UNIVERSIDADE ESTADUAL DA PARAÍBA - UEPB
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS - CCEA
CAMPUS VII - GOVERNADOR ANTÔNIO MARIZ
UEPB

Leonardo Batista Nunes

Gerenciamento de uma Rede de Computadores em um Ambiente Corporativo (UEPB/Campus VII) Utilizando o Software Zabbix

PATOS
2014

Leonardo Batista Nunes

Gerenciamento de uma Rede de Computadores em um Ambiente Corporativo (UEPB/Campus VII) Utilizando o Software Zabbix

Monografia apresentada ao Curso de Licenciatura em Computação da Universidade Estadual da Paraíba UEPB, em cumprimento à exigência para obtenção do grau de Licenciatura em Computação.

Orientador:
Prof°. Dr. Elder Eldervitch Carneiro de Oliveira

Patos
2014

UEPB - SIB - Setorial - Campus VII

N973g Nunes, Leonardo Batista

Gerenciamento de uma rede de computadores em um ambiente corporativo (UEPB/CAMPUS VII) utilizando o Software Zabbix [manuscrito] / Leonardo Batista Nunes. - 2014.

66 p. : il.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Computação) - Universidade Estadual da Paraíba, Centro de Ciências Exatas e Sociais Aplicadas, 2014.

"Orientação: Prof. Dr. Elder Eldervitch Carneiro de Oliveira, Coordenação de Ciências da Computação".

1. Redes de computadores. 2.Gerência de redes. 3. Zabbix. I. Título.

21. ed. CDD 004.6

Leonardo Batista Nunes

Gerenciamento de uma Rede de Computadores em um Ambiente Corporativo (UEPB/Campus VII) Utilizando o *Software* Zabbix

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura em Computação da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do grau de Licenciado em Computação

Aprovado em 26 de fevereiro de 2014

BANCA EXAMINADORA

Elder Eldervitch Carneiro de Oliveira
(Orientador)

Jannayna Domingues Barros Filgueira
(Examinadora)

Leonardo da Costa Santos
(Examinador)

Agradecimentos

Ao término deste trabalho, deixo aqui meus sinceros agradecimentos:

Ao Prof°. Dr. Elder Eldervitch C. de Oliveira, por toda dedicação, paciência e estímulo em sua orientação;

A todos os professores da Universidade Estadual da Paraíba campus VII Patos-PB;

Aos professores da banca pelas valiosas sugestões;

A minha família, pelo incentivo e segurança que me passaram durante todo esse período;

Aos amigos do curso de Licenciatura em Computação pelo agradável convívio;

Ao grupo GEMCA por ter cedido o espaço e a infraestrutura para realização deste trabalho;

A todos que direta ou indiretamente contribuíram para a realização deste trabalho;

“ *Só há duas tragédias na vida: uma é não se conseguir o que se quer,*
a outra é consegui-lo.”
Oscar Wilde.

Resumo

As redes de computadores foram concebidas a princípio como um meio de compartilhar dispositivos periféricos como impressoras, modens, dentre outros. Sendo utilizadas inicialmente apenas em ambientes acadêmicos, pelo governo e empresas de grande porte, hoje as redes de computadores estão presentes em ambientes diversos como residencias, escolas, *shoppings* e em instituições corporativas em geral. A medida que essas redes crescem e se tornam mais complexas gerencia-las se mostra uma atividade difícil, pois se trata de lidar com riscos constantes que podem causar um mal funcionamento da rede. Para desempenhar essa atividade deve-se utilizar um Sistema de Gerenciamento de Rede (*Network Manager System* - MNS). Um sistema bastante conhecido é o Zabbix. Assim este trabalho tem como principal objetivo implementar uma solução de gerência em um ambiente corporativo fazendo uso de uma ferramenta *open-source* para monitoramento de uma rede de computadores com a finalidade de monitorar a disponibilidade e o desempenho dos dispositivos presentes na rede. O monitoramento de uma rede com Zabbix consiste no tipo de arquitetura centralizada onde uma estação gerente é responsável pela coleta e análise dos dados nas estações agentes. Através de alertas e da geração e análise de gráficos é possível identificar os sintomas que apontam para um ou mais problemas na rede o que provoca um baixo nível de qualidade dos serviços oferecidos. Com a implantação de um Sistema de Gerenciamento de Rede, é possível ter um controle sobres os equipamentos da rede, aumentando a qualidade no serviços oferecidos a medida que os possíveis problemas são detectados rapidamente. Parâmetros relevantes a análise de desempenho da rede monitorada foram analisados e discutidos, bem como uma solução de gerência de redes foi proposta.

PALAVRAS-CHAVE: Redes de computadores, Gerência de redes e Zabbix.

Abstract

Computer networks were initially conceived as a means to share peripheral devices like printers, modems, among others. Initially being used only in academic settings, government and large companies, today computer networks are present in various environments, such as residences, schools, shopping malls and corporate institutions in general. With the growth of computer networks, they become more complex, so manage them proves a difficult activity, because it's dealing with constant risks that may cause a network loss performance. To perform this activity must use a Network Manager System (MNS). A well-known system is the Zabbix. Thus this work aims to implement a management solution in a corporate environment by making use of an open-source tool for monitoring a computer network in order to monitor the availability and performance of the devices on the network. Network monitoring with Zabbix is of the type of centralized architecture where a station manager is responsible for the collection and analysis of data at stations agents. Through alerts and the generation and analysis of graphs is possible to identify the symptoms that point to one or more network problems, which causes a low level of quality of services offered. With the implementation of a Network Management System, it's possible to have a control about devices on the network, increasing the quality of services offered as potential problems are detected quickly. Parameters relevant to the performance analysis of monitored network were analyzed and discussed, as well as a network management solution has been proposed.

Keywords: Computer networks, Network management and Zabbix.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Siglas e Acrônimos

ANS.1	*Abstract Syntax Notation One*
CMIP	*Commom Management Information Protocol*
CMISE	*Commom Management Information Service Element*
CPU	*Central Processing Unit*
Daemon	*Disk And Execution MONitor*
DHCP	*Dynamic Host Configuration Protocol* - Protocolo de configuracão dinâmica de host
DNS	*Domain Name System* - Sistema de Nomes de Domínios
GB	*GigaBit*
GPL	*General Public license*
IP	*Internet Protocol*
ISO	*International Organization For Stardadization*
ITU-T	*International Telecommunications Standardisation Sector*
MB	*MegaBit*
MIB	*Management Information Base*
NMS	*Network Management Stations*
NOCs	*Network Operation Center*- Centro de Operacões de rede
OID	*Objetic Identifier*
OSI	*Open Systems Interconnection*
PDU	*Protocol data unit*
QoS	*Quality of Service*
RFC	*Request for Comments*
SMI	*Structure Management Information*
SNMP	*Simple Network Management Protocol*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*

1 INTRODUÇÃO

A informação é o bem mais precioso de uma organização. Antes do advento da informática essas informações eram armazenadas em arquivos, e todo o registro e movimentação eram feitas em papel. A utilização das redes de computadores proporcionou um ganho considerável no tratamento dessas informações, agilizando o processamento e a disponibilidade destas (MELO, 2008).

As redes de computadores tem ganhado grande popularidade e se tornado maiores e mais complexas, com isso as instituições corporativas, empresas, bancos, setor elétrico, de saúde e outros estão dependendo cada vez mais dessa tecnologia.

Porém, com o rápido crescimento, as redes foram se tornando cada vez mais integradas as atividades das organizações. Com isso as vantagens oferecidas pelas redes foram além do simples compartilhamento de dispositivos. As redes de computadores logo passaram a ser parte imprescindível nas atividades das organizações, oferecendo serviços, recursos, simplificando e aumentando a produtividade.

Qualquer organização que tenha uma rede de computadores deve obter meios para manter um bom funcionamento, já que é por ela que as informações relevantes ao funcionamento da organização trafegam. Para isso precisa-se de um acompanhamento constante monitorando e alertando os administradores da rede com a maior rapidez possível.

A atividade de gerência de redes consiste em monitorar e controlar os diversos elementos existentes na rede, sejam eles físicos ou lógicos e assim assegurar um bom nível de QoS *(Quality of Service)*. Porém devido ao grande crescimento das redes de computadores prevê a quantidade de pessoal necessário para manter um sistema de gerenciamento é muito difícil, o tamanho da equipe pode variar de acordo com a complexidade e porte da rede. Para essa atividade é necessário a instalação de um sistema de gerenciamento integrado que monitore a rede alertando os administradores sobre qualquer alteração nos serviços prestados. Uma solução de gerência bem conhecida e com excelente qualidade de monitoramento é a utilização do software Zabbix (ZABBIX, 2013).

Dentre as várias definições para o gerenciamento de redes, dois modelos se destacam o da ISO *(International Organization For Stardadization)* que utiliza o CMIP

(Commom Management Information Protocol) e o modelo Internet (TCP/IP) que utiliza o SNMP *(Simple Network Management Protocol)*. O modelo TCP/IP é o padrão mais usado atualmente em redes de médio e grande porte, locais e metropolitanas (BRISA, 1993).

1.1 Justificativa

Com o grande crescimento das redes de computadores tanto em quantidade como em diversidade de dispositivos, essa tecnologia tem se estabelecido como uma forma muito importante para o compartilhamento de informações e recursos disponíveis. A tecnologia das redes de computadores agiliza o processamento dessas informações além de facilitar o acesso de forma rápida e segura.

Assim uma rede de computadores tem grande importância em uma instituição, uma boa qualidade nos serviços prestados pela rede influi, inclusive no fator econômico. Segundo um estudo realizado pela Universidade de Austin, EUA, uma falha na rede produz um prejuízo na receita e aumenta o custo de uma empresa, esse custo pode variar de 2% da receita anual no primeiro dia, podendo chegar até 30% no 30º dia. Tanto os custos da falta dos serviços prestados pela rede quanto os inerentes a solução do problema são altos, pois muitas vezes essa solução requer uso de equipamento redundante, encaminhamento à outra fonte de atendimento (outro terminal, por exemplo) ou reconfiguração. Tudo isso demanda tempo e trás custos a instituição e aos usuários da rede (BRISA, 1993).

Tanto as pessoas quanto as corporações têm valorizado a informação e o meio no qual essas informações são transportadas, processadas e armazenadas tem requerido bastante atenção. Surge então a necessidade da redução de custos e melhoria da qualidade dos serviços oferecidos pelas redes, para isso há a necessidade de implantar um sistema de gerenciamento de redes. Em um ambiente universitário não é diferente, a necessidade por um sistema de gerenciamento de redes se faz necessário em virtude do crescimento da instituição e a maior demanda do uso dos recursos por alunos e colaboradores. Dessa forma, há a necessidade de melhorar o desempenho proporcionalmente ao seu crescimento.

1.2 Objetivos

1.2.1 Objetivo Geral

Este trabalho tem como principal objetivo implementar uma solução de gerência em um ambiente corporativo fazendo uso de uma ferramenta *open-source* para monitoramento de uma rede local de computadores.

1.2.2 Objetivos Específicos

- Implementar a solução gerência Zabbix na rede de computadores da UEPB/Campus-VII;
- Configurar o ambiente de Gerenciamento para coleta dos dados;
- Apresentar resultados obtidos;
- Propor uma solução de Gerência de rede ao CPD da Universidade Estadual da Paraíba campus VII.

1.3 Organização do texto

Este trabalho apresenta-se distribuído em 5 capítulos, onde busca-se evidenciar um referencial teórico e bibliográfico para o estudo de Gerência de Redes de Computadores, em seguida é proposto uma solução de gerência de redes com o software Zabbix e uma análise dos dados coletados.

O Capítulo 2 apresenta uma revisão bibliográfica sobre redes de computadores, os modelos e arquiteturas de gerência e os protocolos envolvidos no gerenciamento de redes de computadores.

O Capítulo 3 mostra o software Zabbix como alternativa para gerência de redes, apresentando suas principais características, componentes e requisitos para instalação.

No Capítulo 4 são apresentados os dados coletados na rede de computadores da UEPB campus VII, e a análise desses dados relatando aspectos sobre a disponibilidade e desempenho dos dispositivos presentes na rede monitorada.

O Capítulo 5 apresenta as conclusões desse trabalho e sugestões para trabalhos futuros relacionados a Gerencia de Redes de Computadores.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Introdução as redes de computadores

O século XX foi marcado por grandes aquisições tecnológicas porém a grande conquista se deu na área de processamento e distribuição de informações. Depois da instalação de redes de telefonia em todo mundo, da invenção do rádio e da televisão o maior avanço ocorreu na indústria da informática e lançamentos de satélites de comunicação. Apesar de relativamente jovem, a indústria da informática teve um progresso espetacular. Nas duas primeiras décadas os sistemas computacionais eram centralizados instalados em uma única sala, as vezes um único computador, chamado centro de computação. Empresas de médio porte dispunham apenas de um ou dois computadores, instituições maiores tinhas apenas poucas dezenas de computadores (TANENBAUM, 2003).

Porém esse sistema centralizado, uma sala com um grande computador (centro de computação) ao qual os usuários levam seu trabalho para processamento está obsoleto. Essa tecnologia de um único computador realizando todas as atividades computacionais de uma instituição deu lugar a tecnologia das redes de computadores, onde computadores separados mas, interconectados realizam essas tarefas.

As redes de computadores foram concebidas a princípio como meio de compartilhar dispositivos periféricos como impressoras modens dentre outros.

Uma rede de computadores pode ser definido como um conjunto de computadores autônomos interconectados por uma única tecnologia. Dois computadores estão interconectados quando podem trocar informações. Essa conexão pode ser feita por diferentes tipos de enlaces como fio de cobre, fibras ópticas, micro-ondas, ondas de infravermelho e satélites de comunicação (TANENBAUM, 2003).

Com o crescimento da internet que hoje abrange todas as áreas de diversas atividades o uso das redes de computadores vem se tornando um recurso indisponível em todos os ambientes onde existe um conjunto de computadores.

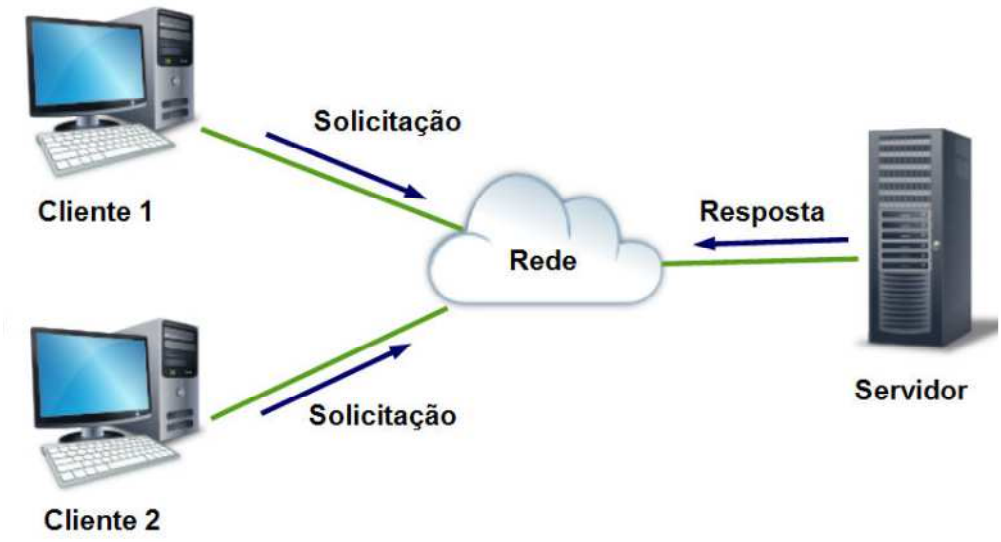
Sendo utilizadas inicialmente apenas em ambientes acadêmicos, pelo governo e empresas de grande porte, hoje as redes de computadores estão presentes em ambiente diversos como residências, escolas, shoppings e em instituições corpo-

rativas em geral. Essa tecnologia alcançou grande popularidade quando os computadores começaram a se espalhar pelo mundo comercial, e a medida que a facilidade ao acesso aos computadores cresceu o desenvolvimentos de programas complexos multiusuários como e-mail, banco de dados, internet, também aumentou (MENDES, 2007).

A Figura 1 mostra o modelo cliente/servidor, que é o modelo mais usado nas redes atualmente. Ele pode ser aplicado quando o cliente e o servidor estão localizados no mesmo local como uma instituição, empresa, ou mesmo uma residência, mas também podem estar geograficamente distantes, entre dois países por exemplo.

Quando uma pessoa acessa de seu computador uma página na Web esse modelo é empregado, com o computador pessoal sendo o cliente acessando um servidor remotamente. Geralmente um único servidor pode ser acessado por vários clientes ao mesmo tempo.

Figura 1: Rede com um servidor e dois clientes.



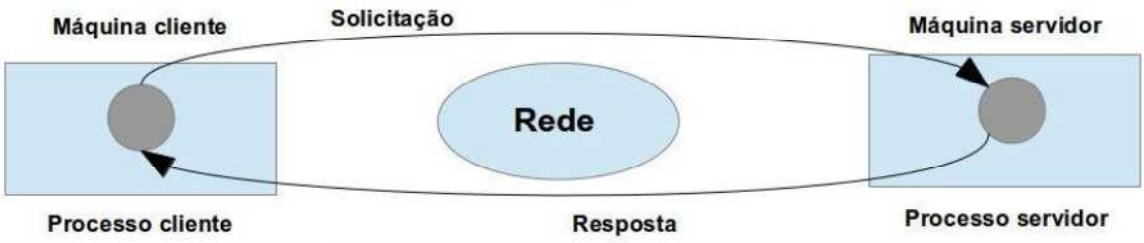
Fonte: autor

Normalmente clientes costumam ser computadores pessoais (*desktops, notbooks*), PDAs, etc, enquanto servidores são máquinas mais poderosas responsáveis por armazenar e distribuir páginas Web, vídeos em tempo real, serviços de *e-mail* e outros encontrados nas redes (KUROSE, 2006).

No contexto de *software* de rede há ainda outra definição de cliente e servidor. Podemos ter um programa cliente e um programa servidor (KUROSE, 2006). Um programa cliente é um *software* que funciona em um cliente ou sistema final, esse programa faz solicitações de serviços a um *software* que funciona em um outro sistema final, o programa servidor. Desse modo uma máquina em uma rede pode se

comportar como cliente e servidor ao mesmo tempo. Na Figura 2 vemos o modelo cli-

Figura 2: Modelo de uma rede cliente/servidor.



Fonte: Kurose (2006).

ente/servidor onde existem dois processos envolvidos, uma na máquina cliente e um na máquina servidora. A comunicação entre o cliente e o servidor acontece quando o processo cliente envia um mensagem ao processo servidor. Depois que o processo servidor recebe a solicitação, ele executa a tarefa solicitada ou coleta os dados solicitados e envia uma mensagem resposta de volta ao processo cliente.

2.2 Gerência de redes

2.2.1 Introdução a gerência de redes

A princípio as redes de computadores surgiram com a necessidade do compartilhamento de periféricos como: impressoras, leitores de fitas, dispositivos de armazenamento, etc. Porém com o rápido crescimento, as redes de computadores foram se tornando cada vez mais integradas as atividades das organizações. Com isso as vantagens oferecidas pelas redes foram além do simples compartilhamento de dispositivos. As redes logo passaram a ser parte imprescindível nas atividades das organizações, oferecendo serviços, recursos, simplificando e aumentando a produtividade.

A informação é o bem mais precioso de uma organização. Antes do advento da tecnologia das redes de computadores essas informações eram armazenadas em arquivos, onde todo o registro e movimentação das informações eram feitas em papel. A utilização das redes de computadores proporcionou um ganho considerável no tratamento dessas informações, agilizando o processamento e a disponibilidade (MELO, 2008). As informações que circulam na rede devem ser transportadas de modo rápido e confiável, desse modo é importante que os dados e dispositivos desse ambiente sejam monitorados, para que seja garantido sua QoS (*Quality of Service*- qualidade de serviço).

Para isso é necessário que os problemas que ocorram sejam resolvidos o mais rápido possível para que o bom funcionamento da rede seja mantido, sendo assim é necessário que se implante um sistema de gerência de redes.

A atividade de gerência de redes consiste em monitorar e controlar os diversos elementos existentes na rede, sejam eles físicos ou lógicos e assim assegurar um bom nível de *QoS*. Porém o grande crescimento em número e diversidade das redes e de seus componentes tem tornado essa atividade cada vez mais complexa. O isolamento e o teste dos problemas das redes têm-se tornado difíceis devido a duas principais causas (BRISA, 1993):

- Diversidade dos níveis de pessoal envolvido: operadores e controladores de rede, técnicos de manutenção, gerentes de sistemas de informações e gerente de comunicações;
- Diversidade de formas de controle e monitoração: embora os produtos envolvidos na rede se tornem gradativamente mais complexos, cada fornecedor oferece ferramentas próprias de controle de redes para monitorar seus produtos (BRISA, 1993)

Devido ao grande crescimento das redes de computadores prevê a quantidade de pessoal necessário para manter um sistema de gerenciamento é muito difícil, o tamanho da equipe pode variar de acordo com a complexidade e porte da rede. Alguns provedores de *backbone* maiores da internet dispõe de setenta pessoas ou mais em seus NOCs (*Network Operation Center*- Centro de Operações de rede) outros podem ter apenas uma.

Geralmente a tarefa de gerenciamento de rede é realizada por uma equipe, o pessoal do *help desk*, o operador da rede, a equipe de suporte técnico e o gerente da equipe de gerência. Porém não existe uma regra rígida sobre os profissionais que fazem parte dessa equipe, geralmente cada organização cria seu grupo de gerência de acordo com suas necessidades (SAUVé et al., 1993). Em organizações pequenas é comum que essas atividades sejam realizadas por apenas uma ou duas pessoas, que ao mesmo tempo são gerente suporte e operador da rede.

No entanto é necessário que esses profissionais tenham algum conhecimento na área de redes. O gerente é importante em um sistema de gerenciamento de redes, porém ele não é necessariamente um técnico em redes, por isso deve conter em sua equipe pessoal com conhecimentos mais apurados na área para solucionar os possíveis problemas. Ainda segundo (SAUVé et al., 1993),

> O gerente da equipe de gerência de rede não é necessariamente um técnico em redes. O gerente tem um certo conhecimento em redes, mas não no nível do suporte técnico. Dentre as atividades deste gerente encontram-se avaliar o desempenho da sua equipe de suporte, solicitar compra de equipamentos aplicações ou outros recursos necessários, providenciar treinamento adequado para a equipe, reesca-

> lonar a solução de problemas para outros membros da equipe quando a solução demora, etc.

Assim um gerente tem um papel mais administrativo, organizando as tarefas e recursos para que a atividade de gerência ocorra de forma eficiente e rápida.

Outro problema é que as redes atualmente são constituídas de equipamentos de múltiplos fornecedores o que faz com que os sistemas de gerenciamento se tornem deficientes.

Uma estrutura manual de gerenciamento baseada em papel só funciona quando a rede é pequena, em uma rede maior essa estrutura é incapaz de sequer registrar o universo dos incidentes (BRISA, 1993). Desde que as tecnologias da informação começaram a ser parte importante de empresas e instituições em geral também surgiu a necessidade de um gerenciamento dos dispositivos presentes nela. A área de gerência de redes:

> foi inicialmente impulsionada pela necessidade de monitoração e controle do universo de dispositivos que compõem as redes de comunicação. Atualmente as redes de computadores e seus recursos associados, além das aplicações distribuídas, tem se tornado fundamental e de tal importância para uma organização que, elas basicamente ”não podem falhar”. Isto significa que o nível de falhas e de degradação de desempenho aceitáveis está cada vez mais diminuindo, sendo este nível igual até a zero, dependendo da importância da rede para uma instituição (LIMA, 2011).

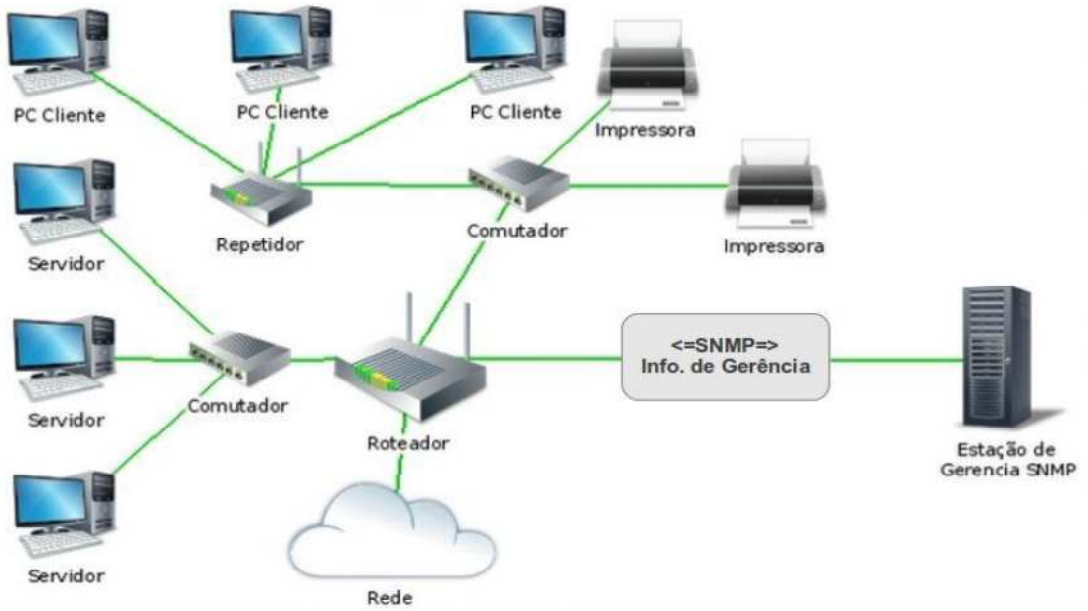
De modo geral um sistema de gerenciamento de rede necessita de alguns componentes para funcionar com eficiência. Em um sistema de gerenciamento de rede são necessário quatro componentes básicos (SAUVé et al., 1993):

- Os elementos gerenciados possuem um *software* especial chamado agente. Este *software* permite que o equipamento seja monitorado e controlado através de uma ou mais estações de gerência;
- Em um sistema de gerência de redes deve haver pelo menos uma estação de gerência. Em sistemas distribuídos existem duas ou mais estações de gerência. Em sistemas centralizados - mais comuns - existem apenas uma. Chamamos de gerente o software da estação de gerência que conversa diretamente com os agentes nos elementos gerenciados, seja com o objetivos de monitorá-los, seja com o objetivo de controlá-los. A estação de gerência oferece uma interface através da qual os usuários autorizados podem gerenciar a rede;
- Para que a troca entre gerentes e agentes seja possível é necessário que eles falem o mesmo idioma. O idioma que eles falam é um protocolo de gerência. Este protocolo permite operações de monitoramento (leitura) e controle (escrita);

- Gerentes e agentes podem trocar informações, mas não qualquer tipo de informação. As informações de gerência definem os dados que podem ser referenciados em operações do protocolo de gerência, isto é, dados sobre os quais gerentes e agentes conversam.

A Figura 3 apresenta um exemplo de uma arquitetura geral de um sistema de gerenciamento. Na rede representada no modelo, temos os elementos gerenciados como, computadores, roteadores, comutadores, impressoras, estes geralmente terão agentes instalados. A estação de gerência obtêm informações desses agentes através do protocolo SNMP (*Simple Network Management Protocol*).

Figura 3: Exemplo de sistema de gerenciamento.



Fonte: Sauvé et al. (1993).

2.2.2 Gerência Pró-Ativa e Gerência Reativa

O tempo que leva para que as medidas de correção de problemas na rede sejam tomadas, é muito importante. Pois quanto maior o tempo que os serviços oferecidos pela rede ficam indisponíveis, maior é o prejuízo para seus usuários.

Assim um conceito importante no gerenciamento de redes é a diferença entre gerência pró-ativa e reativa. A Gerência reativa é aquela em que o Administrador da rede apenas reage aos problemas que surgem (LENO JúNIOR, 2003). Utilizando um sistema para detecção desses problemas, depois de alertado, o administrador toma as devidas providências. Esse modelo é mais fácil de ser implantado, porém oferece menos qualidade nos serviços oferecidos na rede.

A Gerência pró-ativa apesar de ter uma implementação mais complicada é bem mais eficiente, pois resulta em um tempo menor de parada, melhorando a disponibilidade dos serviços na rede. Essa forma de gerência tem como prioridade monitorar a rede colhendo informações (sintomas), que possam revelar possíveis problemas na rede com antecedência. É mantido um histórico contendo informações estatísticas comparando valores para identificar comportamento estranho da rede (LENO JúNIOR, 2003).

2.2.3 Sistemas de Gerência Centralizada e Distribuída

Antes de implementar um Sistema de Gerenciamento, é necessário que se verifique qual arquitetura será mais adequada a rede. A arquitetura mais simples possui apenas uma estação de gerenciamento responsável por toda a rede, toda a informação coletada é enviada para uma única estação gerente central. Essa arquitetura mostrada na Figura 4 é conhecida como Gerência Centralizada (MAURO; SCHMIDT, 2001).

Figura 4: Sistema de gerenciamento centralizado.

Fonte: autor.

Para redes de pequeno porte esse tipo de arquitetura pode suprir as necessidades, essas redes são gerenciadas através da manipulação de agentes. Contudo com o crescimento da rede e o aumento de dispositivos presentes essa arquitetura se tornará um problema. A gerenciamento pode se tornar lento e ineficiente, devido ao grande número de informações que a estação gerente terá que receber (LENO JúNIOR, 2003).

Quando a rede crescer de modo que uma única estação de gerenciamento não for suficiente, a arquitetura mais adequada é a Distribuída. A implementação dessa arquitetura é mais complexa que a Centralizada. Essa arquitetura é composta

por duas ou mais estações de gerenciamento. Nessa arquitetura o gerente age como gerente e agente, assim ele é controlado e monitorado remotamente por outro gerente.

A Figura 5 ilustra um exemplo de gestão distribuída, onde existem duas estações gerentes, sendo uma delas intermediária. A estação intermediária faz o papel de gerente quando controla os agentes sob sua responsabilidade e atua no papel de agente quando controlado pela estação responsável por toda a rede.

Figura 5: Sistema de gerenciamento distribuído.

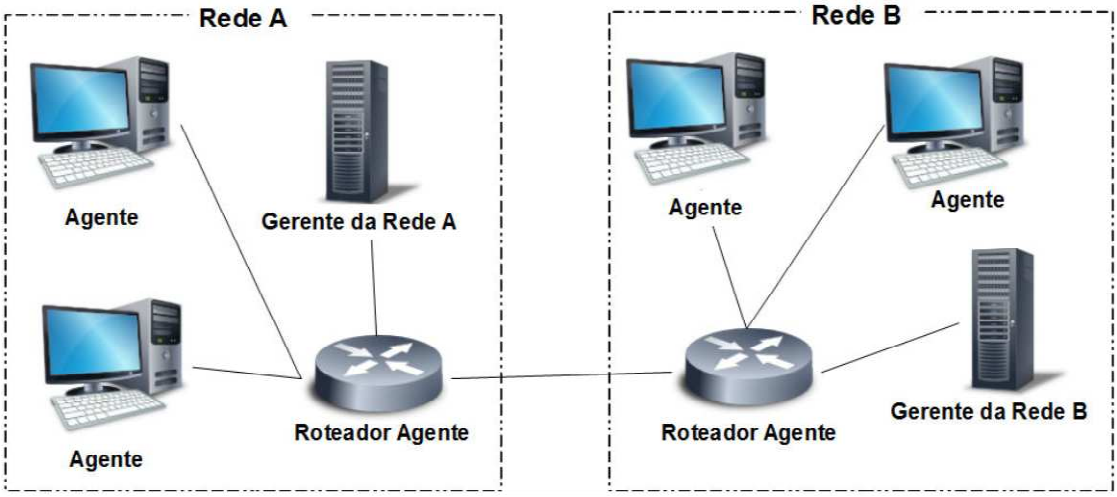
Fonte: autor.

Outra configuração de arquitetura é o modo híbrido como mostrado na Figura 6. Neste modelo o gerenciamento pode ser feito pelas duas estações gerentes, podendo se comportar de forma centralizada e em alguns momentos distribuída. Centralizado quando a rede estiver com funcionamento dentro da normalidade e distribuído nos momentos em que a rede estiver com tráfego elevado (MAURO; SCHMIDT, 2001). Na Figura 6 o Gerente da Rede A é responsável por gerenciar a Rede A e a Rede B tendo uma gerência centralizada, porém quando a rede estiver com tráfego elevado, o gerenciamento passa a ter uma arquitetura distribuída, e o Gerente da Rede B passa a realizar o monitoramento da Rede B. Isso evita um congestionamento na estação gerente da Rede A.

2.3 Modelos de gerenciamento

Desde o início um dos problemas encontrados na implementação de redes era a interoperabilidade entre as diversas máquinas. A ISO desenvolveu o modelo de referência OSI *(Open Systems Interconnection)* buscando a compatibilização por

Figura 6: Sistema de gerenciamento Híbrido. Fonte: do autor.



Fonte: do autor.

parte os vendedores. Com o esforço da ISO as deficiências de compatibilidade foram sendo superadas, e as redes cresceram em volume e importância (DOTTI, 1992).

Dentre as várias definições para o gerenciamento de redes, dois modelos se destacam o da ISO *(International Organization For Stardadization)* que utiliza o CMIP *(Commom Management Information Protocol)* e o modelo Internet (TCP/IP) que utiliza o SNMP *(Simple Network Management Protocol)*.

2.3.1 Modelo de Gerenciamento OSI

O modelo de referência de redes OSI (*Open Systems Interconnection*) foi resultado do trabalho de normalização de redes locais de comunicação de dados. Esse trabalho foi desenvolvido pela ISO (*International Standards Organization)* em colaboração da ITU-T (*International Telecommunications Standardisation Sector*).

Em um ambiente de gerenciamento OSI existem os conceitos de áreas funcionais, gerente, agente e objeto gerenciado. Neste modelo um processo gerente coleta e envia informações de gerenciamento a processos agentes (CASTELO BRANCO, 1999). Esse modelo funcional é característico da arquitetura cliente/servidor. Os componentes de gerência OSI seguem o paradigma de Orientação a Objetos, nessa abordagem os elementos gerenciados são representados por objetos. Um modelo genérico da troca de mensagens entre gerente e agente é mostrado na Figura 7.

Um gerente pode obter informações sobre objetos gerenciados e controla-los, transmitindo, para isso, operações de gerenciamento aos agentes. Já os agentes executam essas operações de gerenciamento sobre os objetos além de transmitir as

Figura 7: Relacionamento gerente, agente.

Fonte: Castelo Branco (1999).

notificações emitidas pelo objeto ao gerente (BRISA, 1993).

No Modelo de Gerência OSI, a troca de informações entre gerente e agente é realizada por meio de um protocolo. O CMISE - *Commom Management Information Service Element* e o CMIP - *Commom Management Information Protocol* tem essa função e juntos formam a base do Modelo OSI. O CMISE define as operações, serviços e parâmetros para um processo gerente, já o CMIP define as regras e mecanismos para que as trocas de informações entre gerente e agente aconteça (GIMENEZ, 2004).

No modelo de gerenciamento OSI, um objeto gerenciado é a representação de um recurso gerenciável, esse recurso pode ser tanto a nível de *hardware* como dispositivos de comunicação, como no contexto de *software* como aplicativos e serviços. Todo o conjunto de objetos gerenciados, e seus respectivos atributos que constituem um sistema de gerenciamento, formam a Base de Informação de Gerenciamento (MIB)(CASTELO BRANCO, 1999).

A ISO (documento ISO 7498-4) classifica a gerência de redes em cinco áreas funcionais: Gerência de Falhas, Gerência de Contas, Gerência de Configuração, Gerência de Desempenho e Gerência de Segurança. Apesar dessa classificação ter sido desenvolvida para um ambiente OSI, foi bastante aceita por parte dos fabricantes de *hardware* e *software* de rede tanto em tecnologia padronizada quanto proprietárias (GIMENEZ, 2004). A Tabela 1 mostra um resumo dessas áreas.

2.4 MIB *(Management Information Base)*

A comunicação entre os gerentes e agentes no modelo OSI é realizado através do protocolo CMIP *(Common Management Information Protocol)*. As informações

Tabela 1: Áreas funcionais OSI.

Gerência de Falhas	Implementa facilidades para detecção, isolamento e correção de operações que se apresentam anormais nos recurso de funcionamento da rede;
Gerência de Contas	Implementa facilidades para alocação dos recursos de rede e define métricas para uso desses recursos;
Gerência de Configuração	Implementa facilidades na atualização ou modificação dos recursos de rede;
Gerência de Desempenho	Implementa facilidades para avaliação e analise de desempenho dos recursos;
Gerência de Segurança	Implementa facilidades para proteger as operações dos recursos da rede

Fonte: Gimenez (2004).

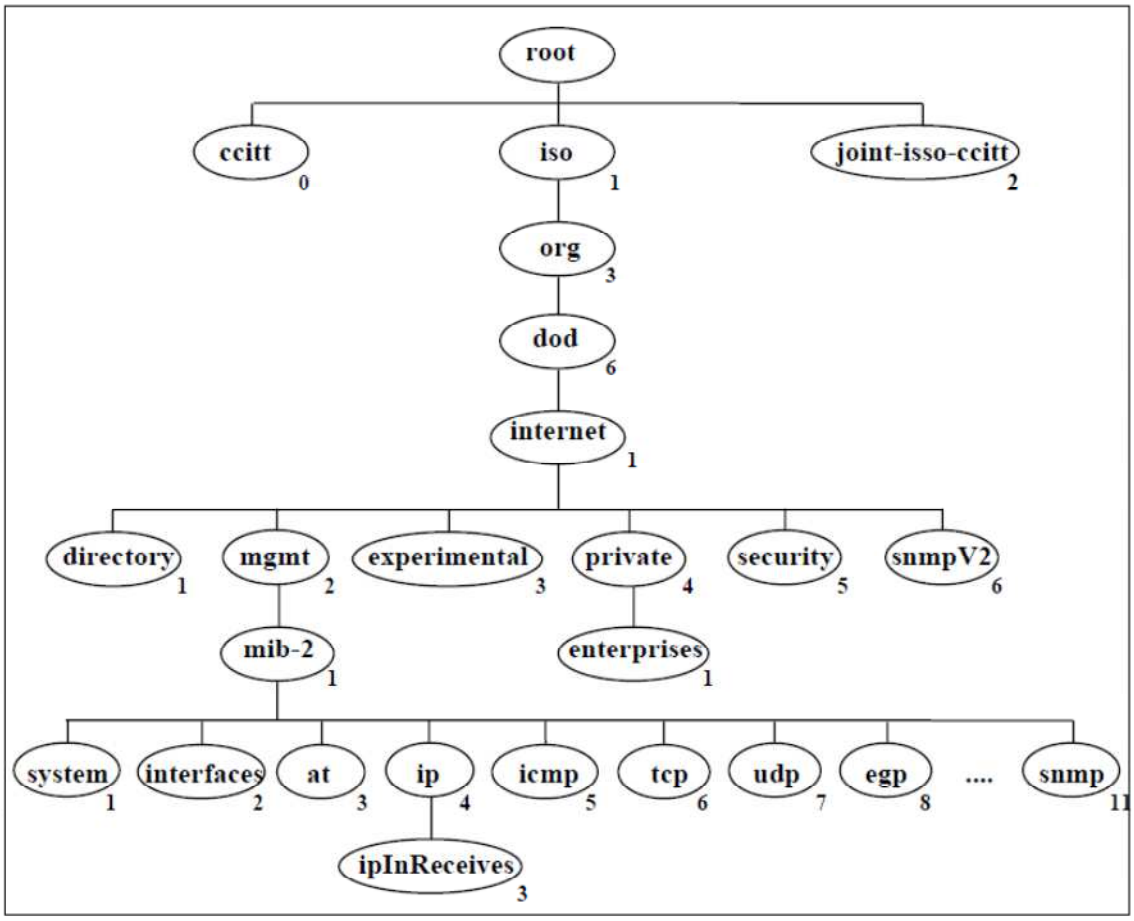
transferidas ou modificadas pelos protocolos de gerenciamento OSI, são guardadas na MIB (Base de informação de gerenciamento). A estrutura de informação de gerenciamento (SMI - *Structure Management Information*) proposta pela ISO define a estrutura de informação de gerenciamento, que é armazenada nessa base de dados, as operações que podem ser efetuadas sobre estas informações e as notificações que serão emitidas durante essas operações (GIMENEZ, 2004). Assim um conjunto de todos os objetos gerenciados, e seus respectivos atributos, constituem a Base de Informação de Gerenciamento (MIB).

Os objetos gerenciáveis nessa base de dados tem sua estrutura organizada em uma hierarquia em árvore como mostra a Figura 8. Um OID *object identifier*, é formado por uma sequência de inteiros seguindo os nós da árvore, os números separados por pontos identificam os OIDs. Outra forma de representação, além de uma *string* de inteiros, é uma sequência de nomes que representam cada nó da árvore, essa forma é mais legível para pessoas. Por exemplo a OID *1.3.6.1* pode ser representada por *iso.org.dod.internet* (iso(1).org(3).dod(6).internet(1)) (MAURO; SCHMIDT, 2001).

Os modelos ISO e Internet (TCP/IP) possuem MIBs modeladas através de técnicas de programação por objeto. Porém a grande diferença entre essas MIBs está nas hierarquias usadas para representar os objetos (BRISA, 1993).

No caso da ISO, são definidas três tipos: hierarquia de herança, hierarquia de nomeação e hierarquia de registro. A hierarquia de herança ou de classes está relacionada às propriedades de um determinado objeto. No caso da Internet os conceitos de classes de objetos não existe, são definidos tipos de objetos. Essa definição contém cinco campos: nome textual com respectivo identificador de objeto (*Object Identifier*), uma sintaxe ASN.1, a definição de semântica associada a um tipo de objeto, o tipo de acesso (*read-only, read-write, write-only* ou não acessível) e o *status* (obrigatório,

Figura 8: Estrutura hierárquica de uma MIB.



Fonte: Gimenez (2004).

opcional ou obsoleto).

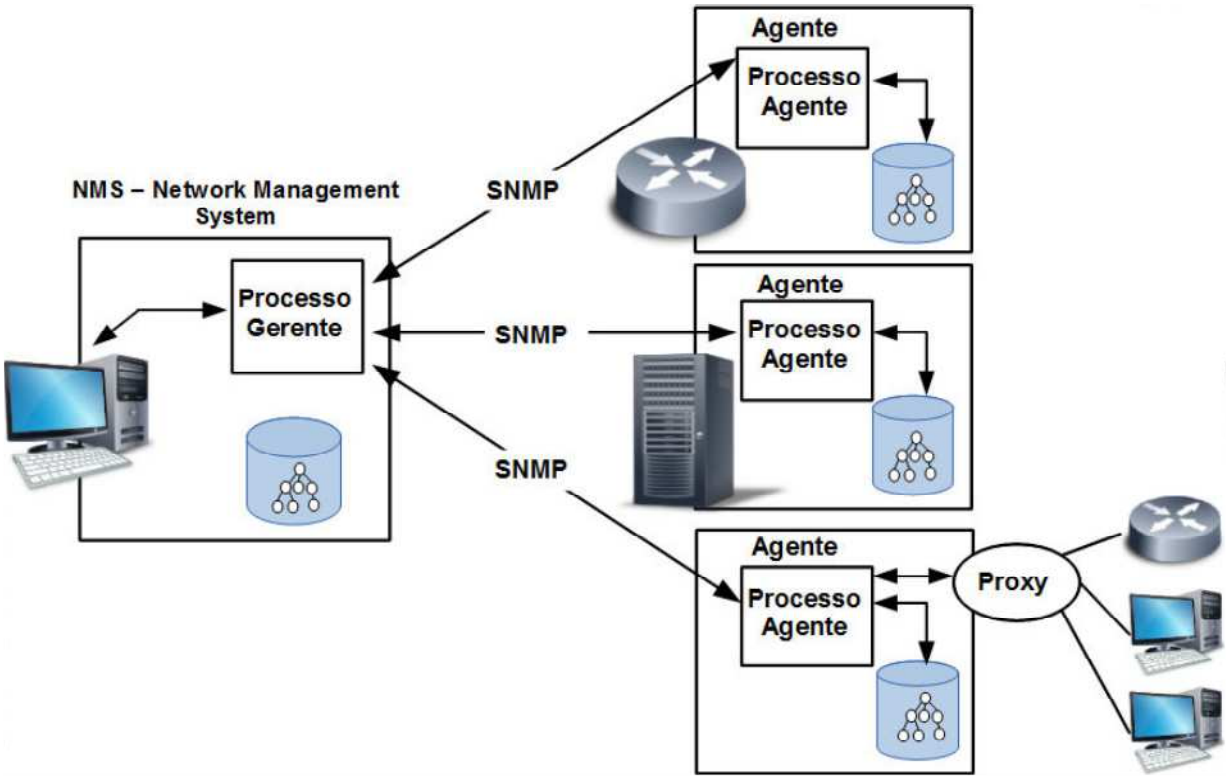
No caso da Internet, não exite a hierarquia de nomeação. Na ISO a hierarquia de nomeação identifica instâncias de objeto, enquanto que na Internet é definido apenas o conceito de instância de objeto.

A hierarquia de registro é especificada pela notação ASN.1 usada na atribuição de identificação de objetos. É usada tanto na ISO quanto na Internet e identifica de maneira universal os objetos.

A MIB é um coleção de objetos gerenciados. Os recursos gerenciados são representados por esses objetos. AS MIBs estão presentes nos dispositivos gerenciáveis onde essa base de dados reflete o estado dos recursos de gerenciamento (LENO JúNIOR, 2003). Uma entidade de gerenciamento, gerente ou agente, pode monitorar esses dispositivos, para isso ele necessita realizar leituras dos objetos da MIB e controlar esses recursos. Esse sistema é mostrado na Figura 9.

A *RFC 1213* define os objetos da *MIB* para *SNMP* chamada de *MIB-II*. Essa

Figura 9: Sistema de gerenciamento com MIBs.



Fonte: autor

MIB é em quase sua totalidade implementada em produtos comerciais.

Existem ainda padronizações de MIBs desenvolvidas para suprir necessidades específicas de novas tecnologias. O intuito é que essa MIB contenha objetos de essencial interesse para um determinado equipamento, ou componente.

Duas MIBs especiais podem ser descritas (STALLINGS, 1999) *apud* (LENO JúNIOR, 2003):

- As MIBs experimentais são aquelas que estão em fase de testes, com a perspectiva de serem adicionadas ao padrão e que, em geral, fornecem características mais específicas sobre a tecnologia dos meios de transmissão e equipamentos empregados.
- As MIBs proprietárias são específicas dos equipamentos gerenciados, possibilitando que detalhes particulares a um determinado equipamento possam ser obtidos. É desta forma que é possível obter informações sobre colisões, configuração e várias outras de um roteador, por exemplo. Também é possível fazer um teste, desabilitar uma ou mais portas de um hub ou de um switch utilizando as MIBs proprietárias. Elas fazem parte da MIB estendida.

As informações de gerenciamento possuem suas próprias regras de definição, assim as MIBs se tornam base de informações completamente desvinculadas do pro-

tocolo de gerenciamento. A definição do SNMP surgiu com necessidade de facilitar a migração da estrutura de informações para um protocolo de gerencia OSI, apesar de isso não ter acontecido, houve uma aproximação que ajudou a evolução do SNMP.

2.5 Modelo de gerência TCP/IP e o Protocolo SNMP

A gerência de rede na arquitetura Internet (TCP/IP), possui um facilitador para introdução visto que esse modelo possui uma boa base instalada de protocolos tradicionais (sem gerência). Esses protocolos se espalharam rapidamente devido a seus conceitos que foram bem explorados no Departamento de Defesa Americano, tornando-se como padrões de fato (DOTTI, 1992). Esse padrão é o mais usado atualmente em redes de médio e grande porte, locais e metropolitanas.

Devido a complexidade das redes atuais com os diversos tipos de dispositivos presentes a tarefa de monitoração é difícil. Há então a necessidade de um padrão para o gerenciamento de dispositivos IP *(Internet Protocol)*, em 1988 surge o SNMP para atender essa necessidade. O SNMP *(Simple Network Management Protocol)* oferece aos usuários um conjunto de operações permitindo um gerenciamento remoto de dispositivos na rede.*"O núcleo do SNMP é um conjunto simples de operações (e das informações obtidas por essas operações) que permite ao administrador modificar o estado de alguns dispositivos baseados em SNMP."*(MAURO; SCHMIDT, 2001).

Através do SMNP pode-se encerrar a interface de um roteador, verificar a temperatura de um servidor a velocidade da interface *Ethernet*, mandar alertas de qualquer alterações de algum dispositivo monitorado. É possível utilizar o SMNP para gerenciar sistemas Unix, *Windows*, impressoras ou qualquer dispositivo que execute um software e que permita a recuperação de informações, como também é possível gerenciar softwares como servidores Web e banco de dados.

Em um sistema de gerenciamento baseado em SNMP existem duas entidades, os gerenciadores e os agentes. Um gerenciador também chamado de NMS (*Network Management Stations* - estações de gerenciamento de redes) são responsáveis pelas operações de *pooling* e *traps* recebidos dos agentes. Já o agente é um software executado nos dispositivos monitorados da rede. Atualmente a maioria dos dispositivos IP já disponibilizam algum tipo de agente SNMP interno (MAURO; SCHMIDT, 2001).

2.5.1 Evolução do protocolo SNMP

Existem atualmente 3 versões do SNMP. Em maio de 1990, na RFC (*Request For Coments*) 1157 fez-se a definição da primeira versão do SNMP que logo passou a ter ampla aceitação comercial e se tornou padrão para o gerenciamento de redes

baseado em TCP/IP. Apesar dessa arquitetura baseada em SNMP ter surgido como solução provisória direcionada para sistemas TCP/IP, ela sobreviveu até os dias atuais passando por três grandes evoluções, como representado na Figura 10. O SNMP alcançou grande popularidade devido a simplicidade já que a arquitetura SNMP é escrita em poucos documentos, o que possibilita uma rápida compreensão além de facilitar o desenvolvimento de aplicações de gestão (LOPES, 2002).

Figura 10: Evolução da arquitetura SNMP.

Fonte: Lopes (2002).

Na primeira versão do SNMP (SNMPv1) a comunicação das informações de gerenciamento é feita através de apenas cinco PDUs *(Protocol data unit)*, que são unidades de dados trocados durante as mensagens. Dessas cinco, três são iniciadas pelo processo gerente *(get-request, get-next-request e set-request)*, e o processo agente é responsável por gerar as outras duas *(get-response e trap)*. Nesse sistema de gerenciamento SNMP o gerente monitora a rede perguntando aos agentes informações sobre as características e estado. Porém as mensagens enviadas pelos processos agentes, que não precisam ser solicitadas pelos gerentes agilizam o mecanismo de monitoramento. A tabela 2 mostra as operações e suas funções presentes no SNMPv1.

2.5.2 SNMPv2

Os mecanismos de segurança da primeira versão são limitados definindo apenas uma política de autenticação e de controle de acesso (LOPES, 2002). Com o aumento dos utilizadores surgiu a necessidade de acrescentar mais funcionalidades, com ênfase ao nível de protocolo de segurança. O SNMPv2 acrescentou novos tipos de mensagens. Como descrito na RFC 1905 *apud*(LOPES, 2002):

- Operação de informação *(information)* - permite a troca de informação entre estações gestores;
- Operação de consulta múltipla *(get-bulk)* - é semelhante a operação transversal *(get-next)* mas torna possível a especificação de múltiplos parâmetros;

Tabela 2: Operações presentes no SNMPv1.

Operação	Função
Get-requestet	Solicitação de recuperação do valor de uma ou um conjunto de variáveis informados na solicitação
Get-next-request	Solicitação de recuperação do valor de uma ou um conjunto de variáveis informados na solicitação que sucedem lexicograficamente àquelas informadas a solicitação
Set-request	Solicitação para atribuição de valor a uma ou um conjunto de variáveis
Get-response	Resposta às operações get-request, get-next-request e get-response
Trap	Envio de um evento não solicitado para uma ou várias estações de gerenciamento. Tipos de traps definidos no RFC 1215: cold start, warm start, link down, link up, authentication failure, egp neighbor loss e enterprise specific.

Fonte: Lopes (2002).

- Get não atômico - a falha de consulta a uma variável não impede o comando de prosseguir com outras consultas.

A alteração mais significativa no SNMPv2 foi a inclusão da *get-bulk-request*, que permite ao gerente a recuperação eficiente de grandes blocos de dados, preferencialmente várias linhas de tabelas. E a *information-request*, que é uma PDU *(Protocol data unit)* gerada pelo gerente para informar outro gerente da sua visão da MIB *(Management Information Base)*.

A segunda versão do SNMP (SNMPv2) contém três tipos de acesso a informações de gerenciamento. O primeiro chamado de *request-reponse*, que acontece quando uma agente SNMPv2 responde a uma solicitação de de um gerente SNMP. O segundo é um *request-response* onde há uma comunicação entre dois gerentes, e o terceiro tipo é um *trap*, que é uma mensagem enviada pelo agente, não solicitada pelo gerente. Essa mensagem não solicitada pode não ser retornada pelo gerente. Dentre essas apenas o segundo tipo é nova as outras já existiam no SNMPv1 (SPECIALSKI, s.d.).

2.5.3 SNMPv3

O SNMPv3 proposto na RFC2570 acrescenta melhores mecanismos de segurança, principalmente na área de autenticação e controle de acesso. Essa modificação na segurança visa evitar a alteração nas mensagens enviadas, além de restringir o acesso a elementos estranhos as operações de controle. A terceira versão do SNMP (SNMPv3) não é a substituição das versões anteriores e sim, a incorporação de soluções dos problemas de segurança no acesso aos objetos. Mesmo com as inovações, essa ultima versão ainda trás uma certa complexidade. Conforme Leno Júnior (2003) *"Os agentes serão mais complexos e os dispositivos gerenciáveis de-*

verão contar com plataformas de processamento mais robustas". A grande vantagem dessa nova versão é o fato dela possuir a capacidade de atuar em ambientes que contenham entidades das versões anteriores.

O SNMPv3 não especifica nenhuma nova PDU podendo ser usada tanto na versão 1 como na versão 2, as especificações da versão 3 falam basicamente da arquitetura geral, sobre as estruturas das mensagens e sobre características de segurança.

O SNMP é parte do protocolo TCP/IP à nível de aplicação, usa o UDP *(user datagram protocol)* como protocolo de transporte entre gerentes e agentes. Esse protocolo foi escolhido por não ser orientado a conexão, ou seja, nenhuma conexão ponto-a-ponto é estabelecida entre agente e NMS quando realizam trocas de pacotes. Dessa forma cada troca de mensagem é uma transação independente entre gerente e agente, e não inunda a rede com retransmissões. Segundo Mauro e Schmidt (2001)

> q uando uma rede está falhando, um protocolo que tenta obter os dados, mas desiste quando não consegue, é certamente uma opção de *design* melhor do que um protocolo que inunda a rede com retransmissões, na tentativa de obter credibilidade.

Se uma rede monitorada está muito congestionada, um gerenciamento feito através de um protocolo TCP, orientado a conexão não é a melhor opção, já que este é exige resposta a cada requisição. Por sua vez, o SNMP foi desenvolvido para trabalhar com redes que enfrentam problemas. Não seria necessário monitorá-la se a rede não falhasse.

2.6 Gerência de Desempenho em um ambiente Corporativo

Com o aumento da competitividade, as instituições de diversos segmentos tem buscado a redução de custos e o aumento da eficiência em suas atividades.

As redes corporativas, presentes nas instituições, estão crescendo em diversidade e quantidade de dispositivos de hardware e software formando uma estrutura essencial nas atividades dessas instituições e o desempenho dessa estrutura influência socialmente e financeiramente as corporações. De acordo com Gimenez (2004):

> As redes corporativas estão sendo constituídas por uma quantidade cada vez mais significativa e diversificada de recursos de hardware, software e meios de comunicação, servindo de base para o aprovisionamento de inúmeros serviços de teleinformática às corporações, influenciando cada vez mais nas áreas produtiva, financeira e social das mesmas.

A eficiência das aplicações executadas em uma rede está ligada a seu bom desempenho, para realizar o Gerenciamento de Desempenho é necessário entender alguns conceitos (LENO JúNIOR, 2003):

- **Serviços:** são um conjunto de procedimentos computacionais que permitem ao usuário realizar tarefas, alguns serviços encontrados em uma rede são: serviços de *e-mail*, Web, etc;
- **Ocupação de Recursos e Caracterização de Serviços:** a execução de um determinado serviço e o tempo que leva para sua execução;
- **Indicadores de qualidade de serviços:** parâmetros mínimos de operação como: tempo de resposta, taxa de transmissão, taxa de erros;
- **Demanda sobre os Serviços:** dois ou mais usuários podem usar um serviço ao mesmo tempo, ocupando um recurso e mesma natureza simultaneamente;

A atividade de gerência de desempenho pode ser dividida em três grandes áreas: Monitoramento de Eventos Relevantes ao Desempenho de Sistemas, Análise de Desempenho e Planejamento de Capacidade (GIMENEZ, 2004).

2.6.1 Eventos Relevantes ao Desempenho do Sistema

Esta área consiste na coleta de informações que possam indicar a qualidade de serviço da rede ou identifica a carga de trabalho para uma instância de serviço. As atividades englobam: Monitoramento para Verificação de Desempenho - Análise de Desempenho, Monitoração para caracterização de Carga de Trabalho - Planejamento da Capacidade.

2.6.2 Análise de Desempenho

Através da análise de Desempenho é possível avaliar a capacidade instalada da rede e usando dados da análise da carga de trabalho, identificar possíveis gargalos, esses gargalos são recursos responsáveis pela degradação dos serviços, ajustar os parâmetros de configuração. Os resultados dessas análises são obtidos através da construção de modelos matemáticos ou computacionais.

2.6.3 Planejamento da Capacidade

o Planejamento de Capacidade consiste em garantir qualidade de serviço ou indicar a capacidade excedente. Dessa forma é possível prever e estabelecer alterações na capacidade do sistema em função do crescimento.

De modo geral o Planejamento de Capacidade é usado como complemento a Análise de Desempenho. Mas também pode ser usado para definição e parâmetros de capacidade em um ambiente de rede em fase de projeto.

Um sistema de gerenciamento de redes visando garantir um desempenho satisfatório dos serviços é importante não só para assegurar o melhor nível de *QoS*, mas também para que esses níveis sejam alcançados com o menor custo possível (GIMENEZ, 2004).

É nesse contexto que o gerenciamento em uma instituição de ensino superior se faz necessário. A crescente demanda por recursos, dispositivos e usuários, tornam uma rede de computadores em uma ambiente corporativo cada vez mais complexa, necessitando de uma infraestrutura de gerenciamento que provê um melhor desempenho para uma rede, sem perda de qualidade e nível de QoS (*Quality of Service*).

3 O Software ZABBIX

3.1 Introdução

A cada momento uma nova perspectiva de utilização das redes de computadores surge, desafiando os responsáveis pela manutenção do sistema. Assim a medida que a rede cresce, aumenta a complexidade de gerenciamento e a adoção de ferramentas automatizadas para a monitoração e controle se torna necessária.

Um sistema de gerência de redes ideal dever ser composto por uma coleção de ferramentas com uma interface única onde esta, apresenta informações sobre a rede possibilitando a execução de comandos usados na gerência de rede, (STALLINGS, 1999) *apud* (SAUVé et al., 1993) diz:

> Este sistema oferece uma interface única, com informações sobre a rede e pode oferecer também um conjunto poderoso e amigável de comandos que são usados para executar quase todas as tarefas da gerência da rede (STALLINGS, 1999).

Com o aumento da quantidade e diversidade dos ativos presentes nas redes, e o aumento dos usuários dessa tecnologia, a gerência de redes tem se tornado uma atividade complicada. Para manter a qualidade dos serviços oferecidos pela rede é necessário ter controle sobre os processos e recursos utilizados pelos usuários. Por isso é importante que o administrador tenha acesso a informações como tráfego, carga de processamento, memória utilizada, verificar se serviços como banco de dados, servidores web estão funcionado entre outros.

A melhor solução seria um gerenciamento de rede coerentemente estruturado, um elemento de controle integral, que permitisse a conexão de equipamentos compatíveis ou não. Uma rede de grande porte e de grande complexidade, com vários dispositivos diferentes, não pode ser gerenciada por uma única pessoa. É necessário uma ferramenta automatizada para tal fim.

3.2 O que é o Zabbix

o Zabbix atualmente desenvolvido e mantido pela ZABBIX SIA, foi criado por Alexei Vladishev, é um software de monitoramento distribuído capaz de monitorar a

disponibilidade e a performance de dispositivos presentes em uma rede, além de serviços como servidores Web, banco de dados, etc.

O Zabbix é um *software* livre *(Open Source - de código aberto)* , gratuito, distribuído e desenvolvido de acordo com a GPL *(General Public license)* versão 2. Assim seu código fonte é distribuído livremente. O suporte comercial é fornecido pela *Zabbix Company*.

Com suporte a *polling e trapping* o zabbix monitora vários parâmetros da rede, a saúde e integridade de servidores. Usando mecanismos de notificação bastante flexíveis permite que usuários configurem alertas de *e-mail* sobre qualquer evento, isso possibilita uma rápida reação dos responsáveis pela rede na correção de problemas. O Zabbix também oferece a possibilidade de visualização de relatórios gerados através de dados coletados e armazenados durante o monitoramento.

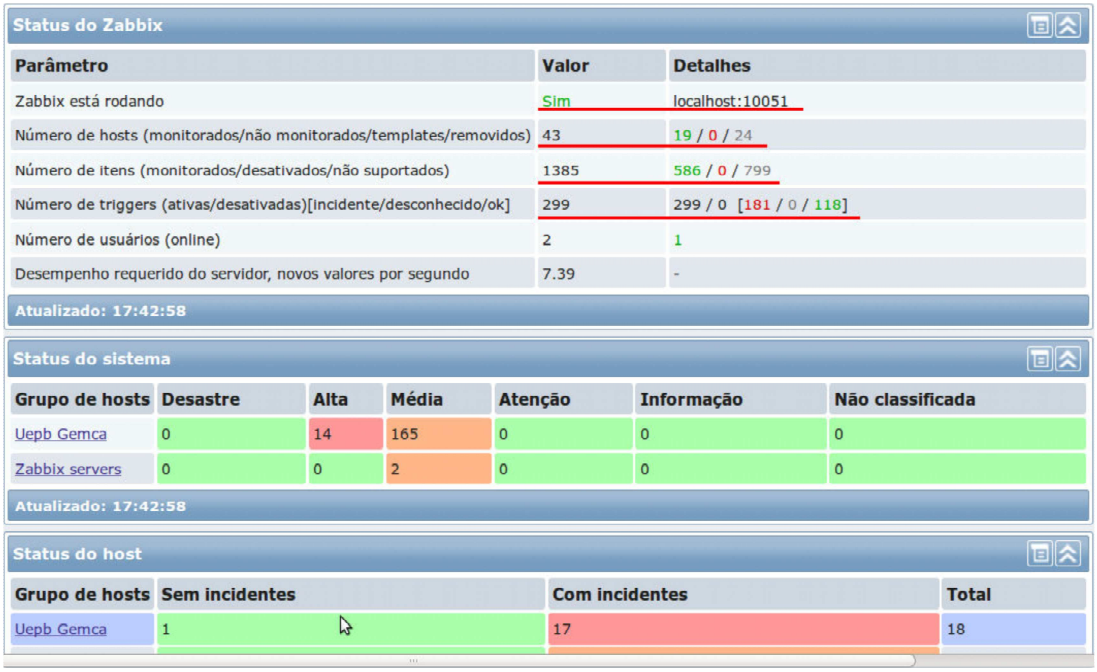
Todos os serviços oferecidos pelo Zabbix como: relatórios, estatísticas, parâmetros de configuração, são acessados pelo *front-end* (parte do sistema que interage diretamente com o usuário) do software em uma ferramenta Web (navegador). Essa possibilidade de acesso através do navegador permite que o status da rede possa ser verificado de qualquer lugar onde se tenha acesso a internet mesmo que o administrador esteja fora da rede monitorada. Com a configuração correta o Zabbix desempenha um papel importante no controle da infraestrutura da rede tanto de pequenas empresas como de instituições de médio a grande porte. A Figura 11 mostra o *Front-end* do Zabbix com o *Dashboard*. O *Dashboard* do Zabbix é o painel principal e exibe um resumo de todas as informações importantes.

3.3 Características

O Zabbix possui características que facilitam sua implementação e utilização em um sistema de gerenciamento de redes de computadores, dentre elas destacam-se:

- Oferece suporte a maioria dos sistemas operacionais: Linux, Solaris, HPUX, AIX, FreeBSD,OpenBSD, NetBSD, Mac OS X, Windows, entre outros;
- Suporte a monitoração de serviços simples (HTTP, POP3, IMAP, SSH, ICMP Ping) sem o uso de agentes;
- Suporte nativo ao protocolo SNMP;
- Interface Web, de fácil utilização;
- Integração com banco de dados (MySQL, Oracle, PostgreSQL ou SQLite);

Figura 11: *Front-end* do Zabbix com *Dashboard*.



Fonte: *print screen* do software Zabbix.

- Geração de gráficos em tempo real;
- Fácil instalação e customização;
- Agentes disponíveis para diversas plataformas: Linux, Solaris, HPUX, AIX, FreeBSD, OpenBSD,SCOOpenServer, Mac OS X, Windows 2000/XP/2003/Vista;
- Agentes para plataformas 32 bits e 64 bits;
- Integração com os Contadores de Performance do Windows;
- Software *Open Source* distribuído pela Licença GPL v2;
- Excelente Manual (Possui licenciamento próprio) Não GPL;
- Envio de alertas para: Email, Jabber, SMS;
- Suporte a Scripts personalizados.

3.4 Estrutura do Zabbix

O Zabbix tem como uma importante característica sua portabilidade, dando suporte a diversos sistemas operacionais. Porém a única limitação é que o seu servidor (estação gerente) necessariamente tem que ser instalado em um sistema Linux ou

MAC OS. A grande vantagem é sua versatilidade. Como há disponibilidade de agentes para as mais diversas plataformas, o Zabbix pode ser usado em sistemas onde existem máquinas com diferentes configurações e plataformas.

O Zabbix se divide em alguns componentes distintos (ZABBIX, 2013),, conforme mostrado na Figura 12.

- *Zabbix Server*(Servidor Zabbix);
- *Database storage* (Banco de dados);
- *Web interface* (Interface Web);
- *Proxy*;
- *Agent* (Agente);

Figura 12: Componentes Zabbix. Fonte: Déo e Pires (2010).

Fonte: Déo e Pires (2010).

3.4.1 Zabbix Server

Servidor ou núcleo, é onde fica toda a lógica do sistema, realizando todo o processamento de dados. O servidor é o repositório central no qual todas as configurações, dados estatísticos e operacionais são armazenados. É o componente principal onde os agentes reportam todas as informações estatísticas e de integridade. Depois que essas informações chegam até o servidor Zabbix ele processa as

informações gerando gráficos, estatísticas, relatórios, envia alertas e executa ações dependendo da configuração que o usuário adotar.

O Servidor Zabbix monitora os dispositivos através do agente Zabbix, porém o software também pode realizar o monitoramento através de um agente SNMP em dispositivos que suportam esse protocolo, além de checagens através de *simple Check*, que são checagens que não necessitam de agentes instalados nos dispositivos. Esse tipo de checagem retornam 0 ou 1 (”sim”ou ”não”) e é usado para checagem de sistemas embarcados como os presentes em catracas, no-break, câmeras de vigilância, etc.

3.4.2 Banco de dados

Banco de dados, é onde ficam armazenados todas as informações, tanto de configuração, quanto de monitoramento coletados pelos agentes e enviados ao servidor. Esse banco geralmente, dependendo da configuração usada pela rede, fica localizado no servidor zabbix, porém se o tráfego de informações for muito grande é recomendado que o banco seja instalado em uma máquina dedicada.

3.4.3 Interface Web

A interface do Zabbix é acessada através de um navegador, essa característica facilita o acesso já que o responsável pela administração da rede pode acessar o status dos serviços da rede em qualquer lugar onde tenha acesso a internet. Através da interface Web o usuário interage com todo o sistema realizando a configuração de todos os elementos (Hosts, Mapas, Gráficos, Screens, Slide Show, Actions, Discovery, Usuários e etc). Essa interface geralmente é executada na máquina onde está o servidor. A Figura 13 mostra a interface Web do Zabbix onde o usuário fornece seu *username* e senha.

3.4.4 Proxy Zabbix

Zabbix Proxy é um processo que coleta dados de gerenciamento de um ou mais dispositivos e envia para o servidor Zabbix a qual o *proxy* pertence. Esses dados são armazenados em um banco separado e depois enviados ao servidor. A implantação de um *proxy* não é obrigatório mas pode ser uma solução útil para monitoração centralizada de redes remotamente, essa prática também diminui a carga de processamento no servidor.

Figura 13: Tela de *login* do Zabbix.

Fonte: *print screen* do software Zabbix.

3.4.5 Agente Zabbix

O Agente Zabbix é um processo implantado no dispositivo para monitorar ativamente os recursos e aplicações locais (discos rígidos, memória, estatísticas do processador, etc.). O agente coleta informações operacionais localmente e manda para processamento no servidor. Agentes Zabbix são muito eficientes graças ao uso do sistema de chamadas nativa para coleta de informações.

O Agente Zabbix pode executar checagem ativas e passivas. Em uma verificação passiva o agente responde a uma solicitação do Servidor Zabbix (ou *proxy*). O servidor pede os dados sobre a carga de processamento, por exemplo, e o agente envia os dados correspondentes. Já em uma checagem ativa o agente deve primeiro possuir uma lista de itens a ser monitorado, e posteriormente o agente envia periodicamente valores atualizados ao servidor. Esse tipo de checagem requer um processamento mais complexo.

3.5 Requisitos

O Zabbix necessita de poucos recursos de hardware para seu funcionamento. Segundo o manual do Zabbix (2013) são necessários apenas 128 MB (*Megabit*) de memória física e 256 MB de espaço livre em disco para começar a executar, porém dependendo da configuração da rede, quantidade de *hosts* e parâmetros que são monitorados será exigido um pouco mais da capacidade do hardware.

Deve-se levar em conta também, que um sistema de gerenciamento deve manter um histórico dos dados coletados para consulta posterior, isso pode requerer alguns GB (*Gigabit*) de espaço em disco para armazenamento desses dados. Outro ponto a ser pensado é que um processo daemon (*Disk And Execution MONitor* Monitor de Execução e de Disco) Zabbix requer várias conexões com o banco de dados isso pode exigir um esforço significativo da CPU. Em uma rede de grande porte onde é preciso gerenciar uma grande quantidade de itens a taxa de atualização é muito alta. Nestes casos o manual do Zabbix recomenda que o banco de dados seja executado em uma máquina a parte.

Porém uma configuração de *hardware* adequada depende do número de itens ativos presentes na rede a Tabela 3 mostra alguns exemplos de configuração de hardware, e software de acordo com a quantidade de *hosts* monitorados.

Tabela 3: Exemplos de configurações.

Name	**Platform**	**CPU/Memory**	**Database**	**Monitored hosts**
Small	Ubuntu Linux	PII 350MHz 256MB	SQLite	20
Medium	Ubuntu Linux 64 bit	AMD Athlon 3200+ 2GB	MySQL InnoDB	500
Large	Ubuntu Linux 64 bit	Intel Dual Core 6400 4GB	RAID10 MySQL InnoDB or PostgreSQL	>1000
Very large	RedHat Enterprise	Intel Xeon 2xCPU 8GB	Fast RAID10 MySQL InnoDB or PostgreSQL	> 10000

Fonte: Zabbix (2013).

O Zabbix é compatível com a maioria dos sistemas operacionais do mercado, porém existem alguns requisitos de software para a instalação do Zabbix, de acordo com o manual do Zabbix temos a Tabela 4 que lista os pacotes necessários.

3.6 Motivação para usar o Zabbix

A principal vantagem em usar o Zabbix para a tarefa de gerenciamento de redes é sua praticidade. Com uma interface bastante interativa e agradável a manipulação de objetos se torna uma tarefa fácil agilizando as atividades de gerência (DéO; PIRES, 2010).

O Zabbix é uma solução de gerência de redes altamente integrada, que oferece uma multiplicidade de recursos em um único pacote (ZABBIX, 2013). De acordo com (ZABBIX, 2013) o *software* oferece,

Tabela 4: Requisitos para o *frontend*.

Software	Version	Comments
Apache	1.3.12 ou Superior	Servidor Web
PHP	5.1.6 ou Superior	
PHP extensions:		
gd	2.0 ou superior	Módulo PHP para suporte a imagens.
bcmath		php-bcmath (–enable-bcmath)
libXML	2.6.15 or later	php-xml or php5-dom.
session		php-session.
sockets		php-net-socket (–enable-sockets). Requerido para uso de script.
mbstring		php-mbstring (–enable-mbstring)
gettext		php-gettext (–with-gettext)
ibm_db2		Requerido se IBM DB2 for usado como banco de dados integrado ao Zabbix.
mysql		Requerido se o MySql for usado como banco de dados integrado ao Zabbix.
oci8		Requerido se o Oracle for usado como banco de dados integrado ao Zabbix.
pgsql		Requerido se o PostgreSQL for usado como banco de dados integrado ao Zabbix.
sqlite3		Requerido se o SQLite for usado como banco de dados integrado ao Zabbix.

Fonte: Zabbix (2013).

Checagem de disponibilidade e desempenho;

Suporte para SNMP (ambos *trapping* e *polling*) ,monitoramento IPMI, JMX;

Verificações personalizadas;

Coleta de dados desejados em intervalos customizados;

Realizada por servidor / *proxy* e por agentes.

Ainda de acordo com Déo e Pires (2010) o Zabbix é um *software All-in-one* (tudo em um), oferece visualização do histórico dos dados que são armazenados em um banco. Solução *Open Source* GPLv2 (sem versões comerciais), podendo ser usado para controle de ambientes de pequeno porte até ambientes distribuídos de grande porte. Oferece grande flexibilidade dando suporte a configuração de *Triggers, escalations, new checks, screens*, suporte total a IPv6 e projetado para trabalhar com comunicações instáveis.

Outra grande vantagem do Zabbix é a possibilidade de verificação de alguns parâmetros relevantes ao desempenho da rede como: carga do processador, número

de processos, atividade de discos, capacidades de memória, etc. Todos esses dados são visualizados pelo administrador da rede através de gráficos gerados em tempo real, o que dá ao gerente informações atuais do desempenho dos serviços oferecidos na rede.

O Zabbix também possui um mecanismo de notificação muito eficiente, através de *triggers* (*trigger* é um recurso que é executado sempre que um evento acontece) o gerente recebe uma notificação do evento ocorrido. Com esse sistema o usuário pode configurar *scripts*, que são executados através de uma *trigger*, para enviar e-mails com informações sobre eventos ocorridos.

4 Resultados

4.1 Implementação da Solução de Gerência

O ambiente monitorado foi a rede de computadores da Universidade Estadual da Paraíba Campus VII localizado na cidade de Patos-PB. A infraestrutura da rede neste cenário baseada em uma rede local é composta por computadores, impressoras, roteadores e *switchs*. A infraestrutura é composta por cabeamento estruturado categoria 5E com protocolo TCP/IP com *link* de 6 MB para todo o campus. Esses equipamentos estão distribuídos entre diversos setores: laboratório de informática, biblioteca, coordenações dos cursos e o Grupo de Eletromagnetismo e Matemática Computacional Aplicada (GEMCA).

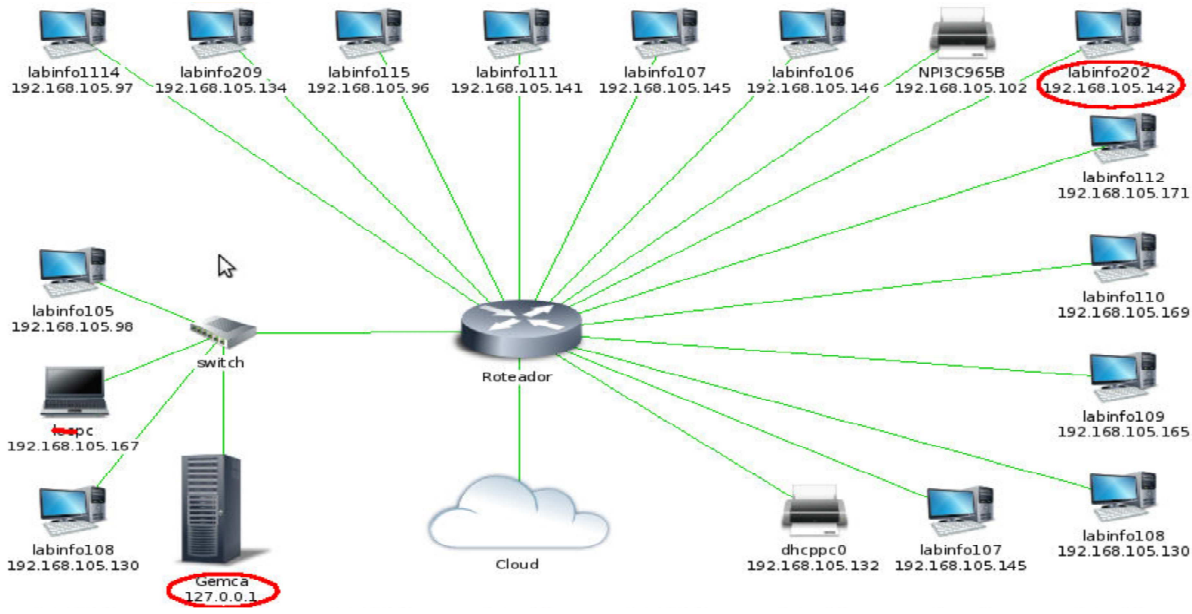
O software Zabbix possibilita a criação e configuração de um mapa da rede onde pode-se representar cada dispositivo monitorado. O cenário monitorado é mostrado na Figura 14. Esse recurso é muito importante porque permite ao gerente da rede visualizar em tempo real e de forma intuitiva qualquer evento relacionado ao elemento monitorado.

O cenário representado na Figura 14 mostra parte dos dispositivos (*hosts*) monitorados. O servidor Zabbix (estação gerente) foi instalado em um computador do grupo GEMCA onde foram coletados os dados dos dispositivos da rede monitorada.

O servidor foi configurado para coletar os dados dos dispositivos através do protocolo SNMP, para isso foi necessário instalar um agente SNMP nos computadores monitorados. Como a rede era configurada com DHCP (*Dynamic Host Configuration Protocol* - Protocolo de configuração dinâmica de host), ou seja cada *hosts* recebia um IP diferente ao ser inciado, os *hosts* no Zabbix foram configurados pelo *host name* (nome do *host*), pois apesar do IP dos *hosts* mudar o *host name* permanece o mesmo. A Figura 15 mostra uma lista de *hosts* monitorados.

Na Figura 15 pode ser observado informações dos elementos monitorados como: nome, número de aplicações, itens monitorados por *host*, *triggers*, gráficos, porta de monitoração, além do *status* indicando se o *host* está ou não ativo.

Figura 14: Mapa da rede UEPB Campus VII.



Fonte: autor.

Figura 15: Lista de *hosts* configurados pelo nome.

Nome	Aplicações	Itens	Triggers	Gráficos	Autobusca	Interface	Templates	Status	Disponibilidade
ww.uepb.edu.br	Aplicações (1)	Itens (0)	Triggers (1)	Gráficos (0)	Autobusca (0)	200.129.73.180: 10050	-	Monitorado	
NPI3C965B	Aplicações (6)	Itens (35)	Triggers (17)	Gráficos (8)	Autobusca (3)	NPI3C965B.local: 161	Template App Agentless, Template Conectividade, Template SNMP OS Linux (Template SNMP Disks, Template SNMP Generic, Template SNMP Interfaces, Template SNMP Processors)	Monitorado	
[illegible]	Aplicações (6)	Itens (77)	Triggers (23)	Gráficos (12)	Autobusca (3)	192.168.105.167: 10050	Template App Agentless, Template App Zabbix Agent, Template SNMP OS Linux (Template SNMP Disks, Template SNMP Generic, Template SNMP Interfaces, Template SNMP Processors)	Monitorado	
labinfo1114	Aplicações (6)	Itens (69)	Triggers (22)	Gráficos (20)	Autobusca (3)	labinfo1114.local: 161	Template App Agentless, Template Conectividade, Template SNMP OS Linux (Template SNMP Disks, Template SNMP Generic, Template SNMP Interfaces, Template SNMP Processors)	Monitorado	
labinfo209	Aplicações (6)	Itens (69)	Triggers (22)	Gráficos (16)	Autobusca (3)	labinfo209.local: 161	Template App Agentless, Template Conectividade, Template SNMP OS Linux (Template SNMP Disks, Template SNMP Generic, Template SNMP Interfaces, Template SNMP Processors)	Monitorado	
labinfo202	Aplicações (6)	Itens (21)	Triggers (15)	Gráficos (5)	Autobusca (3)	labinfo202.local: 161	Template App Agentless, Template Conectividade, Template SNMP OS Linux (Template SNMP Disks, Template SNMP Generic, Template SNMP Interfaces, Template SNMP Processors)	Monitorado	
labinfo115	Aplicações (6)	Itens (81)	Triggers (22)	Gráficos (15)	Autobusca (3)	labinfo115.local: 161	Template App Agentless, Template Conectividade, Template SNMP OS Linux (Template SNMP Disks, Template SNMP Generic, Template SNMP Interfaces, Template SNMP Processors)	Monitorado	
labinfo112	Aplicações (6)	Itens (68)	Triggers (22)	Gráficos (12)	Autobusca (3)	labinfo112.local: 161	Template App Agentless, Template Conectividade, Template SNMP OS Linux (Template SNMP Disks, Template SNMP Generic, Template SNMP Interfaces, Template SNMP Processors)	Monitorado	

Fonte: autor.

4.2 Análise de Desempenho da Rede Monitorada

Segundo (LEITE, 2004) o gerenciamento de desempenho permite avaliar o comportamentos dos elementos e das atividades de comunicação. As redes são com-

postas por diferentes dispositivos que se comunicam e compartilham dados e recursos. E em alguns casos o monitoramento e controle são essenciais para a eficiência dos recursos da rede. Ainda de acordo com Leite (2004) alguns tópicos relativos ao desempenho são:

- Qual é o nível de utilização da rede?
- Existe tráfego excessivo?
- Existe algum gargalo?
- O tempo de resposta está aumentando?

Para verificar essas questões é necessário que o gerente da rede monitore o desempenho de um conjunto de componentes afim de identificar uma possível degradação dos recursos oferecidos pela rede.

De acordo com a implementação proposta para monitoramento da rede da UEPB, foi realizado uma análise de alguns parâmetros que podem indicar o *status* do desempenho da rede, que são:

- Utilização da CPU - Carga de processamento;
- Utilização da rede - Tráfego da rede;
- Disponibilidade dos ativos da rede;

4.2.1 Carga de Processamento na Rede Monitorada

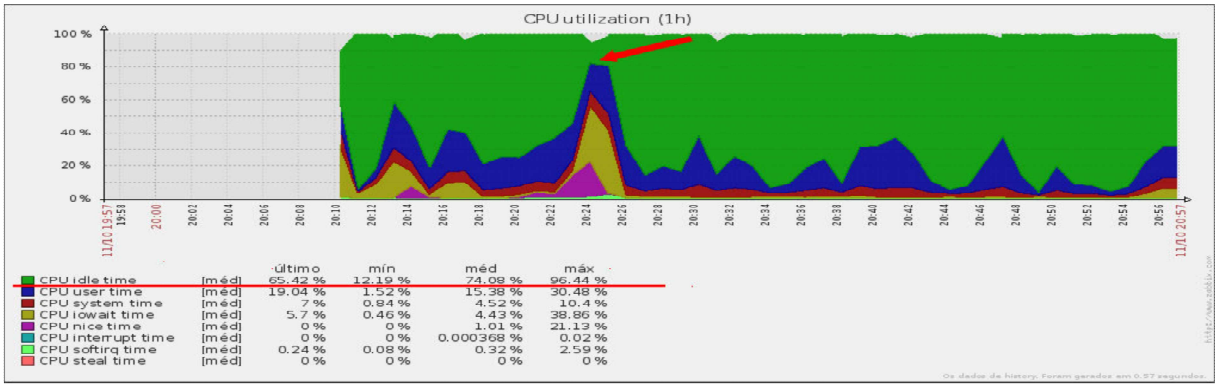
A Figura 16 apresenta um gráfico mostrando o desempenho da CPU de um computador pertencente a rede monitorada, ou seja, refere-se a utilização do processador deste *host*. Nesta Figura pode-se observar alguns parâmetros, tais como: *CPU idle time* (Tempo ocioso da CPU) que apresenta uma média de 74,08% e um máximo de 96.44% mostrando que o processador nesse *host* foi pouco requisitado no período. Analisando esses números verifica-se que o *host* monitorado está com a carga de processamento dentro da normalidade.

A Figura 17 por sua vez, mostra dados referentes a carga de processamento (*Processor load*) com *average per core* (média por núcleo) em 1; 5 e 15 minutos. No gráfico pode ver visualizado que o máximo em 1 minuto foi de 1.68. Neste caso um computador com dois núcleos, um valor acima de 2 já pode representar sobrecarga.

4.2.2 Tráfego da Rede Monitorada

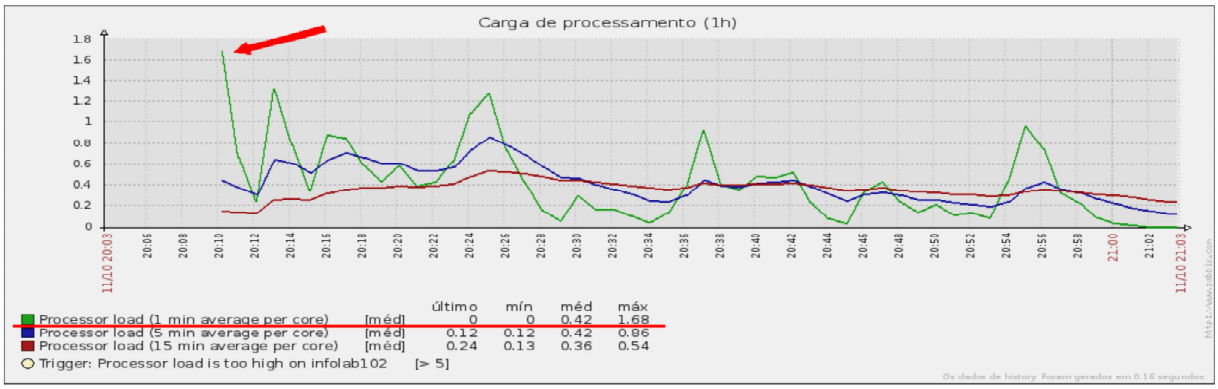
O gráfico da Figura 18 mostra o tráfego na rede em um determinado período de tempo. Pode-se observar que o tráfego de entrada teve um pico de 485,42 kbps

Figura 16: Utilização de CPU.



Fonte: autor.

Figura 17: Carga de processamento.

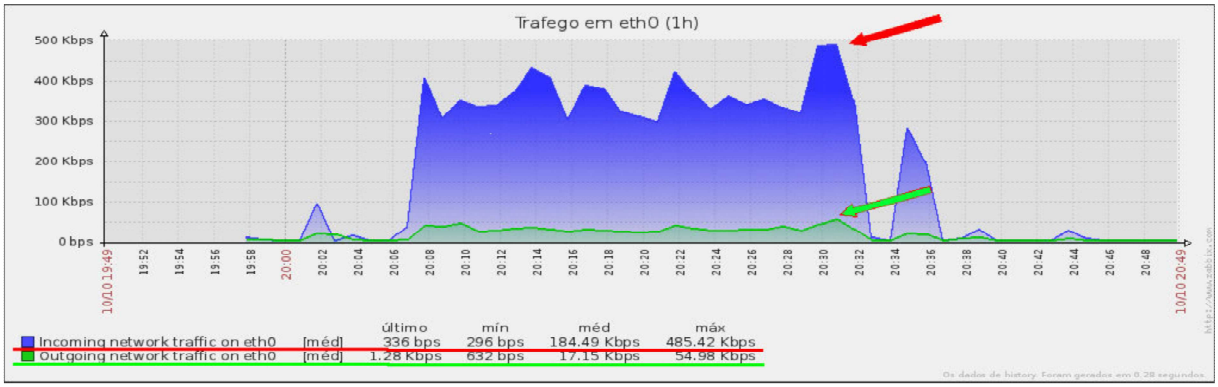


Fonte: autor.

(quilobit por segundo) e uma média de 184,49 kbps. O pico de 485,2 Kbps está associado ao *host* labinfo102 e pode ser atribuído a uma *download* de um arquivo de um tamanho considerável, por exemplo um vídeo ou imagem. Uma taxa muito elevada pode acarretar lentidão da rede já que está ocupando grande parte da banda. Neste caso há a necessidade de verificar o motivo de uma taxa de entrada tão elevada para que se possa realizar configurações afim de controlar de forma mais adequada o tráfego neste ponto. Já o tráfego de saída teve seu pico em 54.98 kbps e uma média de 17.15 kbps estando dentro da normalidade.

A Figura 19 mostra o gráfico com dados de *Incoming* (entrada) e *Outgoing* (saída) em uma porta *ethernet* de uma impressora. Nele pode-se observar que, no período apresentado no gráfico, houve um tráfego de entrada máximo de 15.55 kbps com uma média de 8.86 kbps e um tráfego de saída máximo de 2.42 kbps com uma

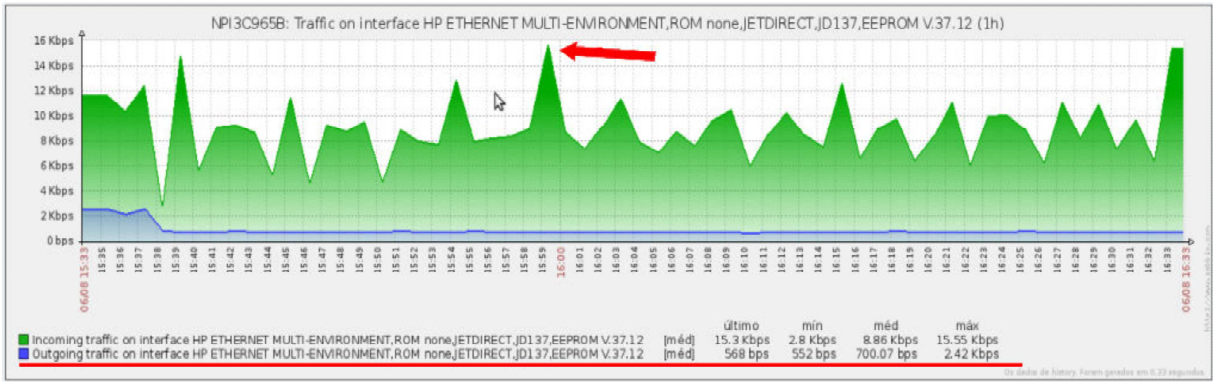
Figura 18: Tráfego na porta *ethernet*.



Fonte: autor.

média de 700.07 bps (bits por segundo). Neste caso o tráfego no dispositivo monitorado está com valores aceitáveis para a rede.

Figura 19: Tráfego na porta *ethernet*.



Fonte: autor.

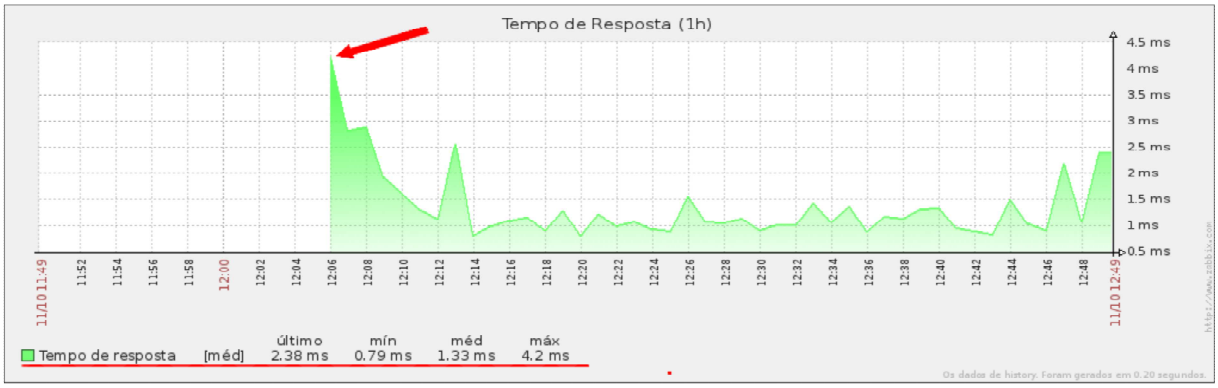
4.2.3 Tempo de Resposta e Perda de Pacotes

Tempo de resposta é o tempo que um sistema leva para responder a uma entrada, porém em aplicações distintas o tempo de resposta pode ter significados diferentes. De modo genérico o tempo de resposta é o tempo que o sistema leva para responder a uma entrada de usuário ou de um serviço. Um tempo de resposta muito alto pode indicar degradação do desempenho da rede, fazendo com que o usuário tenha que aguardar até que sua requisição seja processada.

O gráfico da Figura 20 mostra os dados coletados de um dispositivo da rede

durante o monitoramento do ambiente. Este resultado exibe o tempo de resposta de um ativo da rede. Neste podemos verificar que o tempo de resposta das requisições feitas pelo software Zabbix alcançou um tempo máximo de 4.2 ms (milissegundos) e uma média de 1.33 ms.

Figura 20: Tempo de Resposta.



Fonte: autor.

Por sua vez a perda de pacotes ocorre quando um ou mais pacotes não chega ao destino. Os motivos da perda de pacotes podem ser por falha de hardware ou baixa qualidade da conexão. Essas perdas de pacotes pode aumentar, se o tráfego na rede for muito alto.

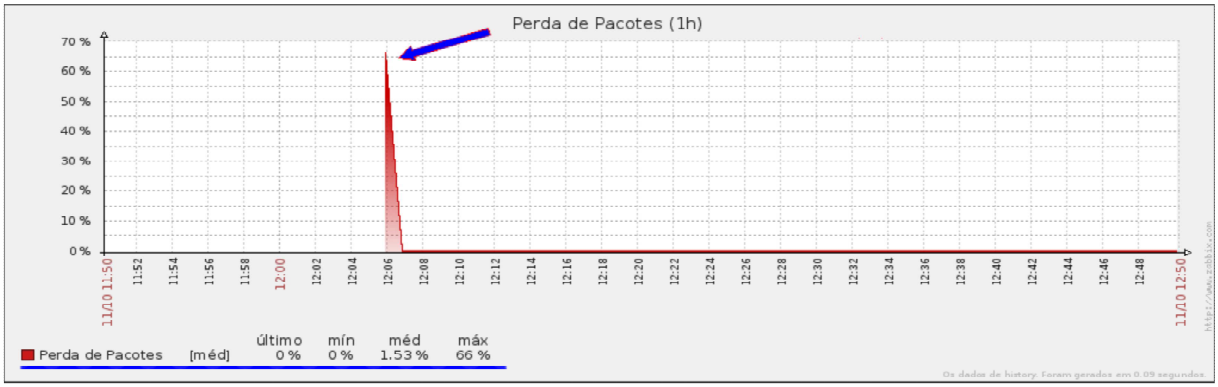
A perda de pacotes em 100% pode significar indisponibilidade do dispositivo. O gráfico da Figura 21 mostra uma porcentagem de 66% de perda de pacotes o que não necessariamente representa um problema, pois como podemos observar essa perca ocorreu no inicio da coleta de dados as 12:06 horas logo após esse momento não houve mais perdas.

O gráfico mostrado na Figura 22 confronta o tempo de resposta com a perda de pacotes. Durante o período compreendido entre 12 horas e 11 minutos e 12 horas e 52 minutos houve uma perda de pacotes de 100% e um tempo de resposta de 0 ms. Esses dados indicam que o dispositivo monitorado pode está indisponível.

4.3 Disponibilidade de Serviços Web

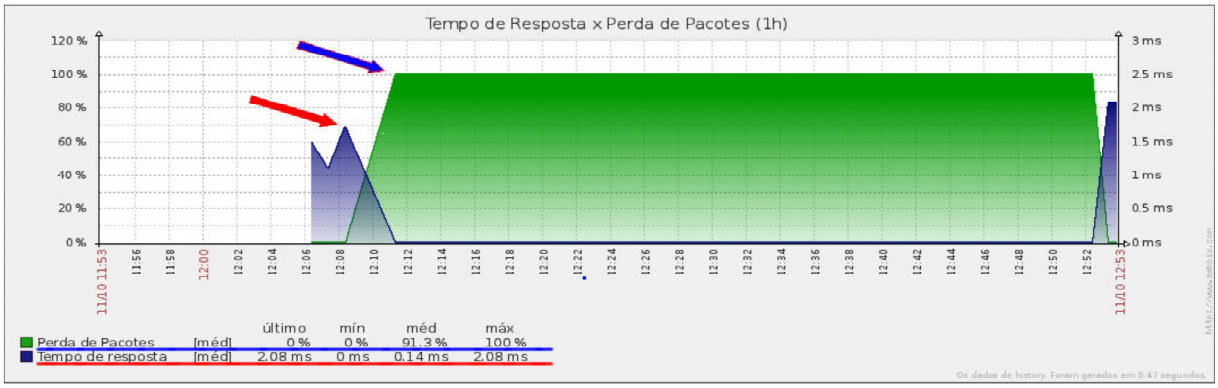
Outro ponto importante a ser observado no monitoramento de uma rede de computadores é a disponibilidade de alguns serviços oferecidos. Serviços como o *Hypertext Transfer Protocol* (HTTP), em português Protocolo de Transferência de Hipertexto, podem ser monitorados para que o gerente da rede identifique algum problema. A Figura 23 mostra a queda do serviço em um nó da rede monitorada aproximada-

Figura 21: Perda de Pacotes.



Fonte: autor.

Figura 22: Tempo de Resposta X Perda de Pacotes.



Fonte: autor.

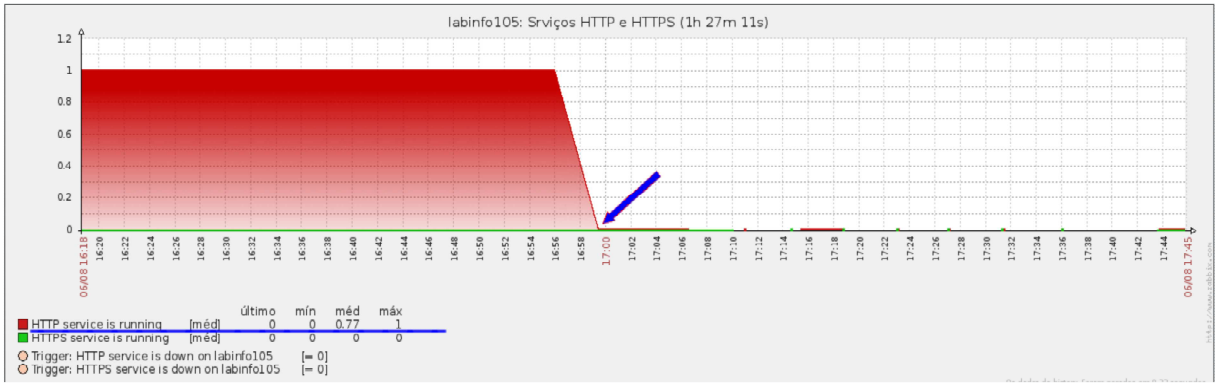
mente as 17:00 horas, neste caso se o *host* monitorado for um *roteador* ou *switch* os outros *hosts* conectados através deste podem ficar sem acesso a internet.

Esse protocolo é a base para a comunicação de dados da *World Wide Web*, como a maior parte dos acessos a rede monitorada é feita por alunos navegando na Internet, o monitoramento desse serviço se torna importante.

Uma aplicação *Web* como um *site* por exemplo tem uma importância relevante dentro de uma instituição já que muitas informações são disponibilizadas em *Web Sites* e a performance dessas aplicações devem ser monitoradas para que seja mantido um nível de *QoS* aceitável para os usuários. A Figura 24 mostra a taxa de download no site da UEPB, pode-se verificar que o houve um pico de 168.32 Kbps e uma média de 59.15 Kbps no período monitorado.

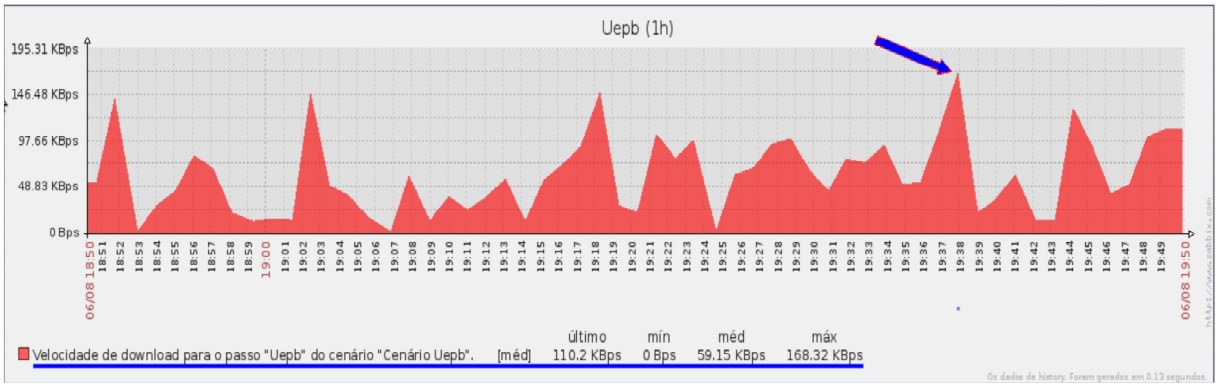
O site da UEPB não tem seu servidor no campus VII, porém o exemplo mos-

Figura 23: Monitoramento do Serviço HTTP e HTTPS.



Fonte: autor.

Figura 24: Monitoramento da taxa de download no site da UEPB.



Fonte: autor.

tra a possibilidade de monitorar uma aplicação que os usuários da rede monitorada utilizam com frequência, buscando informações, notícias, verificando histórico escolar, etc.

5 Conclusão

Neste trabalho apresentou-se uma proposta de implementação de uma solução de gerência de redes de computadores em um ambiente corporativo usando a ferramenta de monitoramento *Open-Source* Zabbix. Para realização deste trabalho foi instalado a ferramenta Zabbix em um computador do Grupo de Eletromagnetismo e Matemática Computacional Aplicada (GEMCA), o qual foi a estação gerente (servidor Zabbix) da rede monitorada. Durante o período de implementação foram coletados dados de ativos com o intuito de analisar o desempenho da rede de computadores da UEPB Campus VII na cidade de Patos Paraíba.

Os dados coletados pelo software Zabbix foram mostrados em gráficos possibilitando a análise de parâmetros relevantes ao desempenho da rede monitorada. Os gráficos foram gerados em tempo real o que proporcionou um acompanhamento mais eficaz e maior rapidez nas decisões tomadas pelo gerente da rede.

Com os resultados obtidos pôde-se verificar características que podem ajudar ao gerente da rede planejar a expansão dos serviços ofertados e da infraestrutura, afim de suprir a demanda dos usuários como também evitar e resolver problemas em tempo hábil, oferecendo assim um nível de *QoS* satisfatório aos usuários da rede.

Ao CPD da UEPB campus VII na cidade de Patos Paraíba, este trabalho propõe a implantação de um sistema de gerenciamento com utilização do software Zabbix, afim de verificar possíveis problemas na rede de computadores. A partir dos resultados obtidos, pode-se verificar também, a necessidade da implantação de um sistema de controle de banda afim de direcionar a maior parte da banda disponível na rede para usuários mais relevantes ao funcionamento da instituição como funcionários, coordenações, laboratórios e grupos de pesquisa.

Nesse contexto como sugestão para trabalhos futuros podem ser realizados: gerenciamento de configuração, onde pode-se implementar facilidades nas atualizações e modificações dos recursos da rede; e gerenciamento de segurança, onde pode-se implementar facilidades para proteger as operações dos recurso da rede.

Referências

BRISA. *Gerenciamento de Redes*: Uma abordagem a sistemas abertos. [S.l.]: Makron Books, 1993.

CASTELO BRANCO, M. A. *Um Algoritmo para Diagnóstico Distribuído de Falhas em Redes de Computadores*. Dissertação (Mestrado) — UNIVERSIDADE FEDERAL DO CEARÁ, 1999.

DéO, A.; PIRES, A. Gerência de redes com zabbix. Setembro 2010. Disponível em: ⟨http://revista.espiritolivre.org⟩. Acesso em: 15 Jun. 2013.

DOTTI, F. L. *Um Sistema de Apoio à Gerência de Redes Locais*. Dissertação (Mestrado) — Universidade Federal do Rio Grande do Sul, 1992.

GIMENEZ, E. J. C. *Metodologia Pragmática para Avaliação de Desempenho e Planejamento de Capacidade em Redes de Computadores*. Dissertação (Mestrado) — Instituto Nacional de Telecomunicações, 2004.

KUROSE, K. W. R. J. F. *Redes de Computadores e a Internet*: uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley, 2006.

LEITE, S. L. *Integrando Ferramentas de Software Livre para Gerenciamento e Monitoração de Redes Locais*. Dissertação (Mestrado) — Universidade Federal do Rio Grande do Sul, 2004.

LENO JúNIOR, E. *Uma Proposta de Metodologia para Análise de Desempenho de Redes IEEE 802.11 Combinando Gerência SNMP com Ferramentas de Simulação*. Dissertação (Mestrado) — Instituto Nacional de Telecomunicações, 2003.

LIMA, M. M. d. A. E. Introdução a gerenciamento de redes tcp/ip. 2011. Disponível em: ⟨http://www.rnp.br/newsgen/9708/n3-2.html⟩. Acesso em: 15 Nov. 2013.

LOPES, R. P. S. d. C. *Gestão Distribuída com SNMP*. Dissertação (Mestrado) — Universidade de Aveiro, 2002.

MAURO, D. R.; SCHMIDT, K. J. *SNMP Essencia*. [S.l.]: Editora Campus, 2001.

MELO, L. P. d. *Proposta de Metodologia de Gestão de Risco em Ambientes Corporativos na Área de TI*. Brasília-DF: PP- GENE.DM, 2008.

MENDES, D. R. *Redes de Computadores: teoria e prática*: teoria e prática. 1. ed. São Paulo: Novatec, 2007. 17-38 p.

SAUVé, J. P.; NICOLLETTI, P. S.; LOPES, R. V. *Melhores práticas para a gerência de redes de computadores*. 1. ed. Rio de Janeiro:Campos: [s.n.], 1993.

SPECIALSKI, E. S. *Gerência de Redes de Computadores e Telecomunicações*. Florianópolis-SC, s.d.

STALLINGS, W. *SNMP, SNMPv2, SNMPv3, RMON1 e RMON2*. 3. ed. Estados Unidos: Addison Wesley, 1999.

TANENBAUM, A. S. *Redes de Computadores*. 4. ed. Campus: [s.n.], 2003.

ZABBIX, S. *Zabbix Manual*. [S.l.], 2013. Disponível em: ⟨https://www.zabbix.com/documentation/⟩. Acesso em: 22 Jul. 2013.

ANEXO A - Tutorial de instalação do Zabbix

OBS.: Neste tutorial, será adotado o PostgreSQL, mas você pode optar pelo IBM DB2, MySQL, Oracle ou SQLite.

Para instalar os pacotes, execute os comandos abaixo de acordo com o tipo da distro GNU/Linux.

OBS.: Só execute os comandos abaixo se estiver usando o Ubuntu Desktop ou Server 12.04:

```
$ sudo apt-get -y install python-software-properties
$ sudo add-apt-repository -y ppa:webupd8team/java
$ sudo add-apt-repository -y ppa:pitti/postgresql
$ sudo apt-get update
$ sudo apt-get install -y --force-yes make flex gcc gpp apache2 php5 php5-pgsql
postgresql-9.2 postgresql-client libapache2-mod-php5 php5-gd php-net-socket
postgresql-client libpq5 libpq-dev snmp libiksemel-dev libcurl4-gnutls-dev vim
libssh2-1-dev libssh2-1 libopenipmi-dev libsnmp-dev oracle-java7-installer curl
fping
```

Depois que executar o comando ***"apt-get update"*** pode aparecer uma mensagem que não foi possível obter a chave pública GPG do repositório "ppa:flexiondotorg/java". Pode ignorar este erro e seguir com a instalação.

Criando o banco de dados

Crie o banco de dados e o usuário zabbix, usando os comandos abaixo.

```
# mysql -u root -p
mysql> create database zabbix character set utf8;
mysql> GRANT ALL PRIVILEGES ON *.* TO zabbix@localhost IDENTIFIED BY
'password' WITH GRANT OPTION;
mysql> quit
```

Crie no sistema operacional, o usuário a ser usado pelo Zabbix.

```
# adduser zabbix
```

OBS.: As senhas do usuário zabbix que será criado no sistema operacional e no MySQL podem ser diferentes.

Configurando o PHP

Edite o arquivo **/etc/php5/apache2/php.ini** delete o símbolo “;”, que porventura estiver no início da linha de cada parâmetro abaixo, e atribua os seguintes valores em negrito.

```
date.timezone = "America/Brasília"
max_execution_time = 300
max_input_time = 300
post_max_size = 16M
```

Reinicie o Apache para aplicar as configurações realizadas.

```
$ sudo /etc/init.d/apache2 restart
```

Instalando o Zabbix

Agora que as dependências estão instaladas, instale o Zabbix. Hoje (18/10/2013) a versão mais nova é a 2.0.9. Para instalá-la é preciso baixar e compilar o código fonte seguindo os passos abaixo.

Obtenha e descompacte o pacote de instalação do Zabbix.

```
$ wget http://downloads.sourceforge.net/project/zabbix/ZABBIX%20Latest
%20Stable/2.0.9/zabbix-2.0.9.tar.gz
$ tar xzvf zabbix-2.0.9.tar.gz
$ sudo chmod -R +x zabbix-2.0.9
```

Os comandos acima são usados para obter o pacote de instalação do Zabbix, salvar no diretório atual (veja qual em diretório que você está, usando o comando pwd) e descompactar o pacote, criando o diretório zabbix-2.0.9 com os arquivos de instalação.

Populando o banco de dados

Execute os comandos abaixo para popular o banco.

```
# cat zabbix-2.0.9/database/mysql/schema.sql | mysql -u zabbix -p<password>
zabbix
# cat zabbix-2.0.9/database/mysql/images.sql | mysql -u zabbix -p<password>
zabbix
# cat zabbix-2.0.9/database/mysql/data.sql | mysql -u zabbix -p<password> zabbix
```

OBS.: Atente para o fato de que a senha deve estar junto à opção " -p ". Sehouver um espaço em branco entre eles, o comando não vai funcionar. Instale o Zabbix, executando os comandos abaixo.

```
# cd zabbix-2.0.9
# ./configure --enable-server --enable-agent --enable-java --with-mysql --with-net-
snmp --with-jabber –with-libcurl=/usr/bin/curl-config --with-ssh2 --with-openipmi
# make install
# cd -
```

Configurando o Zabbix

Os arquivos de configuração do Zabbix 2.0 ficam em /usr/local/etc. Edite o arquivo **/usr/local/etc/zabbix_agentd.conf** e configure conforme mostrado abaixo.

PidFile=/tmp/zabbix_agentd.pid
LogFile=/tmp/zabbix_agentd.log
LogFileSize=2
DebugLevel=3
Server=127.0.0.1
ListenPort=10050
Hostname=informe o nome exato do host, do jeito que aparece no prompt de comandos antes dos símbolos "$", "#"

O parâmetro LogFileSize significa o tamanho máximo que o arquivo de log pode ter em mega byte (MB).

Edite o arquivo **/usr/local/etc/zabbix_server.conf** e informe os seguintes dados, como mostra o exemplo abaixo:

ListenPort=10051
LogFile=/tmp/zabbix_server.log
LogFileSize=2
PidFile=/tmp/zabbix_server.pid
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=senha do zabbix para acessar o banco de dados
StartIPMIPollers=1
StartDiscoverers=5
Timeout=3
FpingLocation=/usr/bin/fping

O parâmetro LogFileSize significa o tamanho máximo que o arquivo de log pode ter em mega byte (MB).

O parâmetro StartIPMIPollers só precisa ser configurado se o Zabbix for compilado com a opção **--with-openipmi**.

Copie os arquivos de frontend do Zabbix para o diretório **/var/www/zabbix**, executando os comandos abaixo.

```
$ sudo mkdir /var/www/zabbix
$ sudo cp -R zabbix-2.0.9/frontends/php/* /var/www/zabbix/
$ sudo chown -R www-data:www-data /var/www/zabbix/
```

Reinicie o Apache para carregar os novos arquivos do Zabbix

```
$ sudo /etc/init.d/apache2 restart
```

Scripts de inicialização do Zabbix

Coloque o Zabbix para iniciar automaticamente, no boot do sistema operacional, criando os scripts abaixo.

====> Crie arquivo ***/etc/init.d/zabbix-server*** e adicione o conteúdo abaixo.

```
#!/bin/sh
#
# Zabbix daemon start/stop script.
#
# Written by Alexei Vladishev <alexei.vladishev@zabbix.com>.
NAME=zabbix_server
PATH=/bin:/usr/bin:/sbin:/usr/sbin:/home/zabbix/bin
DAEMON=/usr/local/sbin/${NAME}
DESC="Zabbix server daemon"
PID=/tmp/$NAME.pid
test -f $DAEMON || exit 0
set -e
case "$1" in
start)
echo "Starting $DESC: $NAME"
start-stop-daemon --oknodo --start --pidfile $PID \
--exec $DAEMON
;;
stop)
```

```
echo "Stopping $DESC: $NAME"
start-stop-daemon --oknodo --stop --pidfile $PID \
--exec $DAEMON
;;
restart|force-reload)
$0 stop
$0 start
;;
*)
N=/etc/init.d/$NAME
echo "Usage: $N {start|stop|restart|force-reload}" >&2
exit 1
;;
esac
exit 0
```

====> Crie o arquivo ***/etc/init.d/zabbix-agentd*** e adicione o conteúdo abaixo.

```
#!/bin/sh
#
# Zabbix agent start/stop script.
#
# Written by Alexei Vladishev <alexei.vladishev@zabbix.com>.
NAME=zabbix_agentd
PATH=/bin:/usr/bin:/sbin:/usr/sbin:/home/zabbix/bin
DAEMON=/usr/local/sbin/${NAME}
DESC="Zabbix agent daemon"
PID=/tmp/$NAME.pid
test -f $DAEMON || exit 0
set -e
case "$1" in
start)
echo "Starting $DESC: $NAME"
```

```
start-stop-daemon --oknodo --start --pidfile $PID \
--exec $DAEMON
;;
stop)
echo "Stopping $DESC: $NAME"
start-stop-daemon --oknodo --stop --pidfile $PID \
--exec $DAEMON
;;
restart|force-reload)
$0 stop
$0 start
;;
*)
N=/etc/init.d/$NAME
# echo "Usage: $N {start|stop|restart|force-reload}" >&2
echo "Usage: $N {start|stop|restart|force-reload}" >&2
exit 1
;;
esac
exit 0
```

Torne os arquivos executáveis com o comando abaixo.

```
$ sudo chmod +x /etc/init.d/zabbix-server /etc/init.d/zabbix-agentd
```

Em seguida, execute os scripts

```
$ sudo /etc/init.d/zabbix-server start
$ sudo /etc/init.d/zabbix-agentd start
```

Habilite os scripts para serem executados quando o computador for ligado.

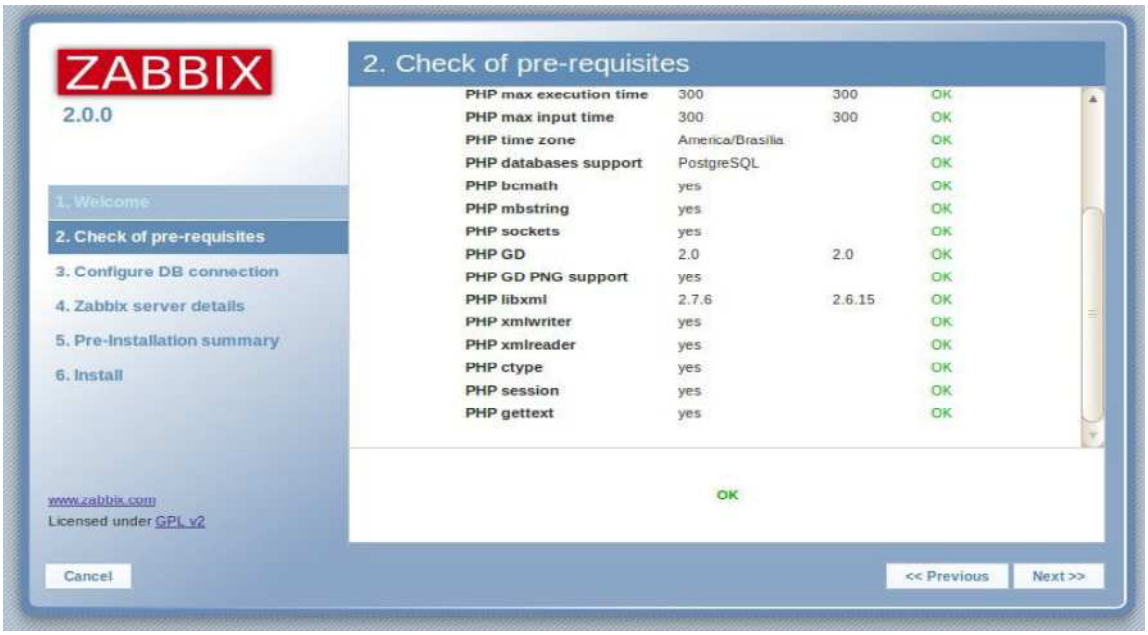
```
$ sudo update-rc.d -f zabbix-server defaults
$ sudo update-rc.d -f zabbix-agentd defaults
```

Acessando a interface web do Zabbix

Usando um navegador acesse o Zabbix no endereço http://ip-do- servidor/zabbix e siga as recomendações abaixo.

Tela 1: Clique no botão Next.

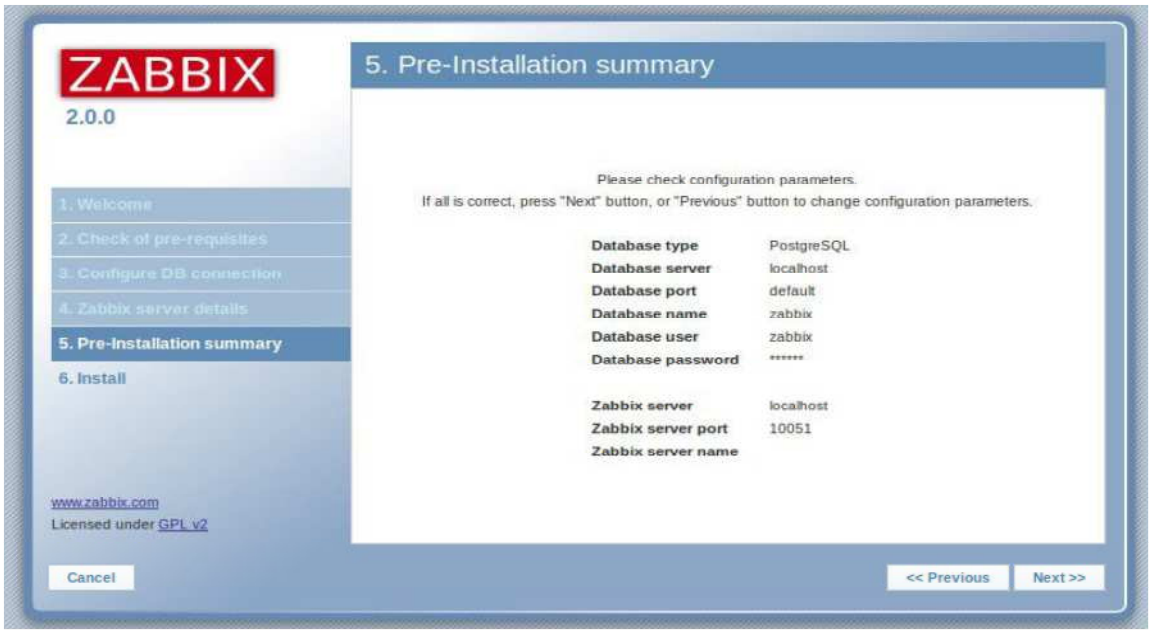
Tela 2: Cheque as dependências do Zabbix. Se estiver tudo ok, clique em Next.



Tela 3: Informe o tipo da base de dados, o usuário e a senha. Em seguida, clique no botão Test Connection. Se estiver ok, clique em Next..

Tela 4: Informe o IP do servidor Zabbix e a porta em que ele será executado (a padrão é 10051). No campo Name você pode usar um nome qualquer, essa informação é útil quando você precisa administrar vários servidores Zabbix. Depois clique em Next.

Tela 5: Revise as configurações e se estiver ok, clique em Next.



Tela 6: Clique em Finish. Se nesta tela for exibido um erro de permissão durante a atualização do arquivo de configuração, cheque a permissão do diretório **/var/www/zabbix** e configure da forma mostrada neste tutorial.

Tela 7: Pronto! O Zabbix está instalado. Logue no Zabbix com o usuário Admin e senha zabbix .

No site da comunidade Zabbix Brasil, mais especificamente na página http://zabbixbrasil.org/?page_id=7, você pode encontrar outros tutoriais que mostram a instalação dos componentes Zabbix Agent e Zabbix Proxy, além de mostrar como usar a interface Web do Zabbix para monitorar alguns tipos de equipamentos.