estejam operantes. Para isso, é preciso monitorar os servidores do CallManager e o gateway que trata da conexão com os links E1 de voz.

### **3.4.5 Estado dos switches locais**

O Sesc DN possui dezenas de switches espalhados pelo complexo que são responsáveis por fornecer acesso à rede para diversos setores da empresa. É de

extrema importância saber o quanto antes se algum deles apresentar algum tipo de problema, pois isto pode afetar toda a operação de uma parte da instituição.

A intenção do monitoramento é agir preventivamente, analisando o comportamento do dispositivo conforme o passar do tempo, mas também poder saber imediatamente se um equipamento está inoperante para substituí-lo o mais rápido possível e diminuir qualquer tipo de prejuízo ao negócio da empresa.

#### **3.4.6 Equipamentos de energia**

Existem outros equipamentos também importantes à infraestrutura de TI da empresa. Os nobreaks fornecem aos equipamentos essenciais da rede um fluxo contínuo de energia para que haja tempo do gerador ser ativado e não provocar nenhum tipo de interrupção dos serviços.

Alguns aspectos importantes de serem monitorados nestes equipamentos de energia são: temperatura, tempo de bateria, capacidade da bateria e estado de uso atual.

#### **3.4.7 Servidores e sistemas internos**

Não só equipamentos físicos precisam de atenção. Sistemas da empresa são vitais para seu negócio. Com base nisto é necessário verificar constantemente todas as aplicações da corporação e garantir que elas estejam funcionando corretamente, ou acionar a equipe adequada para providenciar os reparos.

### **3.5 Solução antiga**

Boa parte da infraestrutura de TI atende com folga as necessidades de seus clientes. Algumas outras requerem um pouco mais de atenção, como o serviço de telefonia, que é inteiramente dependente da rede interna e baseado em uma solução proprietária. Outro ponto mais delicado é a estabilidade dos links de Internet e Intranet fornecidos pela Embratel para a empresa.

Inicialmente a equipe de Infraestrutura da Coordenadoria de TI possuía dois grandes monitores em sua sala, cada um ligado à um computador. Um deles, ilustrado na Figura 10, mostrava informações obtidas por um sistema de

monitoramento bem conhecido: o Nagios. O segundo monitor informava dados obtidos por outro protocolo, o Netflow, proprietário da Cisco.

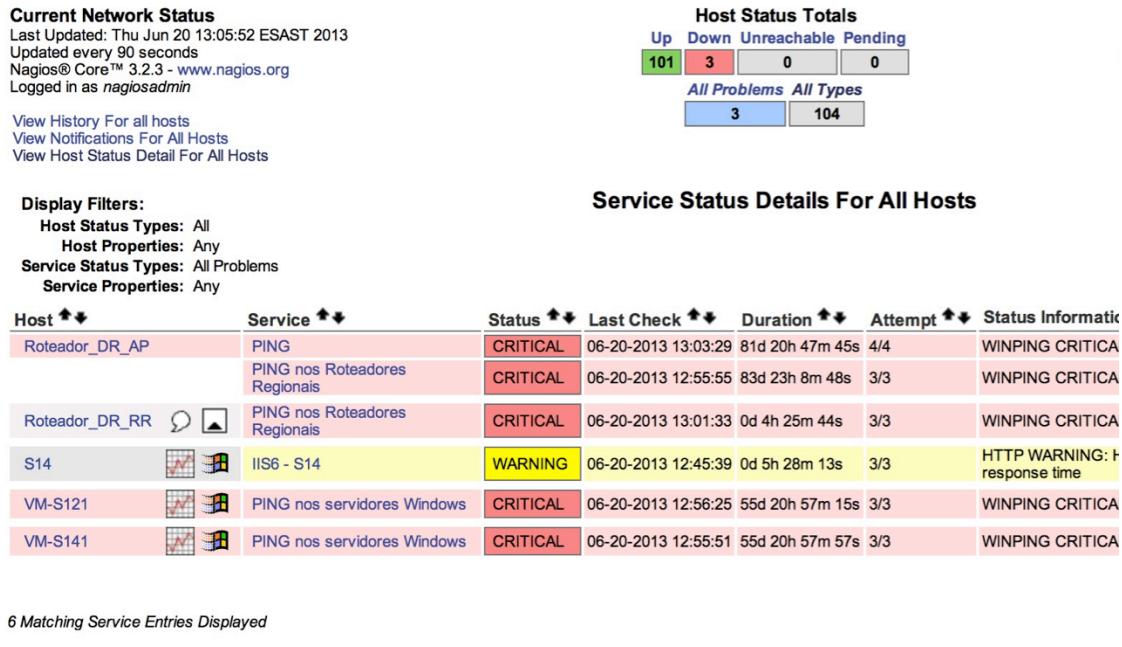


Figura 10 - Interface principal do Nagios utilizado anteriormente

Os dois sistemas falhavam em alguns sentidos:

- Eram de difícil configuração/manutenção – Os sistemas possuíam um nível de complexidade relativamente alto para administradores que não eram familiarizados com eles.
- Não monitoravam parte significativa da rede – Por causa da dificuldade em manter os sistemas de monitoramento, frequentemente novos dispositivos e serviços de rede não eram incluídos nas ferramentas, deixando-as gradativamente obsoletas.
- Não monitoravam aspectos mais profundos dos dispositivos – O monitoramento feito pelos sistemas em sua maioria era superficial. Por exemplo, era possível saber se um roteador de Intranet estava alcançável, mas não se tinha dados adicionais sobre ele, como o tráfego de dados.

- Não possuíam uma ferramenta de alertas eficiente – Os sistemas apresentavam regularmente problemas na exibição de alertas. Era comum um roteador estar sendo exibido na lista de alertas, mesmo que não houvesse qualquer tipo de problema.
- Não permitiam customização da maneira com que as informações eram mostradas (telas/gráficos/mapas) – As falhas eram de difícil visualização, sendo usados basicamente os painéis principais dos sistemas para obtenção de informações.

Para se ter uma ideia, com estes sistemas, poderia haver uma falha com qualquer um dos switches de qualquer bloco, e a equipe não saberia desse problema, muito menos, a localização do equipamento defeituoso. Isto tinha como origem a falta de atualização dos sistemas: apenas parte da infraestrutura estava configurada para ser monitorada, e a cobertura não era expandida devido ao elevado grau de dificuldade de manutenção desses sistemas.

Outro exemplo: A empresa possui dois roteadores de Internet. Os sistemas de monitoramento já existentes apenas monitoravam a conectividade com a rede externa através de um deles, ou seja, um dos links poderia falhar e a equipe não estaria ciente do ocorrido. Um caso de problemas na configuração das ferramentas.

## 4 Zabbix

O Zabbix é um software desenvolvido para monitorar a disponibilidade e desempenho de componentes da infraestrutura de TI de nível corporativo. Ele possui código livre, e é isento de custos [12].

Diversas empresas no Brasil são referência no uso do Zabbix como sistema de gerência de TI, dentre elas estão: Dataprev, Petrobras e Serpro [13].

É possível obter diferentes tipos de dados sobre a rede com a ferramenta. Podem ser monitorados simultaneamente milhares de servidores, máquinas virtuais e dispositivos de rede. Além de armazenar os dados obtidos, o Zabbix oferece diversas formas de visualizar as informações através de telas, mapas, gráficos e outros. O sistema também é muito flexível na questão da análise dos dados obtidos com a finalidade de criar alertas.

O Zabbix pode ser escalonado para ambientes muito grandes sem que seu desempenho seja afetado, através de servidores “proxies”. Ele já vem com uma interface web própria, assim como um sistema de autenticação bem flexível.

O monitoramento pode ser feito através de agentes instalados nos sistemas operacionais dos servidores desejados, mas também estão disponíveis outros meios de efetuar a coleta de dados sem que qualquer software precise ser instalado no alvo. Monitoramento web e de máquinas virtuais também são recursos nativos do Zabbix.

Dentre os pontos principais que levaram à escolha do Zabbix estão:

- Recursos da interface
- Facilidade na instalação, configuração, atualização e manutenção
- Farta documentação disponível na Internet
- Flexibilidade na customização de telas
- Software gratuito e livre
- Atualizações constantes fornecidas pelos desenvolvedores
- Implementação do Zabbix já realizada por outras empresas nacionais

Por se tratar de um sistema preventivo, o fato de ser gratuito ajuda bastante em sua aceitação por parte dos gerentes do departamento, e o desenvolvimento do projeto se torna mais fácil.

## 4.1 Recursos de monitoramento

### 4.1.1 Agente Zabbix de monitoramento

Os desenvolvedores do Zabbix criaram junto com o sistema, um agente de monitoramento. Esse agente, desenvolvido em C, é suportado em várias plataformas (incluindo Windows, Mac OS, e Linux), e é capaz de coletar dados sobre processador, memória, disco e interface de rede de um dispositivo. [14]

A princípio, uma das preocupações de se instalar um programa que não é “essencial” em um servidor é o fato de que ele poderia consumir recursos preciosos da máquina. Não é o que acontece neste caso. Nos testes realizados nos servidores da empresa, foi constatado um uso de CPU insignificativo, e uso memória por volta de 4MB em uma máquina com Microsoft Windows Server 2008, conforme ilustrado na Figura 11.

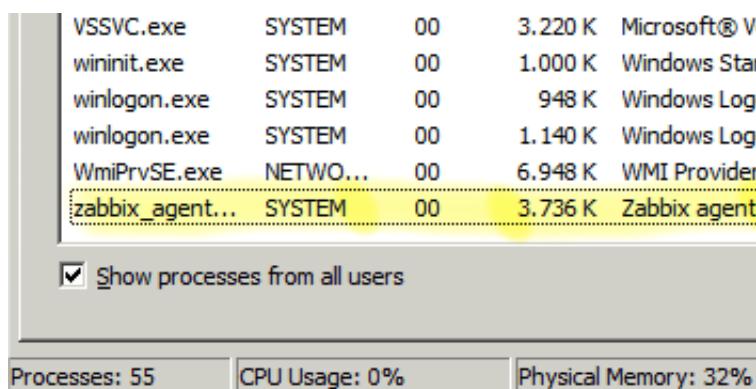


Figura 11 - Consumo de recursos do agente em um dos servidores do Sesc DN

O agente é capaz de gerenciar checagens passivas (polling) e ativas (trapping). Nas verificações passivas, a requisição parte do servidor Zabbix e atinge o agente da máquina sendo monitorada, que então responde com os dados coletados. No caso das verificações ativas, o agente requisita do servidor Zabbix uma lista de checagens ativas e envia os resultados periodicamente.

A Figura 12 e a Figura 13, desenvolvidas pelos criadores do Zabbix, ilustram como funcionam esses tipos de verificação.

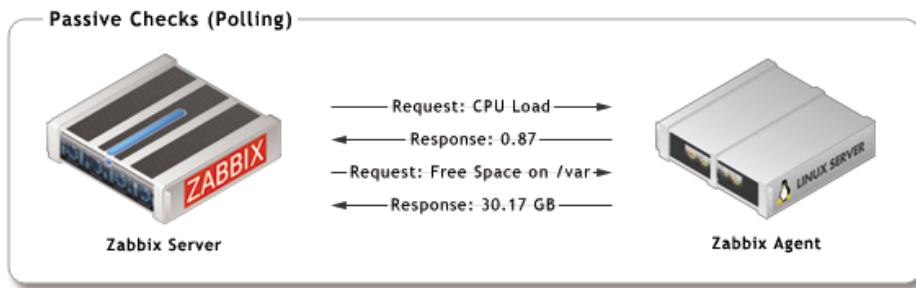


Figura 12 - Verificações passivas (comunicação começa do servidor Zabbix)

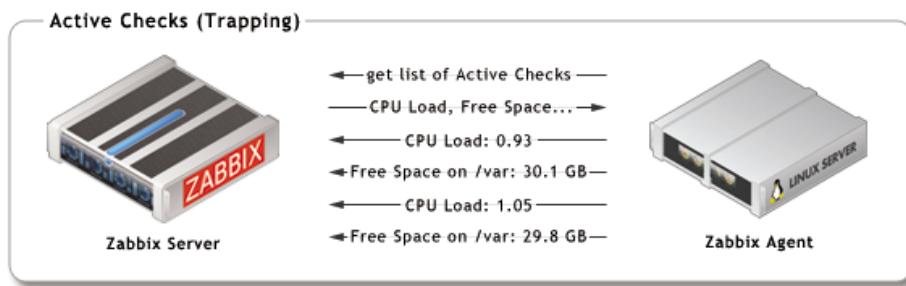


Figura 13 - Verificações ativas (comunicação começa do agente Zabbix)

O agente de monitoramento suporta diversos tipos de verificações nativamente, listados na Tabela 3, mas sua funcionalidade também pode ser ampliada através de módulos e parâmetros pelo usuário.

<b>Rede</b>	Pacotes/bytes transferidos Erros/pacotes descartados Colisões
<b>CPU</b>	Média de carga Uso/Tempo ocioso da CPU
<b>Memória</b>	Memória em uso/livre Utilização de swap/paginação
<b>Disco</b>	Espaço em uso/livre E/S de leitura e escrita
<b>Serviço</b>	Estado do processo Uso de memória do processo Estado do serviço (SSH, NTP, LDAP, SMTP, FTP, HTTP, POP, NNTP, IMAP) Estado de serviços Windows Resolução de DNS Conectividade TCP Tempo de resposta TCP
<b>Arquivo</b>	Tamanho de arquivo Existência de arquivo Soma de verificação (checksum) Hash MD5

	Pesquisa por expressão regular
Log	Log de texto
	Log de eventos do Windows
Outros	Tempo em atividade Tempo do sistema Usuários conectados Contadores de desempenho (Windows)

Tabela 3 - Funções de monitoramento do agente Zabbix

#### 4.1.2 Agente SNMP

O servidor Zabbix pode coletar dados de dispositivos que suportam SNMP (Simple Network Management Protocol). Esse tipo de monitoramento é particularmente interessante pois permite que sejam verificados diversos tipos de dispositivos de rede que não suportam o método de monitoramento mencionado no tópico anterior.

Isso significa que se torna possível a obtenção de informações de roteadores, switches, impressoras, nobreaks e vários outros, sem que seja necessária a instalação de qualquer programa adicional nesses dispositivos, visto que a maioria deles já vem com suporte ao protocolo SNMP de fábrica [15].

#### 4.1.3 Monitoramento sem agente

Também é possível no Zabbix efetuar o monitoramento de um host sem qualquer tipo de agente. Isto é útil quando não é possível alterar qualquer configuração de um servidor, muito menos instalar algum programa nele.

Contudo as informações que podem ser obtidas com este tipo de serviço são muito limitadas. Na Tabela 4 estão listadas as funções que o monitoramento sem agente proporciona [16]:

Serviços de Rede	Disponibilidade de porta TCP Tempo de resposta de porta TCP Verificação de serviço
Ping ICMP	Disponibilidade de servidor Tempo de resposta ICMP Perda de pacotes
Verificação Remota	Execução de comando por SSH ou Telnet

Tabela 4 - Funções do monitoramento sem agente

O servidor Zabbix pode verificar se um serviço está ativo em uma porta, e também se ele está respondendo adequadamente. Isto é válido apenas para os seguintes serviços: FTP, IMAP, LDAP, NNTP, POP3, SSH e Telnet.

Para outros casos, o sistema pode verificar se algum serviço está utilizando uma porta específica TCP, desta forma indicando se ele está disponível ou não.

O Zabbix também pode checar se um host está respondendo à pacotes ICMP ping. Apesar de ser uma verificação simples, ela é bastante importante para controlar a disponibilidade de um servidor, assim como seu tempo de resposta e perda de pacotes.

É possível configurar o sistema para acessar outro dispositivo através de SSH e Telnet. O comando é executado remotamente e o valor é retornado ao servidor Zabbix.

#### **4.1.4 Monitoramento web**

O Zabbix fornece uma maneira de monitorar sistemas web de forma eficaz e flexível. O módulo de verificação web periodicamente executa cenários pré-definidos e armazena os resultados obtidos.

Dessa forma, a ferramenta permite checar o desempenho e disponibilidade de diversos recursos web, e a partir dos dados coletados, consegue gerar gráficos, alertas e notificações.

Para cada passo de um cenário, o Zabbix armazena os seguintes dados: tempo de resposta, código de resposta e velocidade de download.

Este monitoramento também possui alguns recursos adicionais, como o uso de variáveis, utilização de métodos GET e POST, autenticação básica e suporte a HTTP e HTTPS [17].

Na Figura 14 temos um exemplo de gráfico criado a partir do recurso de monitoramento web do Zabbix:

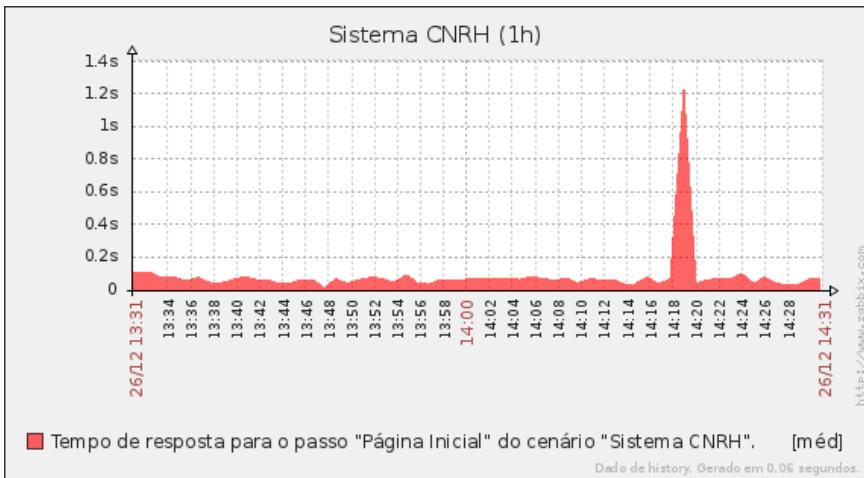


Figura 14 - Gráfico do tempo de resposta de um sistema web do Sesc DN

#### 4.1.5 Monitoramento de máquinas virtuais

Acrescentado recentemente na versão 2.2, o Zabbix conta com suporte nativo ao monitoramento de máquinas virtuais VMware.

Este recurso inclui a descoberta automática de hypervisors e máquinas virtuais, assim como de instalações do vCenter e vSphere para obter informações sobre diversas propriedades e estatísticas das máquinas [18].

A instalação padrão do Zabbix já conta com um modelo de verificações pronto para monitorar a solução de virtualização da VMware.

#### 4.1.6 Outros métodos de monitoramento

A partir da versão 2.0, é possível monitorar aplicações Java usando a tecnologia JMX (Java Management Extensions). Dessa forma, o servidor Zabbix requisita um contador JMX específico ao gateway Java do Zabbix, que remotamente pela API JMX fornece informações sobre a aplicação Java, sem a necessidade de outros softwares.

Também é possível efetuar o monitoramento de bancos de dados com o Zabbix. Através da tecnologia ODBC (Open Database Connectivity), o servidor pode coletar dados em diversos tipos de bancos de dados, tais como: Oracle, MySQL, PostgreSQL, e Microsoft SQL Server.

#### **4.1.7 Monitoramento de serviços de TI – SLA**

Outro recurso que o Zabbix oferece é o gerenciamento de serviços de TI. O monitoramento feito pelo sistema se traduz em uma visão de alto nível da infraestrutura analisada.

Esta característica da ferramenta permite que os administradores da rede tenham informações sobre a disponibilidade dos serviços prestados pelo departamento de TI, assim como por empresas externas, e possibilita a apuração do SLA dos diversos serviços.

## 5 Implementação do Sistema

### 5.1 Testes com Appliance

Os desenvolvedores do Zabbix fornecem uma forma muito prática para que pessoas interessadas possam testar o sistema. Através do download da Appliance fornecida no site da empresa, ilustrado na Figura 15, não é necessário instalar nem sistema operacional, nem o próprio Zabbix: eles vêm pré-instalados na imagem disponibilizada [19].

#### Zabbix Appliance

The Appliance is based on OpenSuSE Linux with MySQL back-end. Zabbix software is pre-installed and pre-configured for trouble free deployment.

You can use this Appliance to evaluate Zabbix. The Appliance is not intended for serious production use at this time.

Please refer to [Zabbix manual](#) for Appliance related documentation.

Package	Release	Date	Release Notes	Download
VMware / VirtualBox (.vmdk)	2.2.1	17 December, 2013		<a href="#">Download</a>
KVM	2.2.1	17 December, 2013		<a href="#">Download</a>
Open virtualization format (.ovf)	2.2.1	17 December, 2013		<a href="#">Download</a>
Live CD/DVD (.iso)	2.2.1	17 December, 2013		<a href="#">Download</a>
Preload ISO	2.2.1	17 December, 2013		<a href="#">Download</a>
USB stick / hard disk image	2.2.1	17 December, 2013		<a href="#">Download</a>
Xen guest	2.2.1	17 December, 2013		<a href="#">Download</a>
Microsoft VHD	2.2.1	17 December, 2013		<a href="#">Download</a>
Preload USB Image	2.2.1	17 December, 2013		<a href="#">Download</a>

Figura 15 - Opção de download de Appliance na Homepage do Zabbix

Para isto, basta que se tenha na máquina que servirá como teste, um programa de virtualização como VMware, VirtualBox ou Virtual PC. Existem diversos formatos de imagem na página de download do site.

Vários testes foram realizados nessa etapa, principalmente no que se refere aos recursos de monitoramento, interface do sistema, e opções de exibição dos dados obtidos.

Um pensamento que pode surgir no momento da implementação do sistema é colocar a imagem fornecida para ser executada de fato em “produção”, evitando o trabalho de ter que efetuar a instalação manualmente. Isso não deve ser feito principalmente por causa de quatro fatores:

- A imagem fornecida não vem otimizada para o ambiente de produção da empresa

- O sistema operacional embutido vem com senhas padrões ou de baixa segurança
- Não é possível atualizar o Zabbix facilmente em uma Appliance
- As imagens não incluem sistemas operacionais com suporte a arquitetura 64bit

A imagem da Virtual Appliance fornecida deve ser utilizada, portanto, somente para testes e avaliação da ferramenta, e nunca deve ser tratada como um sistema definitivo.

## **5.2 Escolha do sistema operacional**

O sistema operacional escolhido para este projeto foi o Ubuntu Server 12.04. Se trata de um sistema robusto para servidores, com documentação abundante pela Internet e familiar à maioria dos administradores de redes.

Outro motivo fundamental que levou à escolha do Ubuntu como sistema operacional, foi o fato de os desenvolvedores do Zabbix disponibilizarem para ele um repositório para a instalação e atualização do sistema de monitoramento. Isso permite que a instalação seja iniciada simplesmente com um “`apt-get install`”, sem que seja necessário baixar diversos pacotes.

Sendo assim, os seguintes pontos contribuíram para a escolha do Ubuntu como sistema operacional para a instalação da ferramenta:

- Conta com repositório exclusivo para instalação e atualização do Zabbix
- Versão exclusiva para servidores
- Compatível com a tecnologia de virtualização VMware implementada na empresa
- Documentação extensa disponível na Internet
- Sistema robusto e bem conhecido pela maioria dos administradores de TI

## **5.3 Instalação do Zabbix**

Uma particularidade do Sesc DN, é que a instituição optou por adotar a virtualização para seus servidores de aplicações. Desta forma, mais de 95% de

seus sistemas não são físicos, o que também influenciou a implementação do Zabbix em um servidor virtualizado.

Após a instalação sistema operacional, foi necessário a configuração do repositório do Zabbix. Estes são os comandos para Ubuntu 12.04 [20]:

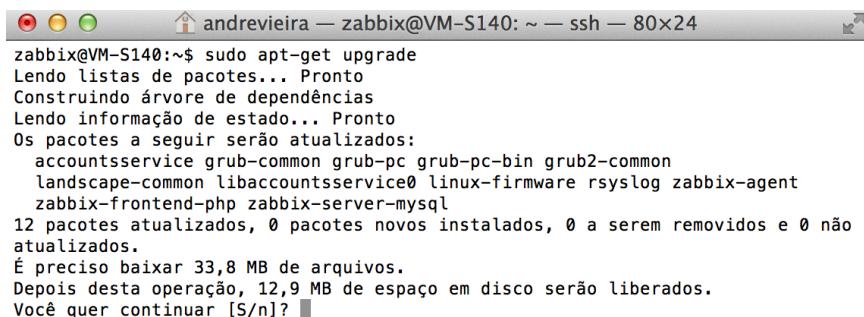
```
# wget http://repo.zabbix.com/zabbix/2.0/ubuntu/pool/main/z/zabbix-
release/zabbix-release_2.0-1precise_all.deb
# dpkg -i zabbix-release_2.0-1precise_all.deb
# apt-get update
```

Com a instalação do repositório, podemos fazer a instalação do sistema com um simples comando:

```
# apt-get install zabbix-agent zabbix-frontend-php zabbix-proxy-mysql
zabbix-server-mysql
```

Em seguida basta seguir as instruções do programa de instalação. Ele pedirá principalmente a definição de senhas para a criação do banco de dados e do usuário de administrador do Zabbix.

Uma das grandes vantagens de se instalar a ferramenta através do repositório disponibilizado é que a tarefa de atualização do sistema se torna algo muito mais fácil e rápido, bastando um simples comando “`apt-get upgrade`”, conforme ilustrado na Figura 16, para que o Zabbix seja migrado para a versão mais nova, procedimento que leva menos de cinco minutos em condições normais.



```
andrevieira — zabbix@VM-S140: ~ — ssh — 80x24
zabbix@VM-S140:~$ sudo apt-get upgrade
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
Os pacotes a seguir serão atualizados:
  accountsservice grub-common grub-pc grub-pc-bin grub2-common
  landscape-common libaccountsservice0 linux-firmware rsyslog zabbix-agent
  zabbix-frontend-php zabbix-server-mysql
12 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 0 não
atualizados.
É preciso baixar 33,8 MB de arquivos.
Depois desta operação, 12,9 MB de espaço em disco serão liberados.
Você quer continuar [S/n]? ■
```

Figura 16 - Atualizando o Zabbix por linha de comando

## 5.4 Configuração de hosts

Hosts são basicamente tudo aquilo que possui um endereço de IP e que é de desejável monitoramento. No caso da empresa estudada, estes equipamentos incluem:

- Roteadores de Internet

- Roteador de Intranet Local e de 28 Departamentos Regionais
- Switches
- Firewall
- Proxy
- Controladora da Rede sem Fio
- Telefonia (Gateway de Voz)
- Nobreaks
- Servidores de E-mail
- Servidor de AntiSpam
- Servidores de Aplicações
- Servidores Web

#### 5.4.1 Servidores

Na Figura 17 temos a tela de configuração de um host no Zabbix representando a configuração do monitoramento de um servidor de aplicações da empresa.

The screenshot shows the 'Host' configuration screen in Zabbix. At the top, there are tabs for Host, Templates, IPMI, Macros, and Inventário do host. The 'Host' tab is selected. Below the tabs, the 'Nome do host' field contains 'S01' and the 'Nome visível' field contains 'S01 - Servidor de Aplicações Desktop'. Under the 'Grupos' section, 'Servidores SESC' is listed under 'Nos grupos'. To the right, under 'Outros grupos', are several other monitoring categories: Conectividade SESC, Discovered hosts, Hypervisors, Infraestrutura SESC, Linux servers, Roteadores DRs, Servidores, Servidores CSS, Switches CSS, and Switches SESC. A 'Novo grupo' input field is also present. The 'Interfaces do agente' section shows an interface entry with 'Endereço IP' set to '10.1.' and 'Nome DNS' empty. The 'Connectado a' dropdown is set to 'IP' and 'Porta' is set to '10050'. A radio button for 'Padrão' is selected. Below this, sections for 'Interfaces SNMP', 'Interfaces JMX', and 'Interfaces IPMI' each have an 'Adicionar' link. At the bottom, 'Monitorado por proxy' is set to '(sem proxy)' and 'Status' is set to 'Monitorado'.

**Figura 17 - Configuração de monitoramento de um servidor**

Primeiro coloca-se um nome mais simples para servir de identificador do host, em seguida um nome mais explicativo sobre ele. Em seguida, selecionamos o grupo em que o host ficará (um grupo novo pode ser criado na hora), e colocamos seu endereço IP. No caso ilustrado, o host será monitorado através do agente Zabbix instalado nele, então colocamos esta informação apenas na linha “Interfaces do agente”.

#### 5.4.2 Roteadores

Da mesma forma que um servidor, a tela para configuração de qualquer outro dispositivo é a mesma. A Figura 18 ilustra a configuração do monitoramento de um dos roteadores da Intranet do Sesc DN.

Interface	Valor
Endereço IP	200.200.1.1
Status	Monitorado

Figura 18 - Configuração de monitoramento de um roteador

O monitoramento dos roteadores da empresa é feito através de SNMP, portanto preenchemos as informações de endereço IP apenas na linha “Interfaces SNMP”.

#### 5.4.3 Switches

Outro tipo de dispositivo muito monitorado neste projeto são os switches. O monitoramento é feito do mesmo modo que um roteador, através de SNMP. Na Figura 19 podemos ver a aba de “Templates” na tela de configuração de um novo host.

**CONFIGURAÇÃO DE HOSTS**

« [Lista de hosts](#) Host: [e-2a-sw01](#) Monitorado Aplicações (3) Itens (294)

[Triggers \(90\)](#) [Gráficos \(29\)](#) [Regras de descoberta \(1\)](#) [Cenários web \(0\)](#)

**Host Templates IPMI Macros Inventário do host**

Associado aos templates	Nome	Ação
	Template ICMP Ping	<a href="#">Desassociar</a> <a href="#">Desassociar e limpar</a>
	Template SNMP Interfaces	<a href="#">Desassociar</a> <a href="#">Desassociar e limpar</a>

Vincular a novos templates  [Adicionar](#)

**Figura 19 - Templates associados à um switch**

Nesta aba podemos associar imediatamente um modelo ao host que está sendo cadastrado. O host herdará todos os tipos de alertas e itens a serem monitorados diretamente do(s) modelo(s). Isto também pode ser feito mais tarde.

#### 5.4.4 Outros dispositivos

Podemos monitorar diversos outros tipos de dispositivos no Zabbix. A Figura 20 mostra uma tela que exibe várias informações obtidas através do monitoramento de dois nobreaks.



**Figura 20 - Tela de monitoramento de nobreaks**

Desde que o dispositivo implemente algum dos protocolos que o Zabbix suporta, o monitoramento é possível. Na maioria dos casos, foi utilizado o SNMPv2, amplamente difundido pelos fornecedores de equipamentos de redes.

## 5.5 Configuração de gráficos

Gráficos são um bom recurso para análise e diagnóstico de problemas. Felizmente o Zabbix indexa vários tipos diferentes de dados automaticamente e disponibiliza gráficos para o usuário.

Os gráficos são dinâmicos, atualizados em tempo real, e permitem selecionar um período de tempo específico, como uma determinada semana do mês passado.

Essencialmente, qualquer item sendo monitorado em um host e que possua um valor válido pode ser transformado em gráfico.

Exemplos de dados que podem ser visualizados em gráficos são: taxa de transferência do roteador de Internet (ilustrado na Figura 21), uso do processador da controladora de rede sem fio, número de conexões ao firewall, entre outros.

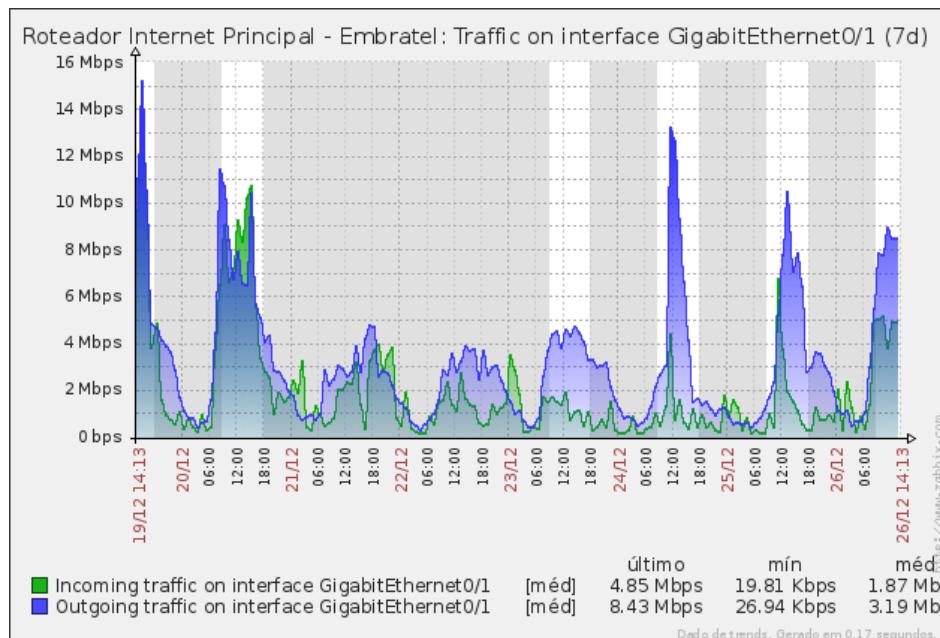


Figura 21 - Tráfego de dados em um dos roteadores de Internet

## 5.6 Configuração de mapas

É possível configurar no sistema de monitoramento, mapas ou diagramas para facilitar a visualização dos dados em tempo real. Para isso, basta criar um novo mapa, adicionar dispositivos já cadastrados no sistema, conectá-los, colocar legendas dinâmicas e/ou links nos dispositivos, e uma imagem de fundo.

É possível adicionar em um mapa qualquer tipo de host, e em cada um, colocar uma legenda estática ou dinâmica (com dados em tempo real). Podemos ainda conectar diferentes hosts através de linhas, também colocando informações entre os dois. Ainda é possível programar a mudança da cor da linha, por exemplo, caso a conectividade entre dois roteadores seja interrompida, a linha entre os dois ficará vermelha.

Os mapas são uma boa forma de se ter uma visão geral da rede e ajudam a localizar um ponto de falha ou “gargalo” com mais facilidade.

## 5.7 Configuração de telas personalizadas

Telas personalizadas são um recurso muito prático do Zabbix. É possível acrescentar diversos tipos de dados diferentes em uma única tela. Por exemplo, podemos criar uma tela que consolide dados importantes do servidor de e-mail. Nela poderíamos colocar gráficos de espaço disponível em disco, número de mensagens recebidas e entregues, usuários conectados, taxa de transferência, uso do processador, entre outros, conforme ilustrado na Figura 22.

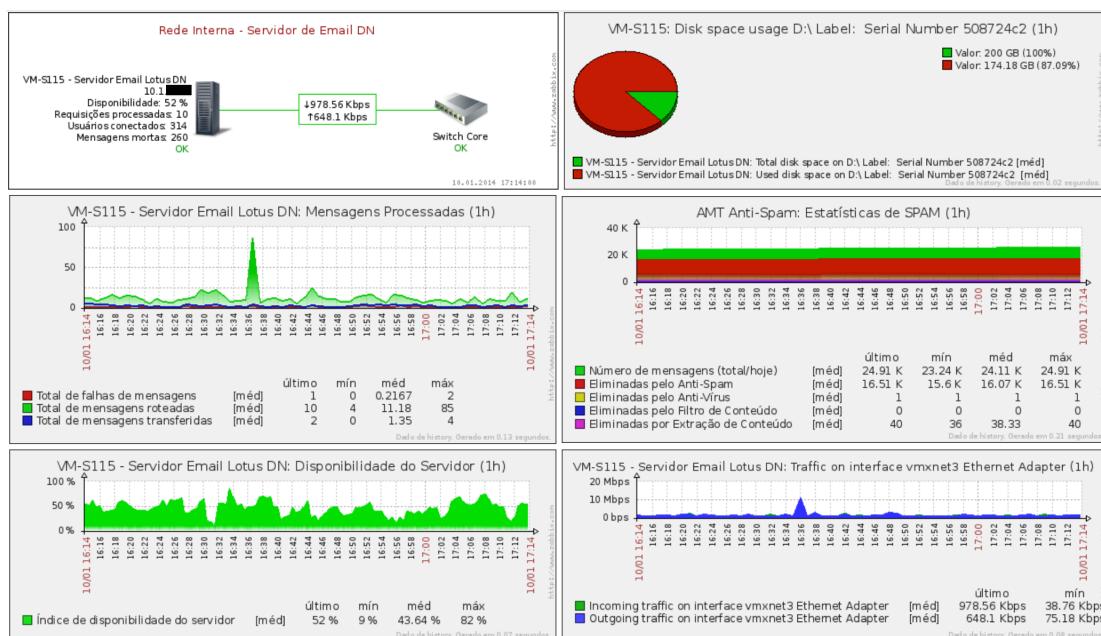


Figura 22 - Tela de monitoramento do servidor de e-mail do Sesc DN

Podemos ainda criar slideshows (apresentações de slides) com as telas anteriormente montadas. Isso é muito útil para configurar monitores dedicados para a exibição desses dados. Na sala de infraestrutura de TI da empresa estudada, após a implementação do Zabbix, passou-se a existir quatro monitores com slideshows diferentes, como podemos ver na Figura 23, exibindo esses dados para a equipe.



Figura 23 - Monitores da infraestrutura na Coordenadoria de TI do Sesc DN

## 5.8 Integração com sistema de autenticação corporativo

Uma tarefa importante era integrar o recurso de autenticação do Zabbix à algum sistema já existente na empresa. Isso é essencial, para evitar ter que criar vários novos usuários e senhas para cada pessoa que fosse utilizar o serviço.

A ferramenta oferece, além de autenticação apenas com usuários internos, integração com servidores LDAP, conforme ilustrado na Figura 24, e também permite realizar autenticação baseada em Apache (via HTTP).

**CONFIGURAÇÃO DE AUTENTICAÇÃO**

**Autenticação LDAP**

Autenticação padrão	<b>Interno</b>	<b>LDAP</b>	<b>HTTP</b>
Servidor LDAP	10.1.██████		
Porta	389		
Base DN	o=sescdn		
Atributo de pesquisa	mail		
Bind DN			
Senha para o Bind			
Teste de autenticação	[necessário um usuário LDAP válido]		
Login	██████@sesc.com.br		
Senha do usuário			

**Figura 24 - Modos de autenticação de usuários no Zabbix**

Existiam duas opções principais: integrá-lo ao Active Directory, ou ao Lotus Notes (Servidor de E-mail da instituição). A segunda acabou sendo escolhida, pois uma das vantagens de se realizar a autenticação pelo servidor de e-mail, é a possibilidade de, futuramente, usuários de outros Departamentos Regionais poderem acessar o Zabbix utilizando seus endereços de e-mail e senhas. Isto por que apenas funcionários do Departamento Nacional possuem credenciais no Active Directory local, porém todos os funcionários (inclusive os de Departamentos Regionais) têm e-mails do domínio `sesc.com.br`.

## 5.9 Configuração de avisos por e-mail

O Zabbix permite o envio de alertas por e-mail. Para isto, basta inserir as configurações do servidor de e-mail da empresa e habilitar esse tipo de notificação, conforme demonstrado na Figura 25.

**Tipo de mídia**

Nome	Email
Tipo	E-mail
Servidor SMTP	10.1.██████
SMTP helo	sesc.com.br
Email SMTP	██████@sesc.com.br
Ativo	<input checked="" type="checkbox"/>

**Salvar**   **Remover**   **Cancelar**

**Figura 25 - Tela de configuração de servidor de e-mail no Zabbix**

Após esta configuração, é necessário que cada usuário do sistema tenha um endereço de e-mail cadastrado em seu perfil para que possa receber as notificações. A Figura 26 mostra a possibilidade de especificar o nível de alertas que se deseja receber, assim como o horário.



Figura 26 - Tela de configuração do endereço de e-mail de um usuário no Zabbix

Este recurso não é ideal para alertas em tempo real, porém é um bom aliado no monitoramento preventivo. Ou seja, ao receber vários e-mails sobre um mesmo problema não-crítico, isto impulsiona o analista a investigar as causas do evento.

## 6 Validação da Implementação

Além da implementação e configuração do sistema em si, é importante descrever neste documento as reações da ferramenta em um eventual problema na infraestrutura de TI da empresa.

Para isto, foram tiradas fotos das telas de maneira a demonstrar os efeitos causados pelas falhas. A Figura 27, Figura 28 e Figura 29 mostram telas do sistema quando tudo está normal com a rede.

The screenshot shows the Zabbix main dashboard with the following sections:

- Gráficos favoritos:** Nenhum gráfico adicionado. (No graphs added.)
- Telas favoritas:** A list of monitoring items:
  - Internet e Intranet - Gráfico Geral de Uso
  - Intranet - Mapa dos Roteadores Brasil
  - Rede Interna - Controladora Wireless
  - Rede Interna - Diagrama da Rede
  - Rede Interna - Estado Resumido Infraestrutura Básica
  - Rede Interna - Firewall
  - Rede Interna - Gateway de Voz
  - Rede Interna - Proxy
  - Rede Interna - Últimos Alertas (1)
  - Intranet - Gráfico de Uso por DR (1)
- Últimos 20 incidentes:** Nenhum evento encontrado. (No events found.)
- Status do Zabbix:** Parâmetro | Valor | Detalhes
  - Zabbix está rodando | Sim | localhost:10051
  - Número de hosts (monitorados/não monitorados/templates/removidos) | 263 | 225 / 0 / 38
  - Número de itens (monitorados/desativados/não suportados) | 25809 | 23390 / 0 / 2419
  - Número de triggers (habilitadas/desabilitadas) [incidente/ok] | 8173 | 7761 / 412 [1 / 7760]
  - Número de usuários (online) | 14 | 4
  - Desempenho requerido do servidor, novos valores por segundo | 362.43 | -

Atualizado: 21:17:51

Atualizado: 21:17:21

Figura 27 - Dashboard principal do Zabbix com nenhum alerta ativo

The screenshot shows the status of key infrastructure services:

Serviço	Estado
Internet Principal	OK
Internet Secundário	OK
Intranet	OK
Telefonia	OK
Satélite Videoconferência	OK
Servidores	OK
Infraestrutura	OK
Portal SESC	OK

Buttons at the bottom: OK, Verificar, Falha.

Figura 28 - Tela do estado dos serviços principais da infraestrutura com nenhum alerta ativo

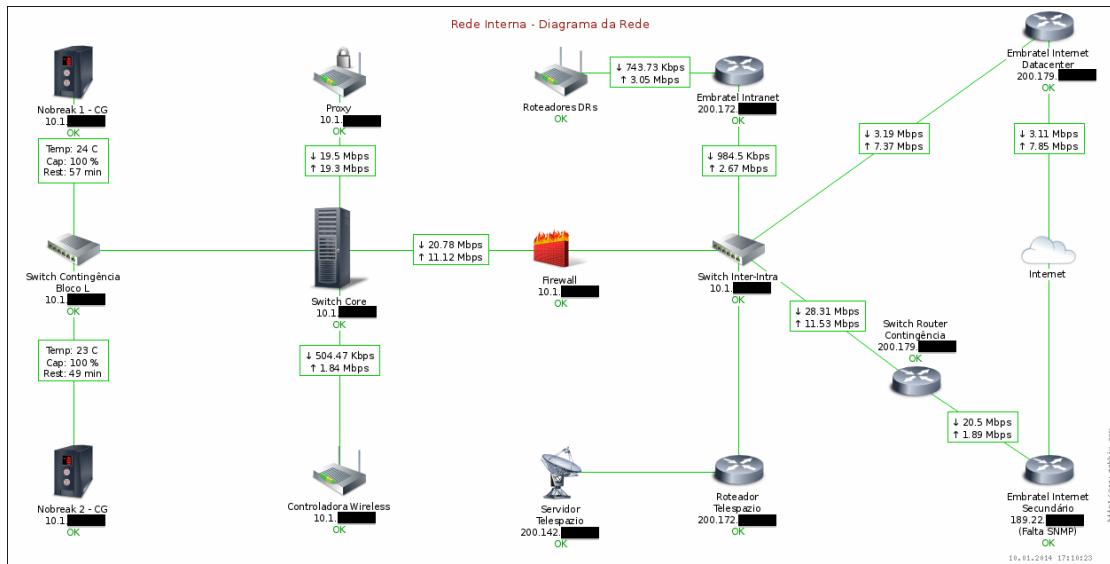


Figura 29 - Diagrama simplificado da rede do Sesc DN com nenhum alerta ativo

## 6.1 Demonstração de falha em um dos links de voz

A primeira demonstração simula uma falha em um dos links E1 de voz fornecidos pela Embratel.

Em menos de um minuto, um alerta aparece no dashboard (painel) principal do Zabbix, conforme ilustrado na Figura 30. Ele indica qual o dispositivo que está com problemas, a descrição da falha e o horário em que o evento começou. O intervalo de coleta de informações é de um minuto por padrão, mas pode ser modificado de maneira global, ou para um dispositivo específico.

Últimos 20 incidentes			
Host	Assunto	Última alteração	Idade
Gateway de Voz - SESC	Link de voz inoperante em Gateway SESC E1 2/0	08 Jan 2014 21:26:17	2m 38s

Figura 30 - Dashboard principal do Zabbix com alerta de falha em link de voz

A Figura 31 demonstra uma tela dedicada que informa o estado dos principais serviços de TI do Sesc DN. O ícone que representa a parte de telefonia fica amarelo, indicando que existe algum problema.



Figura 31 - Tela do estado dos serviços principais com alerta na parte de Telefonía

Outra tela que vale a pena ser mencionada, é a tela de informações do Gateway de Voz da empresa, ilustrada na Figura 32, que é o dispositivo que está diretamente conectado aos links E1 de voz. Ela indica o problema alterando a cor do link com falha, e do gateway conectado à ele.

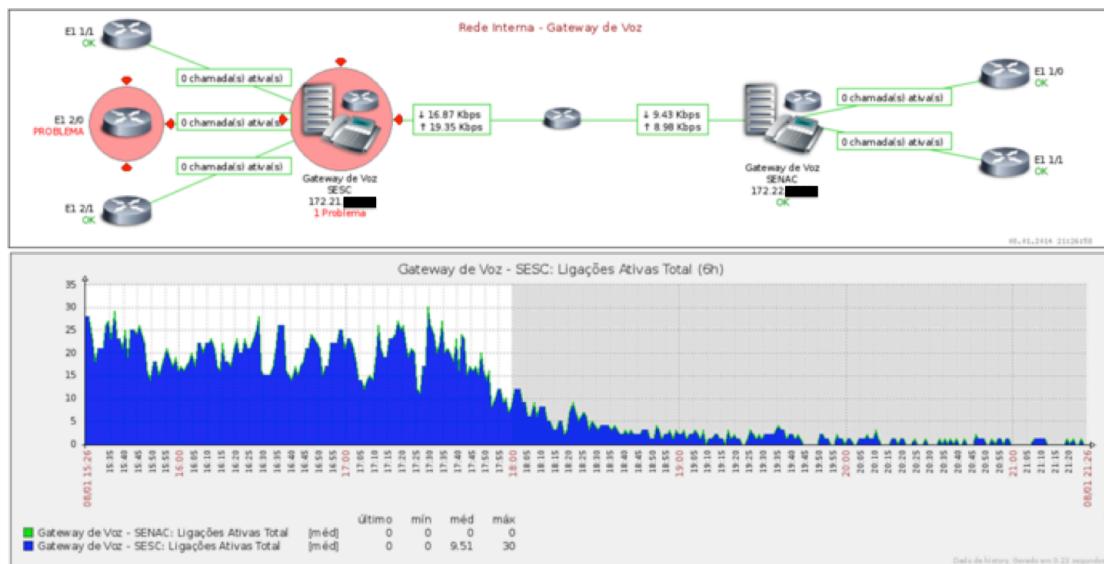


Figura 32 - Tela personalizada de informações do Gateway de Voz com alerta ativo em um dos links

## 6.2 Demonstração de falha em um dos links de Internet

Assim como na demonstração anterior, ao detectar uma falha em um dos links de Internet, a mesma é refletida no dashboard, indicando em qual dos roteadores o problema foi detectado, conforme a Figura 33.

The screenshot shows the Zabbix main interface. At the top, there's a navigation bar with links like 'Users', 'Eventos', 'Gráficos', 'Telas', 'Mapas', 'Autobusca', and 'Serviços de TI'. Below that is a breadcrumb trail: 'hosts > Pesquisar > Configuração dos hosts'. A section titled 'Últimos 20 incidentes' displays a single item: 'Roteador Internet Principal - Embratel' with the subject 'Link de Internet Principal Indisponível'. The status is red, indicating an error. The last update was '08 Jan 2014 21:43:47' and it's been active for '10m 30s'. A timestamp 'Atualizado: 21:54:17' is also visible.

**Figura 33 - Dashboard principal do Zabbix com alerta de falha em um link de Internet**

A falha também é registrada com um símbolo vermelho na tela de serviços principais, ilustrada na Figura 34.



**Figura 34 - Tela do estado dos serviços principais com alerta na conexão principal com a Internet**

No diagrama da rede, demonstrado na Figura 35, um círculo vermelho fica em volta do roteador que apresentou o problema.

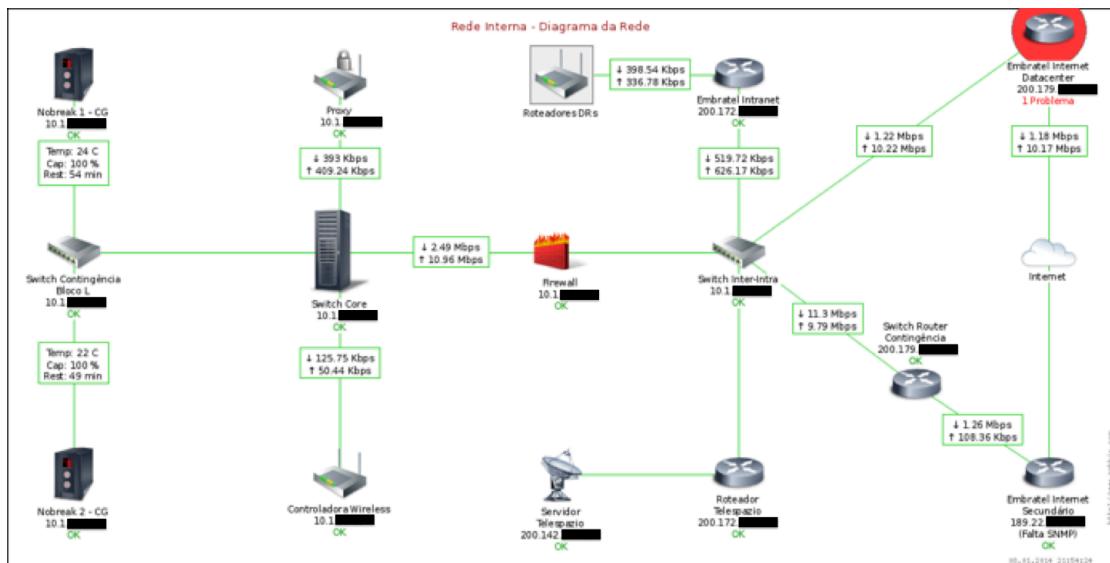


Figura 35 - Diagrama simplificado da rede do Sesc DN com alerta ativo no roteador principal de Internet

### 6.3 Demonstração de aumento excessivo de temperatura em um nobreak

Em um eventual aumento na temperatura de um nobreak, este alerta também é exibido no dashboard do Zabbix, conforme a Figura 36.

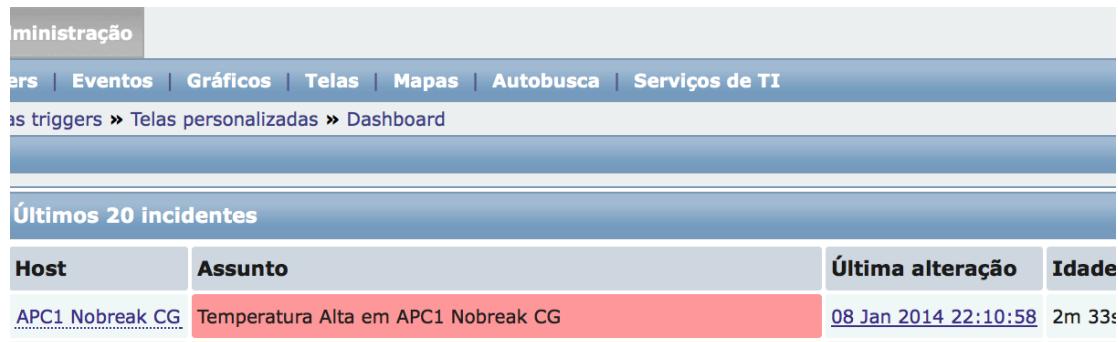


Figura 36 - Dashboard principal do Zabbix com alerta de temperatura em um nobreak

O aviso é refletido como um problema na parte de infraestrutura geral, na tela do estado dos serviços principais, ilustrada na Figura 37.



Figura 37 - Tela do estado principal dos serviços da rede com alerta na parte de Infraestrutura

E por fim, no diagrama da rede, o nobreak afetado é circulado de vermelho, conforme demonstrado no canto superior esquerdo da Figura 38.

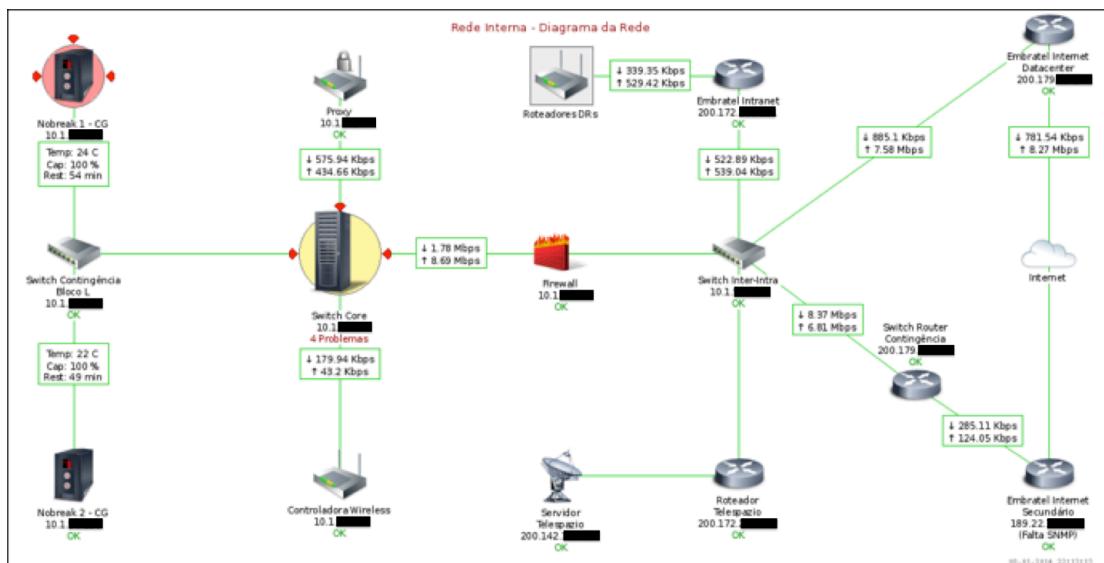


Figura 38 - Diagrama simplificado da rede do Sesc DN com alerta ativo em um dos nobreaks

## 7 Impacto na Equipe de TI

### 7.1 Facilitação da identificação dos problemas da rede

Com o auxílio do sistema, em especial com o recurso de mapas e telas personalizadas, a identificação da origem dos problemas de infraestrutura na rede fica muito mais evidente. Com a exibição de alertas para dispositivos específicos, e com mapas que mostram o estado dos ativos de rede em tempo real, é possível saber exatamente a localização física e lógica do evento em questão.

Dentre os vários recursos do sistema implementado, a criação de telas personalizadas, como ilustrado na Figura 39, foi essencial no desenvolvimento de ferramentas que facilitassem a exibição e customização das informações exibidas para os administradores.

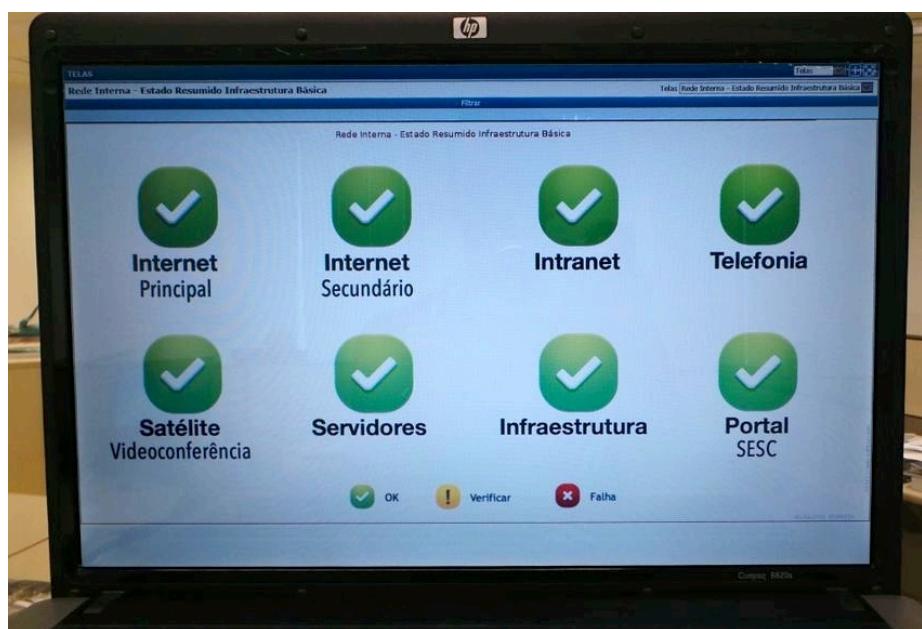


Figura 39 - Monitor do estado dos principais serviços de TI do Sesc DN

### 7.2 Diminuição do tempo de resposta

Evidentemente, com um sistema que informe em tempo real o estado do rede, assim como os problemas que estão ocorrendo naquele momento, é possível diminuir significativamente o tempo de resposta aos incidentes. Mesmo que a solução da ocorrência não dependa diretamente da equipe, é possível acionar com mais antecedência o parceiro responsável ou a concessionária prestadora de serviços para que faça os reparos o quanto antes.

Com o diagrama da Figura 40, podemos representar os simples passos que ocorrem numa eventual falha na rede, após a configuração do Zabbix:

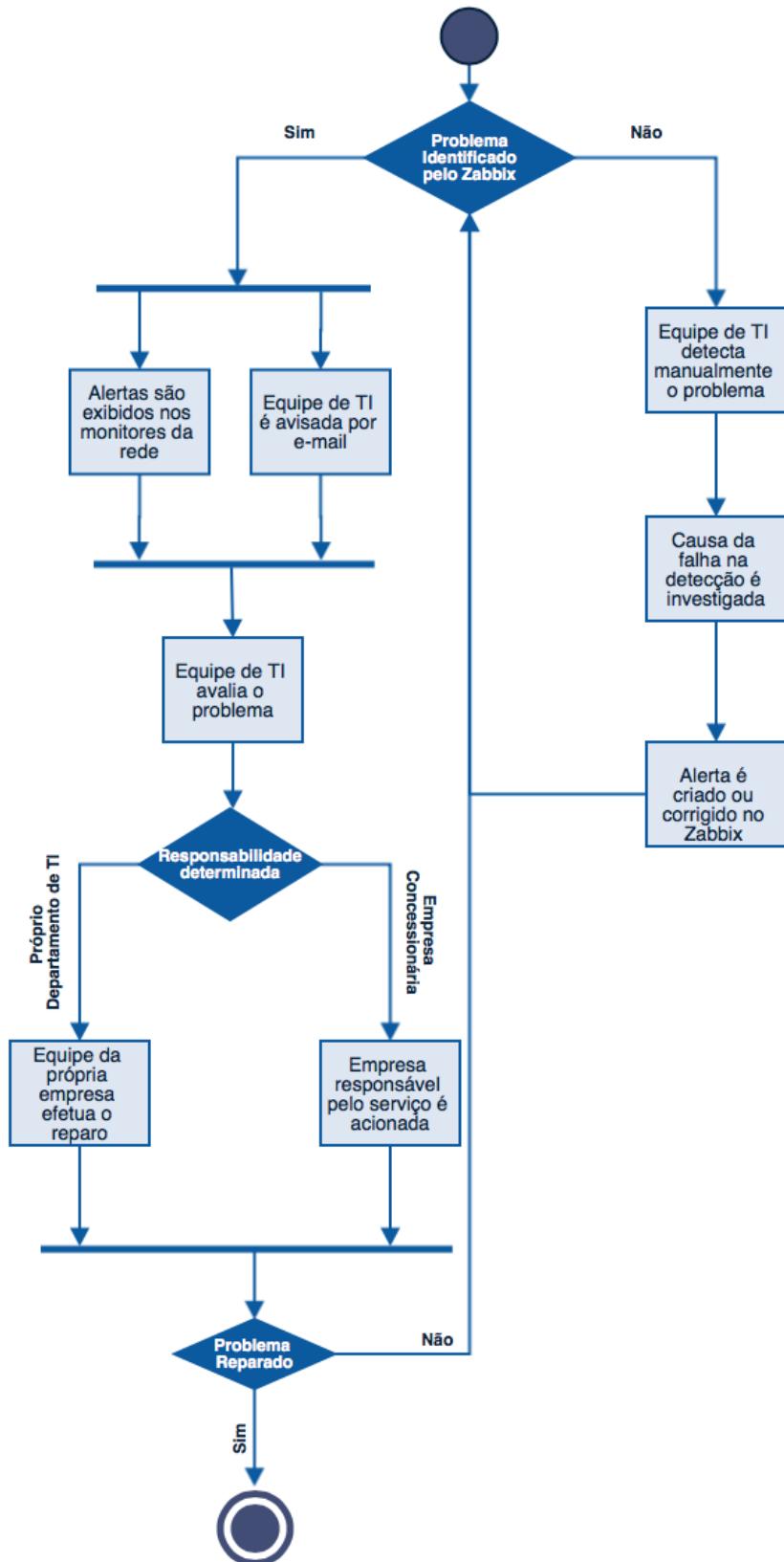


Figura 40 - Diagrama de atividades em uma eventual falha na rede

### **7.3 Priorização de investimentos**

A presença de um sistema de monitoramento eficiente permite que se descubram os pontos de gargalo de uma rede, assim como os locais onde ela mais falha. Isso possibilita que a equipe de infraestrutura possa elaborar uma lista de prioridades com equipamentos que precisem ser substituídos ou reparados. Também permite cobrar de concessionária de serviços a qualidade e disponibilidade do serviço contratado.

## **8 Conclusões**

Não há como negar que atualmente a informática seja uma parte importante de qualquer empresa. Os serviços que ela oferece são essenciais para que os funcionários possam desenvolver suas atividades. Internet, troca de e-mails, telefonia, videoconferência são apenas alguns exemplos.

Uma rede de computadores confiável é aquela que fornece alta disponibilidade e boa performance para seus usuários. Se você não puder monitorar sua própria rede, não há como saber se ela fornece os serviços na qualidade prometida, e consequentemente, não é possível garantir que ela seja confiável.

O projeto permitiu realizar um estudo sobre modelos de referência no gerenciamento de TI, assim como uma análise sobre as principais ferramentas de gerência disponíveis no mercado. Com base nas informações obtidas, foi possível executar um levantamento de requisitos no cenário da empresa estudada e com ele, determinar o sistema que melhor atenderia as necessidades da instituição.

Com os estudos realizados, o Zabbix foi determinado como solução de gerenciamento de TI mais adequada ao ambiente do Departamento Nacional do Sesc. O fato de ser gratuito, de fácil manutenção, de constante atualização, junto com todos os recursos de interface que ele oferece, tornou este sistema o ideal para a empresa e sua Coordenadoria de TI.

O sistema de monitoramento que foi implementado na empresa fornece à equipe de infraestrutura de TI uma nova forma de diagnosticar problemas na rede. As falhas são identificadas imediatamente, e o tempo de resposta pode ser reduzido significativamente. Além de problemas, a equipe pode saber quais são os pontos de gargalo, priorizar e direcionar mais eficientemente investimentos. Por fim, conseguimos proporcionar aos usuários finais da rede, serviços de TI de maior qualidade.

### **8.1 Trabalhos futuros**

Durante a implantação do Zabbix na empresa, foi possível observar algumas demandas que o sistema não conseguia atender adequadamente. Apesar

de não serem essenciais para a equipe de TI, essas demandas trazem à tona aspectos passíveis de melhoria no Zabbix e de possíveis trabalhos futuros.

Em primeiro lugar, a ferramenta não fornece de forma nativa, ou através de integração, uma maneira de visualizar dados Netflow dos equipamentos da infraestrutura. Esta limitação foi contornada através da criação de diagramas e mapas no Zabbix, entretanto isto não substitui o detalhamento fornecido pelo protocolo proprietário. Torna-se necessário encontrar uma solução que une o Zabbix com a coleta de informações através do Netflow.

Outro ponto que merece atenção é a falta de integração do Zabbix com um sistema de help desk baseado em tickets. Esta integração seria interessante para tornar mais eficiente a tomada de decisões nos reparos da infraestrutura, inclusive para a designação de indivíduos responsáveis por tratar determinados casos.

Por fim, um recurso que possibilitasse a divulgação automática de determinadas informações de forma pública seria interessante, principalmente para empresas que zelam pela transparência. Esta demanda surgiu da necessidade em disponibilizar simples indicadores coletados pelo Zabbix no site de Intranet da empresa. Apesar de isto ser possível através de algumas manobras, não existe uma forma simples e segura de tornar um mapa ou gráfico público por exemplo.

## 9 Referências

1. MAURO, D.; SCHMIDT, K. **Essential SNMP**. 2a. ed. Sebastopol: O'Reilly Media, 2005.
2. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 7498-4 - Management framework. **Information processing systems - Open Systems Interconnecton - Basic Reference Model**, 1989.
3. GLITHO, R. H.; HAYES, S. Telecommunications Management Network: Vision vs. Reality. **IEEE Communications Magazine**, mar. 1995.
4. INTERNATIONAL TELECOMMUNICATION UNION. M.3010 - Principles for a telecommunications management network. **Series M: TMN and network maintenance: International transmission systems, telephone circuits, telephony, facsimile and leased circuits**, fev. 2000.
5. OGC - OFFICE OF GOVERNMENT COMMERCE. **The Official Introduction to the ITIL Service Lifecycle**. 2a. ed. [S.l.]: The Stationary Office, 2007.
6. TANENBAUM, A. S.; WETHERALL, D. J. **Computer Networks**. 5a. ed. [S.l.]: Prentice Hall, 2011.
7. CISCO SYSTEMS. Cisco IOS NetFlow. Disponível em:  
[http://www.cisco.com/en/US/products/ps6601/products\\_ios\\_protocol\\_group\\_home.html](http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html). Acesso em: 07 jan. 2014.
8. TELCOMANAGER. O que é Netflow? Disponível em:  
<https://www.telcomanager.com/pt-br/o-que-e-netflow>. Acesso em: 06 jan. 2014.
9. IETF. RFC 4741 - NETCONF Configuration Protocol. Disponível em:  
<http://tools.ietf.org/html/rfc4741>. Acesso em: 07 jan. 2014.
10. COTTRELL, L. Network Monitoring Tools. **SLAC National Accelerator Laboratory**. Disponível em:  
<http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html>. Acesso em: 09 jan. 2014.
11. SERVIÇO SOCIAL DO COMÉRCIO. Sesc - Serviço Social do Comércio. **Sobre o Sesc**. Disponível em: [http://www.sesc.com.br/portal/sesc/o\\_sesc/](http://www.sesc.com.br/portal/sesc/o_sesc/). Acesso em: 30 dez. 2013.
12. ZABBIX SIA. What is Zabbix. **Homepage of Zabbix**. Disponível em:  
<http://www.zabbix.com/product.php>. Acesso em: 06 jan. 2014.
13. ZABBIX SIA. Customers and Users. **Homepage of Zabbix**. Disponível em:  
<http://www.zabbix.com/users.php>. Acesso em: 09 jan. 2014.
14. ZABBIX SIA. Zabbix Agent. **Homepage of Zabbix**. Disponível em:  
[http://www.zabbix.com/zabbix\\_agent.php](http://www.zabbix.com/zabbix_agent.php). Acesso em: 06 jan. 2014.
15. ZABBIX SIA. SNMP and IPMI Agents. **Homepage of Zabbix**. Disponível em:  
[http://www.zabbix.com/snmp\\_ipmi\\_agent.php](http://www.zabbix.com/snmp_ipmi_agent.php). Acesso em: 06 jan. 2014.
16. ZABBIX SIA. Agentless Monitoring. **Homepage of Zabbix**. Disponível em:  
[http://www.zabbix.com/agentless\\_monitoring.php](http://www.zabbix.com/agentless_monitoring.php). Acesso em: 06 jan. 2014.
17. ZABBIX SIA. Web Scenarios. **Homepage of Zabbix**. Disponível em:  
[http://www.zabbix.com/web\\_scenarios.php](http://www.zabbix.com/web_scenarios.php). Acesso em: 06 jan. 2014.

18. ZABBIX SIA. Virtual Machine Monitoring. **Homepage of Zabbix**. Disponivel em: <[http://www.zabbix.com/virtual\\_monitoring.php](http://www.zabbix.com/virtual_monitoring.php)>. Acesso em: 06 jan. 2014.
19. ZABBIX SIA. Download. **Homepage of Zabbix**. Disponivel em: <<http://www.zabbix.com/download.php>>. Acesso em: 06 jan. 2014.
20. ZABBIX SIA. Installation from packages. **Zabbix documentation**. Disponivel em: <[https://www.zabbix.com/documentation/2.2/manual/installation/install\\_from\\_packages](https://www.zabbix.com/documentation/2.2/manual/installation/install_from_packages)>. Acesso em: 06 jan. 2014.