

# GERÊNCIA DE REDES: UTILIZANDO O ZABBIX PARA MONITORAR A DISPONIBILIDADE E TRANSFERÊNCIAS DE IMAGENS

Leonardo Dornelas SOARES

Centro de Ensino Superior de Juiz de Fora, Juiz de Fora, MG

Romualdo Monteiro de Resende COSTA

**Resumo:** Este artigo apresenta um estudo de caso sobre o monitoramento de ativos de rede voltados à transmissão de imagens médicas do Grupo Alliar – Medicina Diagnóstica. Neste estudo é apresentada a ferramenta Zabbix e seu emprego no mapeamento dos ativos que provêm a comunicação entre as filiais desse grupo. É definida a qualidade mínima para o funcionamento da comunicação, bem como alertas que indicam quando essa qualidade não é alcançada, permitindo a realização de ações para sanar esse problema.

**Palavras-chave:** Zabbix, PACS, monitoramento de rede, transferências de imagens e Simple Check.

## 1 INTRODUÇÃO

Para atender aos requisitos do negócio, as redes de computadores, principalmente as das médias e das grandes empresas e instituições, são formadas por uma grande quantidade de hardware e componentes de software, deixando-as mais complexas (DEO, 2010). Gerenciá-las significa lidar diariamente com riscos que podem ser causados pela má configuração dos serviços, falhas de software, problemas de segurança, desempenho e interrupção dos equipamentos.

Segundo Lessa (1999): “Estatisticamente, enquanto 30% dos custos de uma infraestrutura computacional estão diretamente associados à aquisição de hardware, os 70% restantes dizem respeito à manutenção e suporte aos recursos e serviços nela contidos”. Tendo em vista esse cenário, Junqueira (2014) conclui que as empresas estão investindo cada vez mais na segurança dos dados que trafegam pela rede, bem como no gerenciamento de seus serviços e ativos de redes, já que o custo de uma informação perdida ou de um serviço indisponível a seus clientes e/ou usuários é imensurável.

O monitoramento da infraestrutura computacional, portanto, torna-se, nos dias atuais, uma atividade que contribui decisivamente para o funcionamento contínuo dos serviços oferecidos, garantindo que a qualidade desses mantenha-se em níveis satisfatórios pelo maior tempo possível. (FACHINI, 2010)

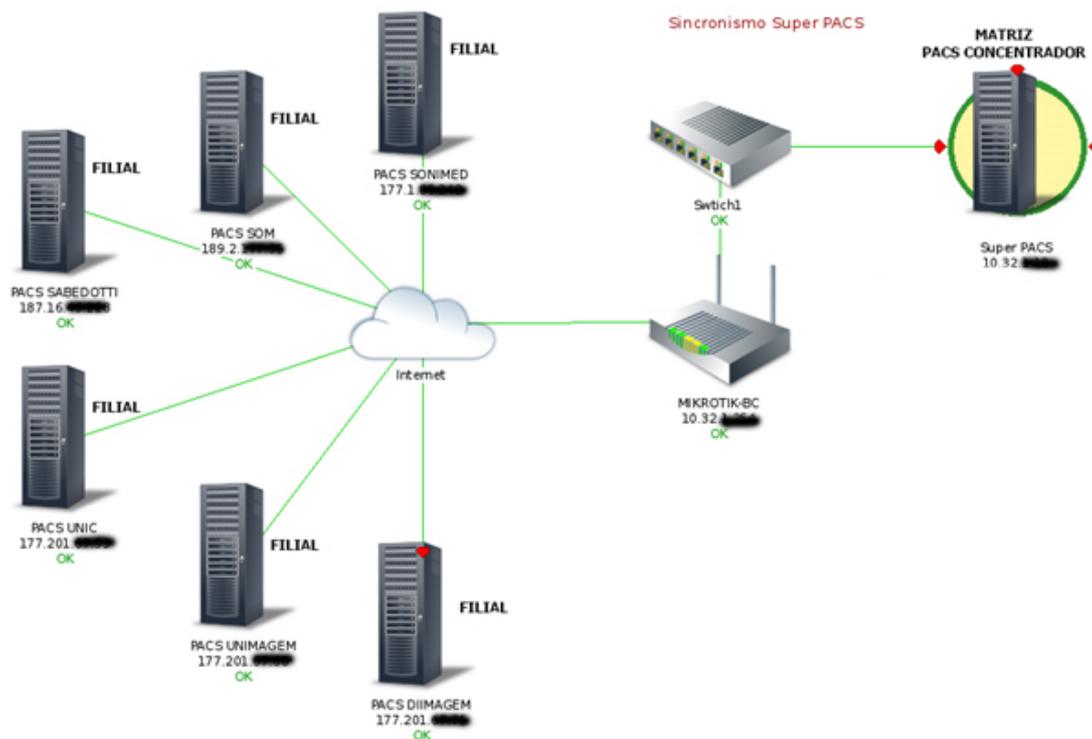
Os equipamentos de rede que utilizam a arquitetura TCP/IP (LOZANO, 1998) tem, como padrão de comunicação para monitoramento e controle, o protocolo SNMP (DIAS, 2001). Esse padrão determina, na sua forma tradicional, uma arquitetura formada por agentes (equipamentos monitorados) e gerentes (equipamento monitor). Cabe aos gerentes coletar as informações

dos agentes e, quando necessário, enviar mensagens solicitando a alteração dos valores. Embora essas operações possam ser realizadas diretamente através de comandos do protocolo, é recomendável a utilização de uma ferramenta que abstraia ao operador, através de uma interface gráfica, por exemplo, o monitoramento e controle dos agentes.

Entre as ferramentas de monitoramento Nagios, CACTI, ZenOSS, OpManager (BLACK, 2008), o Zabbix é um software que se destaca ao monitorar a disponibilidade e desempenho não apenas dos equipamentos, mas também de aplicações de rede de qualquer equipamento que possa ser acessado remotamente por um endereço IP (*Internet Protocol* - Protocolo de Internet). Com ele é possível agir proativamente, detectando e corrigindo falhas antes que os usuários percebam, além de analisar a disponibilidade dos serviços oferecidos na rede (PIRES, 2014).

## 2 OBJETIVOS

Este artigo tem como principal objetivo monitorar equipamentos que realizam a transferência, cópia de imagens de exames entre empresas do Grupo Alliar – Medicina Diagnóstica, um grupo de empresas que atua em diversas regiões do Brasil no ramo de radiologia e diagnóstico por imagem, realizando exames de Ressonância Magnética, Tomografia Computadorizada, PET-CT, Raio-X, Mamografia, Ultrassonografia e Densitometria Óssea. A Figura 1 apresenta o mapa dos equipamentos envolvidos neste trabalho.



**Figura 1.** Mapa de Rede do Grupo Alliar- Medicina Diagnóstica.

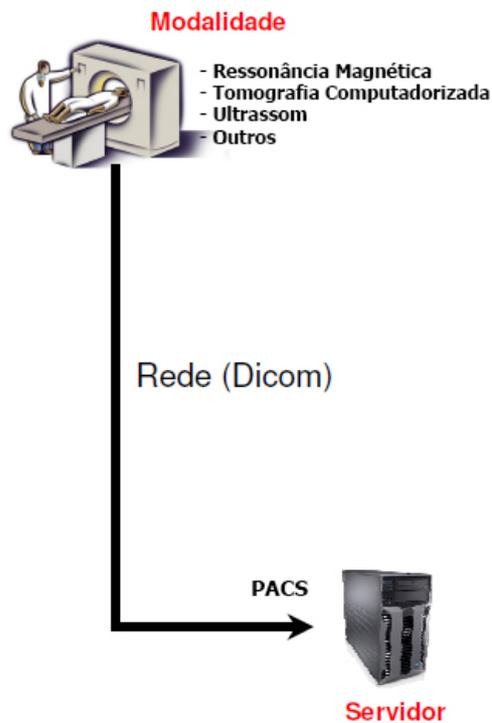
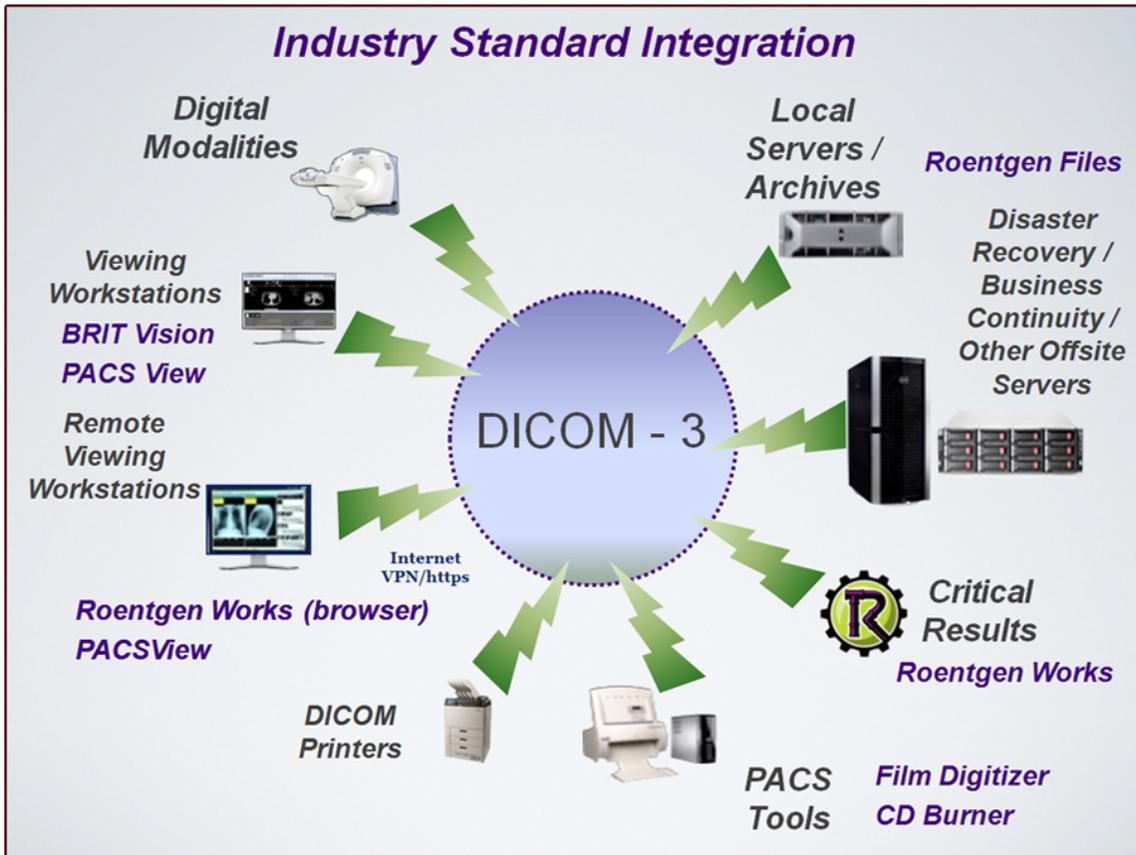
Na Figura 1 são apresentadas as diversas filiais que compõem o grupo com destaque para a matriz, a concentradora localizada em Juiz de Fora – Minas Gerias. Na prática, os exames realizados nas diversas filiais precisam trafegar até a matriz para avaliação/laudo médico, com posterior retorno dessa informação às filiais. Assim, o objetivo principal deste trabalho é construir um processo de mapeamento que identifique, o mais breve possível, qualquer falha nesse processo de comunicação entre as filiais e a empresa CEDIMAGEM (Centro de Diagnóstico Cláudio Ramos Ltda), que representa a matriz.

Na verdade, toda a comunicação entre as filiais e a matriz é gerenciada através do sistema PACS (*Picture Archiving and Communication System* - Sistema de Comunicação e Arquivamento de Imagens) (MARQUES, 2009), que será abordado na seção a seguir. Nesse sistema, como será discutido, ainda que exista um canal de comunicação ativo entre os equipamentos, o tráfego de mídias, principalmente de imagens correspondentes aos exames de diagnóstico, pode apresentar falhas de acordo com a qualidade do serviço oferecido. Assim, este trabalho tem, como objetivo complementar, identificar a qualidade necessária a essa comunicação identificando, portanto, o motivo das falhas que ocorrem na transferência de imagens de exames entre as filiais com a matriz. Na ocorrência dessas falhas, as imagens dos exames não são transferidas por completo, inviabilizando o diagnóstico pelo corpo clínico (médicos radiologistas) da empresa que, na maioria das vezes, encontram-se na matriz.

### **3 TRABALHOS RELACIONADOS**

#### **3.1 PACS**

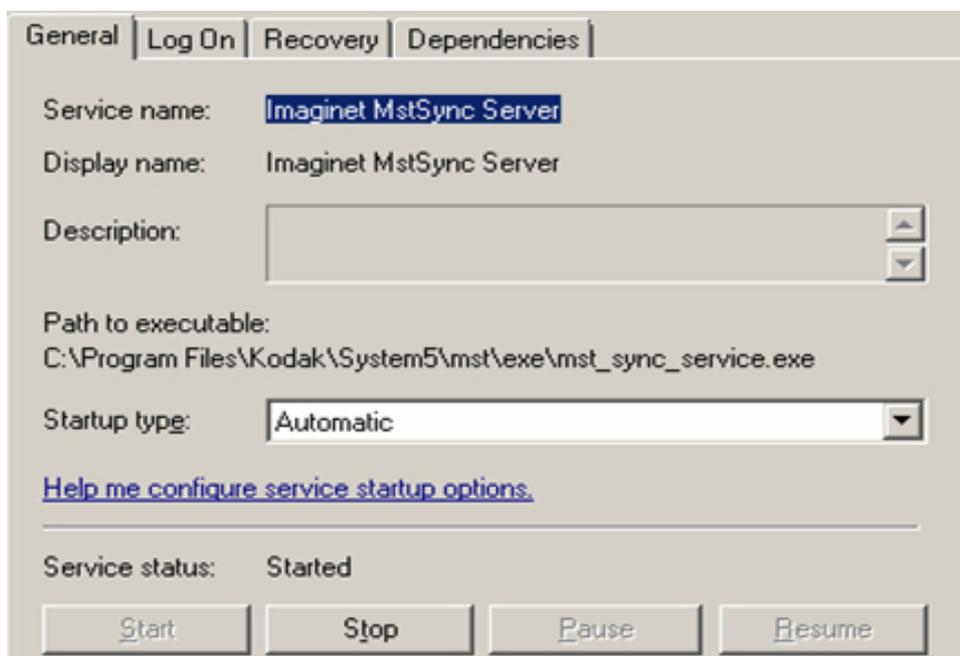
O sistema PACS é um importante software capaz de gerenciar a transferência das imagens de exames entre servidores e, neste trabalho, é o software cuja infraestrutura de rede deve garantir a qualidade necessária à transferência das imagens. Essas imagens são provenientes de modalidades, nome genérico dado a qualquer equipamento médico radiológico que gere imagens. A comunicação entre as modalidades e o servidor PACS é realizada através do protocolo de comunicação DICOM (*Digital Imaging and Communicating in Medicine* – Comunicação de Imagens Digitais em Medicina) (MARQUES, 2009) que define uma sintaxe padrão para a comunicação das imagens e dados demográficos do paciente, entre os mais diversos fabricantes de equipamentos. As Figuras 2a e 2b, demonstram respectivamente as integrações com sistemas e equipamentos e estrutura lógica de uma rede DICOM.



**Figura 2a** – Integrações de uma rede DICOM.

**Figura 2b** – Transferência de Imagens das Modalidades para PACS.

No contexto deste trabalho, o PACS Concentrador, denominado a partir desse ponto de Super PACS, situado na Matriz (Juiz de Fora/MG), comunica-se com os demais sistemas PACS Filiais de várias regiões do Brasil (conforme ilustrado na Figura 1), também através do protocolo DICOM. Essa comunicação é sincronizada através de um serviço chamado Imaginet MstSync Server, ilustrado na Figura 3. Através desse serviço, o Super PACS verifica de



“tempos em tempos” se existe novas imagens e exames nos PACS's Filiais. Em caso afirmativo é iniciada a cópia dessas novas imagens para o Super PACS.

**Figura 3** – Serviço de sincronismo de imagens.

Evidentemente, para que a cópia das imagens possa acontecer deve existir um link de dados ativo entre a matriz e cada uma das filiais. O problema, no entanto, é que, dependendo da relação entre a capacidade do link e o tamanho do conteúdo a ser transmitido, pode ocorrer uma saturação, retardando ou até mesmo impedindo a cópia das imagens.

Além da aleatoriedade na realização dos diversos tipos de exames que, por sua vez, podem produzir quantidades variadas de imagens, um mesmo tipo de exame pode produzir diferentes quantidades de imagens. A Tabela 1 ilustra a média de número de imagens e seu tamanho por exame;

Equipamento de exame	Nº de imagens por exame (Média)	Tamanho aprox. por Imagem (Mb)	Tamanho total (Mb)
Ressonância Magnética	500	0,17	85
Tomografia Computadorizada	700	0,18	126
Raio-X	3	3,66	10,98
Mamografia	4	2,6	10,4

**Tabela 1.** Média de número imagens e tamanho (Mb).

O número de imagens por exame pode variar consideravelmente de acordo com a região de estudo do corpo, para tanto foi extraído uma média de um período de 3 dias. Enquanto que o tamanho dessas imagens relaciona-se com a quantidade de informação presente na estrutura do exame.

Dessa forma, a qualidade do canal deve ser periodicamente monitorada a fim de garantir o sincronismo entre as filiais, onde o exame é realizado, e a matriz, onde o laudo é confeccionado.

### **3.2 ZABBIX**

Desenvolvido a partir de 1998, o Zabbix é uma das mais completas ferramentas de gerência e administração de redes disponíveis no mercado. Através dessa ferramenta é possível monitorar, por exemplo, parâmetros relacionados ao funcionamento de switches, roteadores, computadores e/ou quaisquer outros componentes que estejam conectados à rede. Essa ferramenta também oferece uma configuração amigável, através da sua interface Web, permitindo, entre outras operações, a manutenção de hosts, mapas, templates, gráficos e gatilhos (*triggers*) entre outras funcionalidades que serão descritas nesta seção.

Utilizando-se de um mecanismo de notificação flexível é possível configurar alertas de eventos, informações ou incidentes pertinentes por meio de e-mail ou SMS o que auxilia expressivamente para uma rápida ação por parte dos administradores de redes. Entre as principais características e recursos disponíveis no Zabbix, listamos abaixo as principais características para a escolha dessa ferramenta, conforme documentação associada a ferramenta<sup>1</sup>:

- All-in-one (Tudo em um), solução única quando se trata de monitoramento;
- Projetado para lidar com as comunicações instáveis;
- Todos os dados históricos, tendências e configuração são armazenados em um banco de dados;
  - Oracle, MySQL, PostgreSQL e SQLite.
- Solução verdadeiramente Software Livre (GPLv2), não existe versões comerciais;
- Possui suporte a maioria dos sistemas operacionais: Linux, Solaris, HP0UX, AIX, FreeBSD, OpenBSD, NetBSD, Mac OS X, Windows, entre outros;
- Agentes disponíveis para diversas plataformas: Linux, Solaris, HP0UX, AIX, FreeBSD, OpenBSD, SCO-OpenServer, Mac OS X, Windows 2000/XP/2003/Vista;
- Agentes para plataformas 32 bits e 64 bits;

---

<sup>1</sup> [www.zabbix.com](http://www.zabbix.com)

- Toda a lógica está do lado do servidor, os agentes são usados apenas para coleta de dados;
- Capacidade de monitorar serviços “simples” como (HTTP, POP3, IMAP, SSH, ICMP Ping) sem o uso de agentes;
- Suporte nativo ao protocolo SNMP;
- Geração de gráficos em tempo real;

### 3.2.1 ARQUITETURA DO ZABBIX

Segundo (ZABBIX SIA - Overview, 2012) e (OLUPS, 2010), a solução Zabbix é composta por cinco elementos:

- ⇒ **Servidor:** É o componente central da arquitetura para o qual agentes reportam dados de disponibilidade e estatísticas. Nele, ficam guardadas todas as configurações e dados estatísticos e operacionais. O componente servidor está envolvido principalmente em coletar e gravar dados, disponibilizar mecanismos de alerta e visualização de dados.
- ⇒ **Armazenamento em banco de dados:** Local “físico” para o armazenamento de dados. Componente Banco de Dados Relacional (referencia) que armazena e relaciona os dados em tabelas.
- ⇒ **Interface WEB:** Provida para dar acesso ao Servidor Zabbix, a partir de qualquer lugar e a qualquer dispositivo.
- ⇒ **Proxy:** Componente opcional para monitoramento distribuído. O Proxy pode coletar dados de disponibilidade e performance a favor de um Servidor Zabbix. Pode ser benéfico ao servidor Zabbix distribuir a carga de monitoramento entre vários Proxys. Além disso, com o Proxy é possível monitorar ambientes onde a segurança é mais restrita ao ponto de não ser permitido acesso às configurações do firewall, (restrições com relação a portas de Entrada/Saída).
- ⇒ **Agente:** Agentes Zabbix são instalados para monitorar servidores de rede, coletando dados de seus recursos e aplicações locais, e enviando-os para o servidor Zabbix. O agente monitora itens. Os itens monitorados pelos agentes seguem a lógica das MIBs (*Management Information Base* – Base de Informação de Gerenciamento) (DIAS, 2001) do SNMP. Porém, o agente estende a capacidade de monitoramento, pois proporciona aos Administradores de Redes a possibilidade de customizar itens e ações executadas diretamente no sistema monitorado.

Os componentes do Zabbix podem estar instalados no mesmo equipamento exceto, normalmente, pelo agente, formando um servidor capaz de obter informações dos agentes através de diversos meios. Incluindo, por exemplo:

- ⇒ Via SNMP, IPMI, e monitoramento JMX (Java);
- ⇒ Checagem customizada (através do uso de programação com Scripts);

- ⇒ Instalação de agentes nativos em sistemas operacionais Baseados em UNIX ou Microsoft Windows;
- ⇒ Monitoramento WEB, verificando os códigos de resposta às requisições feitas a servidores HTTP;
- ⇒ Através de dados passados por agentes e Proxys Zabbix.

Na Figura 4 pode-se visualizar o mecanismo de integração entre os diversos tipos de equipamentos e as formas de notificações que a ferramenta oferece.

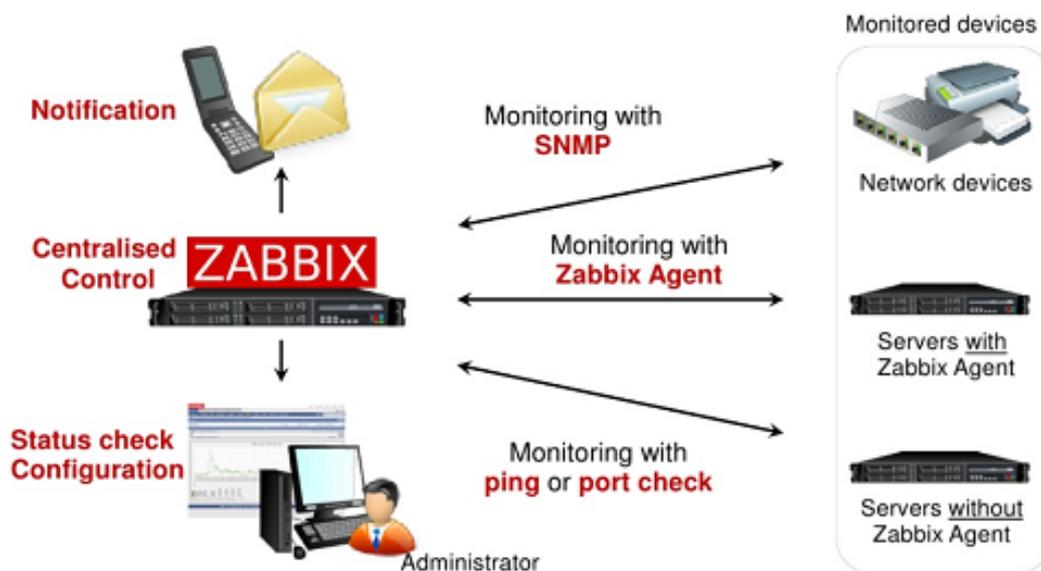


Figura 4. Componentes do Zabbix.

## 4 IMPLANTAÇÃO

### 4.1 ANÁLISE DO AMBIENTE

Neste tópico será apresentado as informações de cada PACS a ser monitorado, que estão conectados através de VPN's (*Virtual Private Network - Rede Privada Virtual*) como ilustrado na "Figura 1. Mapa de Rede do Grupo Alliar- Medicina Diagnóstica", onde a Matriz concentra o recebimento de todas as imagens de exames. Em cada Filial, existe um link utilizado para a transferência de imagens dos exames. A Tabela 2 apresenta a configuração dos links de cada um dos hosts que fazem parte do grupo Alliar. Embora o recomendado pudesse ser que ao menos cada filial tivesse um link dedicado, essa não é a realidade como pode ser verificado nas filiais de Dourados e Campo Grande.

Hostname	Link	Dedicado	Função	Localização
----------	------	----------	--------	-------------

SUPER PACS (CEDIMAGEM)	6MB/s	Sim	Concentrador, Servidor de imagens que recebe dados de todas Filiais.	Matriz, Juiz de Fora/MG.
PACS AXIAL	4MB/s	Sim	Servidor de imagens	Filial, Belo Horizonte/MG.
PACS UNIC	2MB/s	Sim	Servidor de imagens	Filial, Campo Grande/MS.
PACS UNIIMAGEM	2MB/s	Não, compartilhado.	Servidor de imagens	Filial, Dourados/MS.
PACS SONIMED	2MB/s	Não, compartilhado.	Servidor de imagens	Filial, Campo Grande/MS.
PACS SOM	4MB/s	Sim	Servidor de imagens	Filial, Belém do Pará/PA.
PACS SABEDOTI	4MB/s	Sim	Servidor de imagens	Filial, Ponta Grossa/PR.
PACS PLANI	4MB/s	Sim	Servidor de imagens	Filial, São José dos Campos/SP.
PACS DIIMAGEM	2MB/s	Não, compartilhado.	Servidor de imagens	Filial, Campo Grande/MS.

**Tabela 2.** Informações dos Hosts.

Todos os equipamentos das filiais pertencem ao Grupo Alliar, mas são vistas como empresas distintas, isto é, separadas uma das outras. Logo, para o monitoramento dos equipamentos das filiais foi adotado o método Simple Check<sup>2</sup> que é um método que realiza checagens que não necessitam de agentes instalados ou do protocolo SNMP. No equipamento (host) da Matriz, por outro lado, foi instalado o Agente do Zabbix. A configuração geral é resumida na Tabela 3.

Hostname	Monitoramento
SUPER PACS (CEDIMAGEM)	Agente Zabbix
PACS AXIAL	Simple Check
PACS UNIC	Simple Check
PACS UNIIMAGEM	Simple Check
PACS SONIMED	Simple Check
PACS SOM CSH	Simple Check
PACS SABEDOTI	Simple Check
PACS PLANI	Simple Check
PACS DIIMAGEM	Simple Check

**Tabela 3** – Monitoramento dos hosts.

<sup>2</sup> Para que o Zabbix possa coletar essas informações através do modelo de Simple Check é necessário a instalação do Fping, que não será abordado nesse artigo, para detalhes de instalação, acesse o link (<http://goo.gl/DHgJvs>) ou manual oficial do Zabbix, pelo link (<http://goo.gl/pcVCTr>).

## 4.2 CADASTRAMENTO DE GRUPOS E HOSTS

Os hosts são os ativos de rede monitorados pelo Zabbix. Cada host deve ser explicitamente incluído dentro do Zabbix para ter seus parâmetros de desempenho analisados. Além da inclusão de hosts, grupos também podem ser definidos. A criação de grupos facilita a separação dos equipamentos por semelhanças, facilitando, posteriormente, a análise de um conjunto de equipamentos.

Neste trabalho foi criado um grupo para tratar os servidores PACS do grupo Alliar (Menu Configuração do Zabbix, opção Grupos de hosts e botão Criar grupo de host). Após a criação do grupo, os hosts selecionados (servidores PACS) foram adicionados aos grupos (Menu Configuração, opção Hosts e, a seguir, seleção Criar Host). A adição de cada host é apresentada na Figura 5.

Interfaces do agente	Endereço IP	Nome DNS	Connectado a	Porta	Padrão
	197.1		IP DNS	0	

Figura 5. Cadastro de Host.

Como pode ser visualizado na Figura 5, é necessário preencher o nome do host como, exemplo, pacs01FIR, o nome de exibição, isto é, o nome que será exibido, por exemplo PACS AXIAL. Outras configurações incluem o grupo para organização do acesso às máquinas e as informações sobre a interface de acesso aos dados, incluindo o endereço IP válido do host na rede, a porta da interface de transporte e se o host está sendo ou não monitorado.

Após a inclusão dos hosts é possível, dentro do próprio Zabbix, realizar a listagem com informações sobre o monitoramento realizado. Essa listagem é apresentada na Figura 6. As informações específicas, isto é, a especificação daquilo que deve ser monitorado é apresentado na seção a seguir.

<input type="checkbox"/>	Nome	Aplicações	Itens	Triggers	Gráficos	Autobusca	Interface	Templates	Status
<input type="checkbox"/>	PACS AXIAL	Aplicações (1)	Itens (10)	Triggers (9)	Gráficos (3)	Autobusca (0)	187.1.██████████	Template Simple Check	Monitorado
<input type="checkbox"/>	PACS DIIMAGEM	Aplicações (1)	Itens (11)	Triggers (9)	Gráficos (3)	Autobusca (0)	177.201.██████████	Template Simple Check	Monitorado
<input type="checkbox"/>	PACS PLANI	Aplicações (1)	Itens (10)	Triggers (9)	Gráficos (3)	Autobusca (0)	200.220.██████████	Template Simple Check	Monitorado
<input type="checkbox"/>	PACS SABEDOTTI	Aplicações (1)	Itens (10)	Triggers (9)	Gráficos (3)	Autobusca (0)	187.16.██████████	Template Simple Check	Monitorado
<input type="checkbox"/>	PACS SOM	Aplicações (1)	Itens (10)	Triggers (9)	Gráficos (3)	Autobusca (0)	189.2.██████████	Template Simple Check	Monitorado
<input type="checkbox"/>	PACS SONIMED	Aplicações (1)	Itens (10)	Triggers (9)	Gráficos (3)	Autobusca (0)	177.1.██████████	Template Simple Check	Monitorado
<input type="checkbox"/>	PACS UNIC	Aplicações (1)	Itens (10)	Triggers (9)	Gráficos (3)	Autobusca (0)	177.201.██████████	Template Simple Check	Monitorado
<input type="checkbox"/>	PACS UNIMAGEM	Aplicações (1)	Itens (10)	Triggers (9)	Gráficos (3)	Autobusca (0)	177.201.██████████	Template Simple Check	Monitorado

Figura 6. Lista de Host Monitorados.

### 4.3 ESPECIFICAÇÃO DE TEMPLATES PARA MONITORAMENTO

No Zabbix, um template permite a especificação de um conjunto de parâmetros de monitoramento que podem incluir, itens, aplicações, gráficos, entre outros. A criação de templates é importante para que um host ou grupo de hosts possa ser associado a este, de forma que todos os elementos especificados no template passem a funcionar sobre o host em questão. Neste trabalho, um único template foi criado, denominado “Template Simple Check”.

#### 4.3.1 CRIANDO TEMPLATES

Neste trabalho os hosts são monitorados através de um método chamado Simple Check. Esse método realiza checagens que não necessitam de SNMP e nem de agentes instalados, o que é desejável, considerando que a análise será realizada a partir da matriz sem a necessidade de configurações independentes nas filiais. No método Simple Check são retornados valores básicos de 0 ou 1, “sim” ou “não” respectivamente.

Para realizar criação do template (menu Configurações, opção Templates e, em seguida, opção Criar Template). Nesse processo as seguintes informações devem ser preenchidas:

- ⇒ Nome do Template: Template Simple Check.
- ⇒ Nome de exibição: Template Simple Check.
- ⇒ Grupos: Informe o nome do grupo de hosts para esse template (Novo grupo) ou selecione um que já existe.

Uma vez especificado o template, é necessário povoá-lo, com aplicações, itens e gráficos. Na configuração de templates (Configurações > Templates), basta selecionar o template construído (Template Simple Check) e escolher a opção Aplicações a fim de associar uma aplicação a esse template. Uma aplicação é um quesito a ser monitorado como por exemplo, uso de CPU, consumo de memória, consumo de banda etc. Neste trabalho o objetivo é especificar uma aplicação que monitora a disponibilidade dos links, portanto, foi

criada uma aplicação denominada “Disponibilidade”, sendo esse valor informado no campo nome de uma nova aplicação.

Aplicações são normalmente formadas por um conjunto de itens individualmente avaliados. No caso da aplicação disponibilidade, anteriormente construída, será necessário avaliar o tempo de resposta entre a matriz e cada uma das filiais. Esse item pode ser especificado através do protocolo ICMP (Internet Control Message Protocol) (TORRES, 2007). Comandos desse protocolo podem ser periodicamente enviados com o objetivo de obter, como resposta, o tempo de tráfego da mensagem. O atraso na comunicação, denominado latência, é justamente o parâmetro que pode implicar na ausência de disponibilidade do serviço de replicação do PACS, caso valores elevados sejam objetos.

Para criar o item em questão, na página de templates do Zabbix, basta localizar o template criado e escolher a opção Itens selecionando, em seguida, o botão “Criar Item”. Neste trabalho a seguinte configuração foi utilizada:

- ⇒ Nome: nome do Item, definimos “Ping Disponibilidade”.
- ⇒ Tipo de Monitoramento: Monitoração simples.
- ⇒ Chave: icmping[,,60,], icmpingsec
- ⇒ Tipo de informação: Numérico (inteiro sem sinal).
- ⇒ Tipo de dados: Decimal.
- ⇒ Intervalo atualização: 60
- ⇒ Aplicações: Disponibilidade.

Para acompanhar os resultados de uma aplicação, gráficos podem ser especificados e associados ao template. Considerando a utilização de gráficos como uma opção que traz facilmente a informação, novamente na página de templates do Zabbix, através da opção Gráficos foi especificado um gráfico relativo à disponibilidade com os seguintes parâmetros.

- ⇒ Nome: nome do gráfico, adotaremos ICMP Ping – Disponibilidade.
- ⇒ Demais opções padrão
- ⇒ No campo Itens, clique no botão Adicionar. Será aberta uma janela “pop-up”. Marque o Item “Ping Disponibilidade” anteriormente criado e no botão Selecionar.
- ⇒ Clique no botão Salvar.

#### **4.4 TRIGGERS (AÇÕES OU “GATILHOS”)**

Além das configurações de monitoramento, é ideal, para o objetivo deste trabalho, que alterações na aplicação sejam reportadas caso valores limítrofes sejam atingidos. Para isso, triggers (gatilhos) podem ser utilizadas. Triggers são ações configuradas para cada evento que possa ocorrer em resposta a uma informação transmitida pelo host. Na abordagem desse artigo foram definidas duas trigger’s para alertar sobre a alta latência (“Ping” alto), ou então

na eminência de queda de link onde o acesso às informações desse host fiquem inacessível (Perda de conexão).

Para identificar se o host não está acessível foi especificado uma trigger com os seguintes parâmetros:

- ⇒ Nome: descrição da trigger, nesse exemplo caso foi utilizado parâmetro/função do Zabbix que retorna {HOSTNAME} = Nome de hostname do host, e {HOST.CONN} = Retorna o IP do host, juntamente com a descrição da frase.
- ⇒ Expressão: {Template Simple Check:icmpping[,,,60,].last(0)}=0
- ⇒ Risco: Atenção.

Complementarmente, para identificar o link com alta latência foi especificado uma trigger com os seguintes parâmetros:

- ⇒ Nome: descrição da trigger, nesse exemplo caso foi utilizado parâmetro/função do Zabbix que retorna {HOSTNAME} = Nome de hostname do host, juntamente com a descrição da frase.
- ⇒ Expressão: {Template Simple Check:icmppingsec.last(0)}>150
- ⇒ Risco: Informação.

## 5 RESULTADOS

Analisando as informações obtidas através do monitoramento dos hosts foi possível observar que ocorreram vários eventos de alta latência (“Ping alto”) e assim como, de host inacessível (“Host não responde a ping”). A Figura 7, detalha um número excessivo de eventos ocorridos para o PACS DIIMAGEM, foram 3135 ocorrências (vezes) que a latência ultrapassou a barreira de 150 ms (millessegundos). A partir dessa latência, mesmo que o link permaneça ativo, o protocolo do PACS passa a apresentar falhas na replicação do conteúdo, ou seja, falhas na cópia de imagens.

	Risco	Status	Informação	Última alteração ↓	Idade	Duração	Reconhecido	Host	Nome
+	Informação	OK		05 Jun 2014 22:00:40	25m 34s		Reconhecer (3135)	PACS DIIMAGEM	O PACS DIIMAGEM esta com o PING alto!

Figura 7. Falhas ocorridas no host PACS DIIMAGEM.

Avaliando a transferência de imagens de exames das filiais, constatamos que índices de alta latência no link acima de 5% e queda do link com valores acima de 3% é um fator para que contribui para a falta de sincronismo na cópia das imagens de exames para matriz, na Tabela 4 abaixo pode-se constatar esses valores:

Host	Total Exames Filial	Total Exames Matriz	Disponibilidade Link (%) – 1 dia.	Indisponibilidade	Latência (%) – 1 dia.	Alta Latência
PACS DIIMAGEM	252	104	96.9261%	3.0739%	70.3116%	29.6884%
PACS PLANI	467	467	96.1663%	3.8337%	99.6549%	0.3451%
PACS SABEDOTTI	182	182	100%	0%	99.5807%	0.4193%
PACS SOM	143	143	100%	0%	98.0530%	1.9470%
PACS SONIMED	44	41	100%	0%	91.7825%	8.2175%
PACS UNIC	35	33	100%	0%	94.4452%	5.5548%
PACS UNIMAGEM	61	37	100%	0%	94.0155%	5.9845%

**Tabela 4 – Disponibilidade de Link e Latência.**

As Figuras 7 e 8 exemplificam o filtro utilizado para confecção da Tabela 4 e a validação dos valores informados.

⌵ Filtrar ⌵				
Grupo de hosts	PACS ALLIAR			
Host	PACS DIIMAGEM			
Período	De	02 / 06 / 2014	00 : 00	
	Até	02 / 06 / 2014	23 : 59	
<input type="button" value="Filtrar"/> <input type="button" value="Limpar"/>				
Nome	Incidentes	Ok	Desconhecido	Gráfico
<a href="#">Equipamento diima1FIR 177.201.67.75 não responde ao (PING).</a>	3.0739%	96.9261%	0.0000%	<a href="#">Mostrar</a>
<a href="#">O PACS DIIMAGEM esta com o PING alto!</a>	29.6884%	70.3116%	0.0000%	<a href="#">Mostrar</a>

**Figura 7 – Filtro disponibilidade PACS DIIMAGEM.**

⌵ Filtrar ⌵				
Grupo de hosts	PACS ALLIAR			
Host	PACS SABEDOTTI			
Período	De	02 / 06 / 2014	00 : 00	
	Até	02 / 06 / 2014	23 : 59	
<input type="button" value="Filtrar"/> <input type="button" value="Limpar"/>				
Nome	Incidentes	Ok	Desconhecido	Gráfico
<a href="#">Equipamento sabmat 187.16.46.228 não responde ao (PING).</a>	0.0000%	100.0000%	0.0000%	<a href="#">Mostrar</a>
<a href="#">O PACS SABEDOTTI esta com o PING alto!</a>	0.4193%	99.5807%	0.0000%	<a href="#">Mostrar</a>

**Figura 8 – Filtro disponibilidade PACS SABEDOTTI.**

## 5.1 RESULTADOS POR GRÁFICOS

No gráfico apresentado pela Figura 9, demonstra-se as variações de latência (“ping”) para o host PACS DIIMAGEM, podendo facilmente identificar a instabilidade e queda do link em alguns momentos. Essa instabilidade onde o limite desejável para transmissão ultrapassa o valor de 150ms (milissegundos), causa ao sistema de PACS o não recebimento das imagens por completo, inviabilizando o diagnóstico. Nesse momento deve-se interromper o envio das imagens entre os hosts e executar manualmente até que o link retorne a condição de estável para realização automatizada pelo sistema PACS.

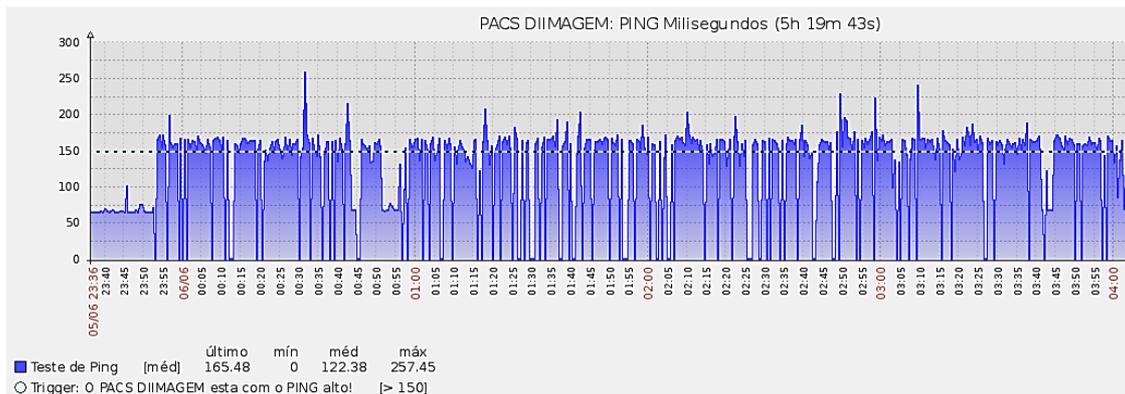


Figura 9. Instabilidade de link para PACS DIIMAGEM.

Para efeitos de comparação o host PACS AXIAL manteve-se em grande parte do tempo estável, garantindo a eficiência da cópia das imagens para a Matriz Cedimagem, como pode ser observado na Figura 10.

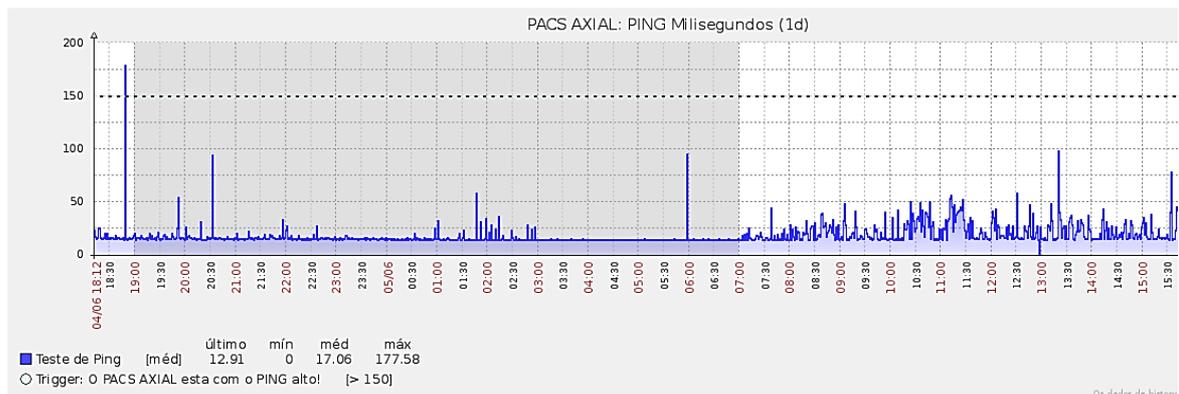


Figura 10. Comparação com host PACS AXIAL.

## 5.2 MAPA – “AMPLIANDO A VISÃO”

O Zabbix permite a personalização de mapas de acordo com a necessidade de cada administrador de rede. Com o uso de um modelo de Mapa o monitoramento torna-se ainda mais fácil, já que é possível adicionar vários hosts de uma forma que consiga monitorá-los em uma visão ampla. Na Figura 10, pode-se verificar que o host Super PACS (Matriz – Concentrador)

está com a capacidade em disco (HD) em menos de 20% livre, enquanto que o host da Filial PACS Unic não está acessível, uma vez que não responde a solicitação do Zabbix.

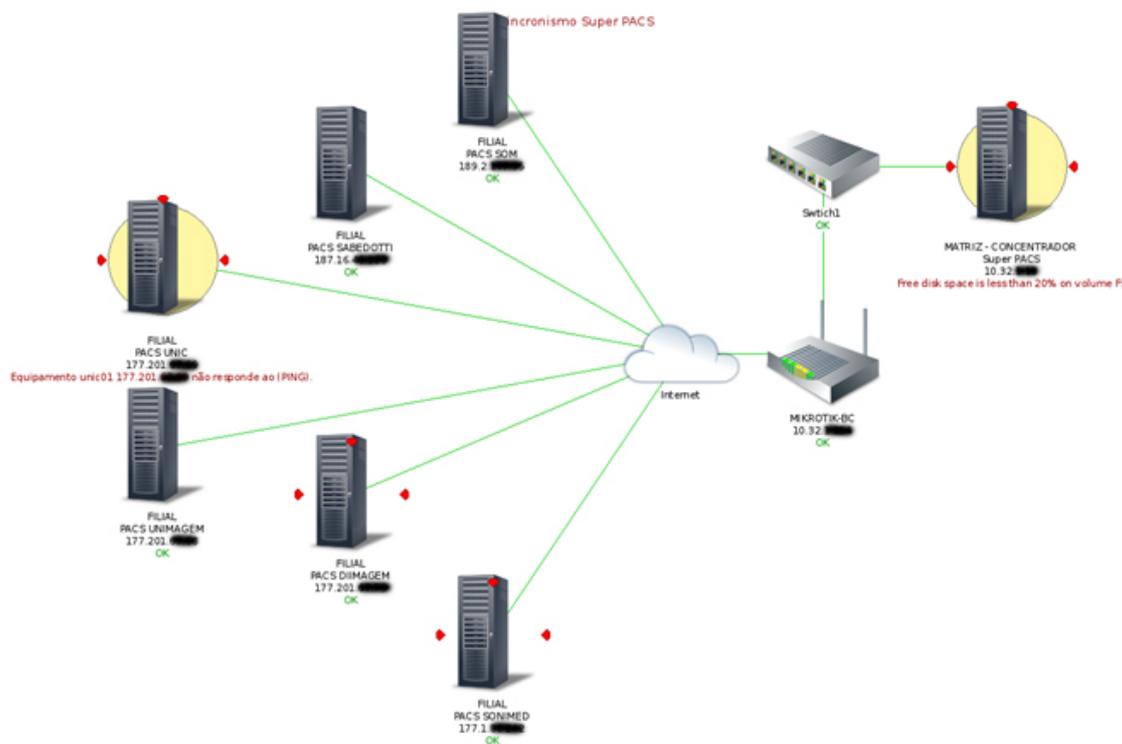


Figura 10. Monitoramento com Mapa Personalizado

## 6 - CONCLUSÃO

Para o correto funcionamento de qualquer rede de computadores é necessário o gerenciamento da mesma através de certas ferramentas, verificando assim erros, falhas, status e qualquer tipo de ação executada nos *hosts*, o que possibilita um melhor planejamento para aumentar o tempo de disponibilidade dos recursos.

No artigo, foi utilizado a ferramenta Zabbix para monitorar hosts que realizam a transferência, cópia de imagens de exames entre filiais para a matriz e através das informações desse monitoramento podemos perceber o quanto a ferramenta Zabbix é eficaz, mesmo quando utilizando-se de um monitoramento simplificado sem a necessidade da instalação do agente, através do modelo simple check aplicado para a maioria dos hosts, salvo o host principal Super PACS que teve o agente instalado.

Por fim, constatou-se que a baixa velocidade dos links, instabilidade na conexão e a alta latência comprometem significativamente a transferência e cópia das imagens de exames enviadas pelas Filiais do Grupo Alliar – Medicina Diagnostica para a Concentradora Matriz, conforme observou-se no durante todo item 5 deste artigo. E, finalmente, pode-se concluir que, filiais com links

compartilhados e/ou abaixo de 2Mb/s como, por exemplo, PACS DIIMAGEM existe um grande comprometimento no serviço de transferência de imagens.

Esse artigo, traz consigo informações uteis e factíveis para que as empresas do grupo possa investir em links de capacidade de 4MB/s, evitando assim problemas no serviço oferecido.

## 7 REFERÊNCIAS

[1] DÉO, André; PIRES, Aécio. **Gerência de Redes com Zabbix**. Revista Espirito Livre, n. 18, p. 69-73, Set/2010.

[2] LESSA, Demian. **O Protocolo de Gerenciamento RMON**. Rede Nacional de Ensino e Pesquisa (RNP), 15 jan. 1999. Disponível em: <<http://www.rnp.br/newsgen/9901/rmon.html>>. Acesso em: 20 abr. 2014.

[3] JUNQUEIRA, Wagner; DÉO, André. **Implementando gerenciamento de redes de computadores usando Nagios e Zabbix**. Disponível em: <<http://goo.gl/6NlvI7>>. Acesso em: 24 fev. 2014.

[4] FACHINI, Thiago. **Implementação da ferramenta Zabbix para monitoramento reativo**. 27 nov. 2010. Disponível em: <[http://www.ulbra.inf.br/joomla/images/documentos/TCCs/2010\\_2/redes-thiago%20fachini.pdf](http://www.ulbra.inf.br/joomla/images/documentos/TCCs/2010_2/redes-thiago%20fachini.pdf)>. Acesso em: 15 fev. 2014.

[5] LOZANO, Fernando. **Arquitetura de Redes TCP/IP**, 08 Ago. 1998. Disponível em: <<http://www.clubedohardware.com.br/artigos/Arquitetura-de-Redes-TCP-IP/329>>. Acesso em: 18 jun. 2014.

[6] DIAS, Beethovem; JÚNIOR, Nilton. **Protocolo de Gerenciamento SNMP, 2001**. Disponível em: <<http://www.rederio.br/downloads/pdf/nt00601.pdf>>. Acesso em: 18 jun. 2014.

[7] BLACK, Tomas. **Comparação de Ferramentas de Gerenciamento de Redes**, Dezembro de 2008. Disponível em: <<http://www.lume.ufrgs.br/bitstream/handle/10183/15986/000695315.pdf>> Acesso em: 18 jun. 2014

[8] PIRES, Aécio. **Aplicando recomendações de segurança na instalação do Zabbix**. Julho 2013. Disponível em: <<http://goo.gl/Q2mjVo>>. Acesso em: 15 fev. 2014.

[9] MARQUES, Paulo; SALOMÃO, Samuel. **PACS: Sistemas de Arquivamento e Distribuição de Imagens**. Revista Brasileira de Física Médica. 2009;3(1):131-9. Disponível em: <[http://www.abfm.org.br/rbfm/publicado/rbfm\\_v3n1\\_131-9.pdf](http://www.abfm.org.br/rbfm/publicado/rbfm_v3n1_131-9.pdf)>. Acesso em: 18 jun. 2014.

[10] ZABBIX SIA - Overview. **Zabbix SIA – Documentation from Zabbix Overview**. 4 Fev. 2014. Disponível em:

<<https://www.zabbix.com/documentation/2.0/manual/introduction/overview>>.

Acesso em: 19 jan. 2014.

[11] OLUPS, Rihards. **Zabbix 1.8 Network Monitoring** – Monitor your network’s hardware, servers, and web performance effectively and efficiently. Abril 2010. MUMBAI (BIRMINGHAM): Packt Publishing.

[12] ZABBIX SIA - **Distributed Monitoring** - Distributed Monitoring - Proxies. 28 set. 2012. Disponível em:

<[https://www.zabbix.com/documentation/2.0/manual/distributed\\_monitoring/proxies](https://www.zabbix.com/documentation/2.0/manual/distributed_monitoring/proxies)>. Acesso em: 27 mai. 2014.

[13] ZABBIX SIA - Features. **Zabbix Features**. 28 dez. 2011. Disponível em: <<https://www.zabbix.com/documentation/2.0/manual/introduction/features>>.

Acesso em: 10 jan. 2014.

[14] TORRES, Gabriel. ICMP (Internet Control Message Protocol), 24 Abr. 2007. Disponível em: <<http://www.clubedohardware.com.br/artigos/Como-o-Protocolo-TCP-IP-Funciona-Parte-2/1352/4>>. Acesso em: 18 jun. 2014.