

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
CENTRO UNIVERSITÁRIO DO RIO GRANDE DO NORTE – UNI-RN
BACHARELADO EM SISTEMAS DE INFORMAÇÃO**

JOÃO RODRIGO SILVA DE CARVALHO

GERENCIAMENTO E MONITORAMENTO DE REDES USANDO O ZABBIX

GERENCIAMENTO E MONITORAMENTO DE REDES USANDO O ZABBIX

Monografia apresentada ao Centro
Universitário do Rio Grande do Norte e
Coordenação do Curso Superior de
Bacharelado em Sistemas de
Informação como requisito parcial para
obtenção do grau de Bacharel em

JOÃO RODRIGO SILVA DE CARVALHO

Orientador:

Prof. M. Sc. Aluizio F. da Rocha Neto

Natal-RN

2012

Natal – RN

2012

JOÃO RODRIGO SILVA DE CARVALHO

GERENCIAMENTO E MONITORAMENTO DE REDES USANDO O ZABBIX

Monografia apresentada ao Centro Universitário do Rio Grande do Norte a Coordenação do Curso Superior de Bacharelado em Sistemas de Informação como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador:

Prof. M.Sc. Aluizio F. da Rocha Neto

Natal-RN

2012

BIBLIOTECA UNI-RN

004.43 C331g - RB: 37269 (M002083)

Título: Gerenciamento e monitoramento de

Autoria: Carvalho, João Rodrigo Silva de
2012, ex. 1

**Catálogo na Publicação – Biblioteca do UNI-RN
Setor de Processos Técnicos**

Carvalho, João Rodrigo Silva de.

Gerenciamento e monitoramento de redes usando o ZABBIX. / João
Rodrigo Silva de Carvalho. – Natal, 2012.
43f.

Orientador: Prof. Luiz Ferreira da Rocha Neto.

Monografia (Graduação em Sistemas de Informação) – Centro
Universitário do Rio Grande do Norte.

1. Redes – Gerenciamento - Monografia. 2. Redes – Monitoramento -
Monografia. 3. ZABBIX - Monografia. I. Rocha Neto, Luiz Ferreira da. II.
Título.

RN/UNI-RN/BC

CDU 004.72

JOÃO RODRIGO SILVA DE CARVALHO

Dedico essa monografia a minha família pelo apoio no passado ao longo desses anos e aos professores pelo fato de estarem dispostos a ensinar.

Minha esposa, pela persistência e perseverança sempre fazendo o impossível para possibilitar a continuação dos meus estudos.

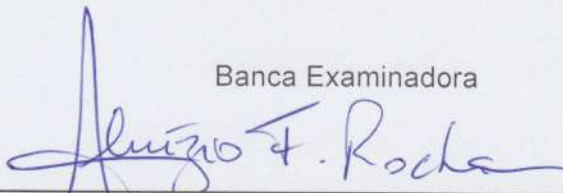
GERENCIAMENTO E MONITORAMENTO DE REDES USANDO O ZABBIX

Minha filha, pelo simples fato de sua existir, me fazenda melhorar sempre e ter estudado junto comigo em vários dias.

Monografia apresentada ao Centro Universitário do Rio Grande do Norte a Coordenação do Curso Superior de Bacharelado em Sistemas de Informação como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Aprovado em: ____/____/____

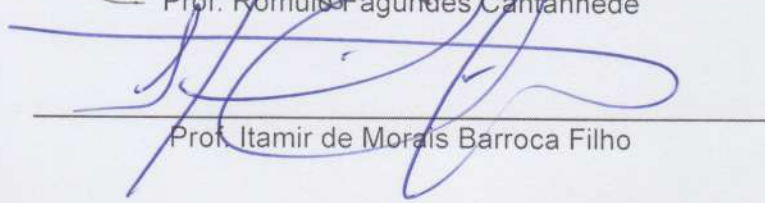
Banca Examinadora



Prof. Aluizio Ferreira da Rocha Neto
Orientador



Prof. Romulo Fagundes Cantanhede



Prof. Itamir de Moraes Barroca Filho

Dedicatória

Dedico essa monografia a minha família pelo apoio me passado ao longo desses anos e aos professores pelo fato de estarem dispostos a ensinar.

Minha esposa, pela persistência e perseverança sempre fazendo o impossível para possibilitar a continuação dos meus estudos.

Minha filha, pelo simples fato de sua existir, me fazendo melhorar sempre e ter estudado junto comigo em vários dias.

RESUMO

Agradecimentos

Agradeço a minha família por me apoiar para fazer um curso de graduação, mesmo depois de muito tempo parado.

Meus amigos de faculdade, que juntos, conseguimos ajudar uns aos outros nessa batalha.

Esse trabalho do curso de Bacharelado em Sistemas de Informação, realizado no IFRN - Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, foi realizado com o monitoramento de redes usando o Zabbix que permite que tanto o usuário que está na Rede, quanto os que estão nos outros quinze Campi, monitorem as atividades da sua rede que incluem, todos os equipamentos de rede, status do link, largura de banda utilizada, uso de CPU, memória entre outros serviços. O grande benefício foi incremento na disponibilidade dos serviços, já que agora se vê em tempo real quando um serviço está funcionando, facilitando o trabalho do setor de Tecnologia da Informação.

Palavras-chave: Open Source, GPL, CPU, Zabbix, IFRN

ABSTRACT

The massive growth of information technology (computers, equipment, network assets, services) is growing exponentially and becomes an integral part of any business today. Thus, it becomes increasingly frequent need to monitor these services more accurately. There are tools on the market as the high quality that Zabbix is an Open Source Software, distributed by the GPL, that supports multiple operating systems, monitors server services, web management interface and easy to use.

This course work for Bachelor of Information Systems, held in IFRN - Federal Institute of Education, Science and Technology of North Rio Grande, was deployed network monitoring using Zabbix which allows both the coach who is at the Rectory, as those in the other fifteen Campi, monitor the activities of your network including: all network equipment, assets, link status, bandwidth used, CPU usage, memory, among other services. The great benefit was an increase in the availability of services, now that you see in real time when a service stops working, facilitating the work of the Information Technology sector.

Keywords: Open Source, GPL, CPU, Zabbix, IFRN

LISTA DE ILUSTRAÇÕES

1. INTRODUÇÃO.....	10
Figura 1 – Funcionamento SNMP.....	16
Figura 2 - Relacionamento entre gerente e agente	18
Figura 3 – Principais clientes do Zabbix	21
Figura 4 - Projeto de infraestrutura de rede do IFRN	24
Figura 5 - Topologia da reitoria do IFRN. Ligações entre switches	25
Figura 5 - Detalhamento dos swiches da reitoria. Ip, modelo, patrimônio	26
Figura 6 – Configurações das portas de ativo de rede	26
Figura 7 – Tela de monitoramento do firewall interno.....	28
Figura 8 – Cadastramento de hosts.....	35
Figura 9 – Criando itens.....	36
Figura 10 – Criando templates.....	38
Figura 11 – Imagens personalizadas de switches	39
Figura 12 - Mapa ifrn interior. Mostrando atividade dos links de internet	39
Figura 13 - Diagrama da rede voip. Telefonia do IFRN	40
Figura 14 - Rede local cnat. Campus natal central - topologia dos ativos de rede.....	40
Figura 15 - Atividade dos links do interior.....	41
Figura 16 - Servidores ativos e inativos.....	41
3.3.2. Banco de dados	29
3.3.3. Instalação e configuração do Zabbix 1.8.3	29
3.3.4. Finalizando a configuração via Web	32
3.3.5. Zabbix – Cadastrando hosts	34
3.3.6. Criando itens.....	36
3.3.7. Zabbix – Criando Templates	37
3.3.8. Zabbix – Adicionando imagens personalizadas	38
3.4. Telas de Monitoramento	39
4. CONCLUSÃO	42
REFERÊNCIAS BIBLIOGRÁFICAS	43

SUMÁRIO

1. INTRODUÇÃO	10
1.1. Objetivos	10
1.1.1 Geral	Error! Bookmark not defined.
1.1.2 Específicos	10
1.1.3 Justificativa	11
1.1.4 Problema de Pesquisa	11
2. REFERENCIAL TEÓRICO	13
2.1. Gerenciamento de Redes	13
2.2. Protocolos de Rede	13
2.3. Componentes de uma rede	14
2.4. Arquitetura de redes TCP/IP	14
2.5. Benefícios da padronização	15
2.6. Arquitetura cliente/servidor	15
2.7. Protocolo SNMP	15
2.7.1. O Agente	17
2.7.2. O Gerente	17
2.7.3. Operações do Protocolo SNMP	18
2.7.4. Operações do Protocolo SNMP	19
2.7.5. Vulnerabilidades SNMP	19
2.8. O Zabbix	20
3. ESTUDO DE CASO	24
3.1. Implantação do Zabbix	24
3.2. Informações para o Monitoramento	27
3.3. Instalação do sistema Zabbix	28
3.3.1. Preparação do sistema	28
3.3.2. Banco de dados	29
3.3.3. Instalação e configuração do Zabbix 1.8.3	29
3.3.4. Finalizando a configuração via Web	32
3.3.5. Zabbix – Cadastrando hosts	34
3.3.6. Criando itens	36
3.3.7. Zabbix – Criando Templates	37
3.3.8. Zabbix – Adicionando imagens personalizadas	38
3.4. Telas de Monitoramento	39
4. CONCLUSÃO	42
REFERÊNCIAS BIBLIOGRÁFICAS	43

1 INTRODUÇÃO

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

Em primeiro momento, foi feita uma reunião definindo atividades a serem feitas por cada um do setor, entre servidores do Instituto, bolsistas e estagiários. Eu na função de servidor do IFRN, fiquei responsável por gerenciar o monitoramento toda a rede, documentação da rede que vai desde impressoras de rede a servidores de grande porte. Toda essa documentação, inclusive do Zabbix, fica documentada num wiki em um repositório do Redmine, que é um software livre, gerenciador de projetos baseados na web e ferramenta de gerenciamento de bugs. Ele contém calendário e gráficos de Gantt (usado para ilustrar o avanço das diferentes etapas de um projeto) para ajudar na representação visual dos projetos e seus deadlines (prazos de entrega). Ele pode também trabalhar com múltiplos projetos.

Este relatório contém a descrição do que foi proposto no plano de estágio, de acordo com as atividades desenvolvidas durante o mesmo, voltado a análise e implantação de um software de gerenciamento e monitoramento da rede. Descreve-se o processo antes, durante e depois da implantação.

1.1 Objetivos

Estudar, analisar e implantar um software de gerenciamento e monitoramento de rede a fim de reduzir o tempo de inatividade de sistemas e rede.

1.1.1 Específicos

- Levantar dados sobre os componentes que existem na rede atual tais como: servidores, roteadores, switch, firewall e computadores.

- Adquirir o conhecimento necessário para poder desenvolver as atividades principais do trabalho a ser executado, entendendo como funciona a infraestrutura atual da empresa de acordo com o negócio da mesma.
- Analisar e levantar os principais softwares disponíveis no mercado preferencialmente de distribuição livre.
- Estudar a ferramenta escolhida para ser implantada e as principais modificações necessárias.

1.1.2 Justificativa

Tendo como interesse e necessidade para a empresa a implantação de um sistema de gerenciamento da infraestrutura de rede, conseguindo analisar e antecipar futuras falhas no sistema. Além disto a empresa conseguirá monitorar seus ativos e ter um controle maior de seu inventário, agregando uma economia de investimento, já o software é livre e tendo o monitoramento e o gerenciamento da rede e dos sistemas citados, não será necessário enviar um técnico ao local, que implicaria em gastos com transporte, diária em hotel e combustível e tempo além de uma maior segurança nas informações, já que estão sob monitoria constante.

1.1.3 Problema de Pesquisa

O principal problema a ser resolvido com a implantação de um software de monitoramento é melhorar o SLA (*service level agreement*) que traduzindo para o português seria o *acordo de nível de serviço*. Níveis de serviço são definidos no início de qualquer relação de *outsourcing* e usados para mensurar e monitorar o desempenho de um fornecedor. Muitas vezes, um cliente pode cobrar multa de um *outsourcer*¹ se determinados SLAs não forem atingidos. Temos empresas que prestam serviço como Embratel, SitecNet que tem contrato com IFRN de fornecimento de Links de Internet em todos os Campi do RN e que em contrato, podem ter uma inatividade desses serviços por um certo tempo, caso não atenda, o Instituto pode aplicar multa. Mas como se pode provar tal inatividade no IFRN? Simples, através de um monitoramento desses links. O Zabbix não vai servir para

¹ Delegar serviços a terceiros.

aplicarmos penalidades as empresas prestadoras de serviços da escola, mas sim não deixar que nossos serviços fiquem parados por muito tempo para os alunos, servidores, professores e público externo.

Com os alertas do Zabbix, que pode monitorar a porta onde está instalado o link, fica mais fácil ver quando há inatividade de um link, serviço e até mesmo um disco rígido cheio para que possamos o mais rápido possível resolver o problema.

aplicações de gestão de redes, estão os backbones, aplicações, provedores de acesso, redes metropolitanas, datacenters. Todas essas estruturas dependem a nível de monitoramento e gerenciamento de rede, onde cada vez mais não são exigidos maiores níveis de estabilidade de rede. Cada vez que as aplicações e serviços de rede estão a falhar, aumenta a necessidade de monitorar e garantir essas atividades (DANTE, 2011).

Algumas boas práticas devem ser lembradas para que uma rede sempre esteja funcionando (RNP, 2011):

- Estabelecer períodos de manutenção e devem ser sempre divulgados aos interessados e assim, evitando surpresas;
- Evitar alterações na rede com ela em produção;
- Melhores dias para manutenção, são nos finais de semana;
- Evitar manutenção de equipamentos de rede fora do período pré-determinado.

2.2- Protocolos de Rede

Nos dias de hoje, vivemos em um mundo cada vez mais globalizado e o crescimento tecnológico está bastante acelerado. Grandes expansões de redes de comunicação, tanto de telefonia quanto de internet. Internet de alta velocidade em todas as regiões de Brasil, mudanças nas estratégias de telecomunicações, comércio eletrônico, amplo ambiente de competitividade.

Vendo tudo isso, podemos perceber que qualquer coisa em qualquer lugar, exige a preocupação grande em receber todas essas informações.

Protocolo de rede, nada mais é do que um padrão que serve de alguns pontos, podemos estabelecer e manter relações entre dois sistemas computacionais, além de transferência de dados entre os mesmos (ODOM, W.

2 REFERENCIAL TEÓRICO (Exam Certification Guide)

2.1 Gerenciamento de Redes

Todas as infraestruturas de redes requer uma grande atuação constantes de profissionais de redes, seja em pequenas e grandes corporações. Entre as aplicações de gerencia de redes, estão os backbones² acadêmicos, provedores de acesso, redes metropolitanas, datacenters. Todas essas estruturas dependem e muito de monitoramento e gerenciamento de redes, onde, cada vez mais são exigidos maiores níveis na qualidade de serviços. Cada vez que as aplicações, links, serviços, são cada vez mais exigidos, aumenta a criticidade de se monitorar e gerenciar essas atividades (DANTE, 2011).

Algumas boas práticas devem ser lembradas para que uma rede sempre esteja funcionando (RNP, 2011):

- Estabelecer períodos de manutenção e devem ser sempre divulgados aos interessados e assim, evitando surpresas;
- Evitar alterações na rede com ela em produção;
- Melhores dias para manutenção, são nos finais de semana;
- Evitar manutenção de equipamentos de rede fora do período pré-determinado.

2.2 Protocolos de Rede

Nos dias de hoje, vivemos em um mundo cada vez mais globalizado e o crescimento tecnológico está bastante acelerado. Grandes expansões de redes de comunicação, tanto de telefonia quanto de internet, internet de alta velocidade em vários locais de Brasil, mudanças nas estratégias de telecomunicações, comércio, negócios, amplo ambiente de competitividade.

Vendo todo esse ambiente, onde queremos qualquer coisa em qualquer lugar, existe a preocupação grande em gerenciar todas essas informações.

Protocolo de rede, nada mais é do que um padrão que através de alguns protocolos, podemos no conectar, estabelecer e manter sessões entre dois sistemas computacionais, além de transferência de dados entre os mesmos (ODOM, W.

² Designa o esquema de ligações centrais de um sistema mais amplo, tipicamente de elevado desempenho.

Algumas das características bem típicas desses protocolos são de: detecção da conexão física ou existência de um nó, estabelecimento de ligação entre os nós de rede, iniciar e finalizar uma mensagem, o que fazer com essas mensagens que são corrompidas ou perdidas no meio do caminho, detectar perda inesperada de pacotes de rede, terminar as sessões entre os sistemas. O uso de um padrão de protocolos de rede foi o ponto chave para o sucesso da internet. O protocolo TCP/IP é um dos protocolos mais usados do mundo e é descrito na RFC³. (IETF, [2012])

2.3 Componentes de uma rede

Uma rede é formada por computadores, periféricos, software local e de rede. O conjunto disso tudo vai nos dizer que tipo de rede se está utilizando (SOARES, 1995)

- Elementos de sistema de comunicação:
 - Hardware de rede – placa de rede, modem, repetidor, conversores de mídia, hub, bridge (ponte), switch, roteador, access point.
 - Meio físico – cabos, conectores, antenas.

2.4 Arquitetura de redes TCP/IP

As primeiras arquiteturas de rede foram desenvolvidas por fabricantes de equipamentos, os quais desenvolviam soluções para interconexão apenas de seus produtos, sem se preocuparem com a compatibilidade de comunicação com equipamentos de outros fabricantes. Assim o fizeram, por exemplo, a IBM (International Business Machines Corporation) ao anunciar sua arquitetura de rede SNA (System Network Architecture), e a DEC (Digital Equipment Corporation) com sua DNA (Digital Network Architecture). Essas arquiteturas são denominadas proprietárias (ODOM, 2004)

Nos dias atuais, toda a arquitetura de redes é adotada pela Internet e é baseada na especificação de protocolos abertos e especificada em documentos técnicos – RFC's (Request For Comments) conforme (ODOM, 2004)

³ É um documento que descreve os padrões de cada protocolo da internet previamente a serem considerados um padrão

2.5 Benefícios da padronização

Padronizar uma rede traz diversos benefícios para a estrutura montada no trabalho. Benefícios como: maior suporte um ambiente aberto, redução/eliminação de problemas ocasionados pela falta de compatibilidade de produtos, possibilidade de uso de normas para o planejamento e instalação de sistemas de cabeamento em prédios comerciais, residenciais, escritórios, definição de critérios técnicos e de desempenho para aferir configurações de sistemas e aterramento, especificação de padrões para documentação e administração dos projetos de cabeamento (KUROSE, 2006).

2.6 Arquitetura cliente/servidor

É uma abordagem da computação que separa os processos em plataformas independentes que interagem entre si, permitindo que os recursos sejam compartilhados enquanto se obtém o máximo de benefício de cada dispositivo diferente, ou seja, Cliente/Servidor é um modelo lógico. (VASKEVITCH, 1995)

- Cliente (entidade que solicita o serviço)
 - Cliente magro é um computador cliente que possui poucos ou nenhum recurso instalado e depende primariamente de um servidor para processar atividades.
- Servidor (entidade que presta o serviço)
 - Servidor é que compartilha com os clientes magros todas as aplicações, armazenamento de arquivos de usuários, banco de dados.
 - Servidor dedicado
 - Servidor não dedicado

2.7 Protocolo SNMP

O protocolo SNMP (do inglês *Simple Network Management Protocol* - Protocolo Simples de Gerência de Rede) é um protocolo de gerência típica de redes

UDP, da camada de aplicação, que facilita o intercâmbio de informação entre os dispositivos de rede, como placas e comutadores (em inglês: *switches*). O SNMP possibilita aos administradores de rede gerenciar o desempenho da rede, encontrar e resolver seus eventuais problemas, e fornecer informações para o planejamento de sua expansão. Nos dias de hoje, todos os equipamentos de rede já saem das fábricas com esse protocolo instalado nele, justamente pensando em gerência e monitoramento. Os padrões que definem a estrutura de gerenciamento de redes Internet são descritos nos documentos RFC-1155 [R1155], RFC- 1156 (MIB – *Management Information Base*) [R1156] e RFC-1157 (SNMP - *Simple Network Management Protocol*) [R1157]. A figura 1 abaixo mostra como funciona basicamente o SNMP, conforme (HUCABY, 2006).

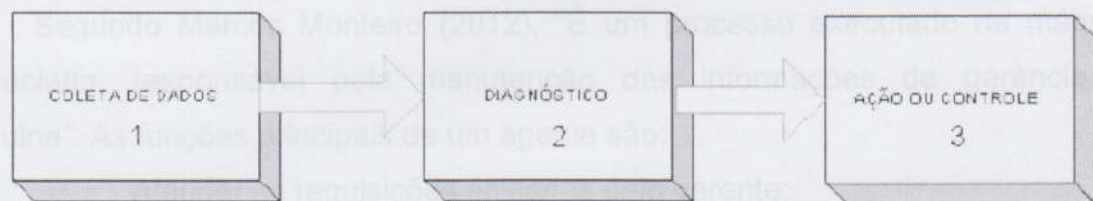


Figura 1 – Funcionamento SNMP

FONTE: <http://www.gta.ufrj.br>

Logo abaixo, há uma lista que engloba todas as versões atuais do SNMP e o status emitido pela IETF para cada uma (CARVALHO, 1993)

- **SNMP Version 1 (SNMPv1)** – É a versão padrão atual do protocolo SNMP, definida na RFC 1157 [R1157] e é um padrão completo da IETF. A segurança do SNMPv1 baseia-se em comunidades, que não são nada mais do que senha: string de texto puro que permitem que qualquer aplicativo baseado em SNMP, que reconheça a string, tenha acesso a informações de gerenciamento de um dispositivo. Geralmente existem três comunidades no SNMPv1: read-only, read-write e trap.
- **SNMP Version 2 (SNMPv2)** – É frequentemente citado como SNMPv2 baseado em string de comunidade. Essa versão tem a denominação técnica de SNMPv2c. Ela está definida na RFC- 1905 [R1905], RFC-1906 [R1906] e RFC 1907 [R1907].

- **SNMP Version 3 (SNMPv3)** – É a última versão do protocolo a alcançar o status completo da IETF. Está definido na RFC-1905 [R1905], RFC-1906 [R1906], RFC-1907 [R1907], RFC-2571 [R2571], RFC-2572 [R2572], RFC-2573 [R2573], RFC-2574 [R2574] e RFC-2575 [R2575], que inclui suporte para autenticação rigorosa e comunicação privativa entre as entidades gerenciadas.

Os comandos são limitados e baseados no mecanismo de busca/alteração. No mecanismo de busca/alteração estão disponíveis as operações de alteração de um valor de um objeto, de obtenção dos valores de um objeto e suas variações.

2.7.1 O Agente

Segundo Marcos Monteiro (2012), "É um processo executado na máquina gerenciada, responsável pela manutenção das informações de gerência da máquina". As funções principais de um agente são:

- Atender as requisições enviadas pelo gerente;
- Enviar automaticamente informações de gerenciamento ao gerente, quando previamente programado;

Outra afirmação de Marcos Monteiro (2012), é que "O agente utiliza as chamadas de sistema para realizar o monitoramento das informações da máquina e utiliza as RPC (Remote Procedure Call) para o controle das informações da máquina".

2.7.2 O Gerente

É um programa executado em uma estação servidora que permite a obtenção e o envio de informações de gerenciamento junto aos dispositivos gerenciados mediante a comunicação comum ou mais agentes conforme mostra a figura 2.

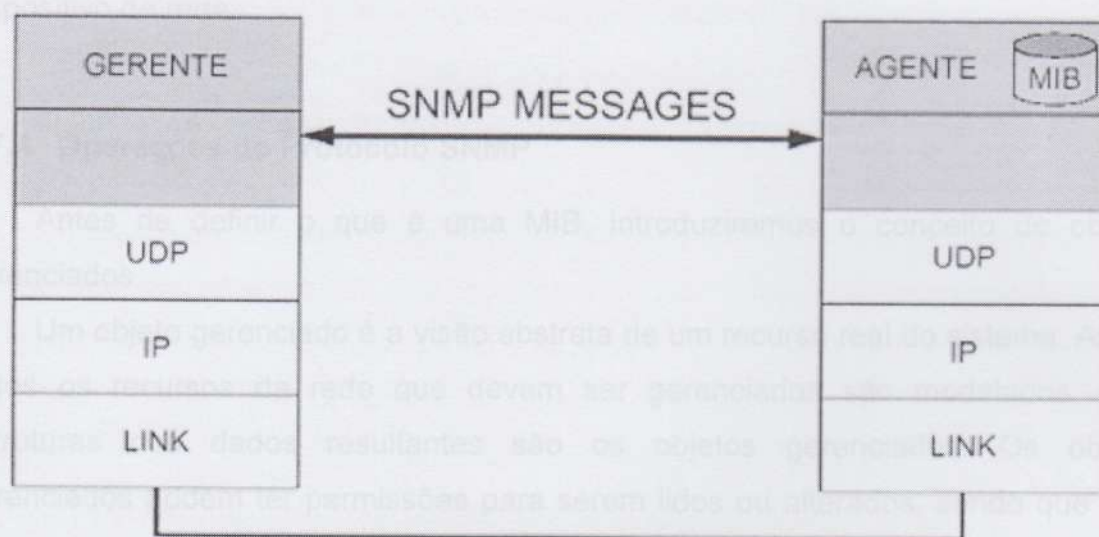


Figura 2 - Relacionamento entre Gerente e Agente

FONTE: <http://pontoderedes.blogspot.com.br/2010/04/protocolo-de-gerenciamento-snmp.html>

2.7.3 Operações do Protocolo SNMP

Existem duas operações básicas dentro do SNMP (Get, Set). Esses serão detalhados a seguir. Antes é bom termos o embasamento teórico sobre alguns termos.

Os comandos são limitados e baseados no mecanismo de busca/alteração. No mecanismo de busca/alteração estão disponíveis as operações de alteração de um valor de um objeto, de obtenção dos valores de um objeto e suas variações.

O software de gerência de redes não segue o modelo cliente-servidor convencional pois para as operações básicas que são as de: *GET* e *SET*⁴, a estação de gerenciamento se comporta como cliente e o dispositivo de rede a ser analisado ou monitorado se comporta como servidor, enquanto que na operação *TRAP*⁵ ocorre o oposto, pois no envio de alarmes é o dispositivo gerenciado que toma iniciativa da comunicação. Por conta disso, os sistemas de gerência de redes evitam os termos 'cliente' e 'servidor' e optam por usar "gerente" para a aplicação que roda na estação de gerenciamento e "agente" para a aplicação que roda no

⁴ *GET* - para obter um valor de um dispositivo. *SET* - para colocar um valor num dispositivo

⁵ Usado para reportar uma notificação ou para outros eventos assíncronos sobre o subsistema gerido

dispositivo de rede.

2.7.4 Operações do Protocolo SNMP

Antes de definir o que é uma MIB, introduziremos o conceito de objetos gerenciados.

Um objeto gerenciado é a visão abstrata de um recurso real do sistema. Assim, todos os recursos da rede que devem ser gerenciados são modelados, e as estruturas dos dados resultantes são os objetos gerenciados. Os objetos gerenciados podem ter permissões para serem lidos ou alterados, sendo que cada leitura representará o estado real do recurso e, cada alteração também será refletida no próprio recurso (RNP, 2011).

O RFC - Request For Comment 1066 apresentou a primeira versão da MIB, a MIB I. A MIB (Management Information Base) pode ser considerada um banco de dados de objetos gerenciados que o agente rastreia, ou seja, é a definição dos próprios objetos. Todo tipo de informação sobre os estados e estatísticas acessados pelo NMS é definida em uma MIB.

Um agente pode implementar várias MIBs, porém todos os agentes implementam uma MIB específica denominada MIB-II (RFC 1213) [R1213]. Esse padrão define variáveis para elementos como dados estatísticos de uma interface, assim alguns outros aspectos relacionados ao próprio sistema. O principal objetivo da MIB-II é fornecer informações gerais sobre gerenciamento de TCP/IP e não engloba todo item possível que um fornecedor gerenciaria em um dispositivo específico

2.7.5 Vulnerabilidades SNMP

Alguns testes feitos na Finland's Oulu University revelaram as seguintes falhas nas versões da SNMP.

- SNMPv1 – Manipulação de Trap's
- Solicitação de manipulação

- A maioria dos dispositivos já vem com o SNMP habilitados com a comunidade *public* para acesso somente leitura e *privado* para acesso de leitura/gravação.

Essas vulnerabilidades podem levar aos seguintes ataques na rede: Denial of service, format string. Ou seja, conseguindo manipular o campo string do protocolo, pode-se mandar várias solicitações de serviço até que o servidor onde o Zabbix está instalado saia do ar ou trave, fazendo que o serviço fique fora por algum tempo. Além disso, algumas implementações do SNMP por padrão aceitam pacotes SNMP enviados pela rede através de broadcast.

2.8 O Zabbix

O Zabbix é um software livre, distribuído pela licença GPL que monitora diversos parâmetros de rede como integridade, desempenho. Oferece relatórios e visualização de dados e recursos com base nos dados armazenados. O Zabbix, usa um flexível mecanismo de alarmes que permite aos usuários configurar e-mail com alertas para qualquer evento, o que permite uma reação rápida para os problemas do servidor. Esse poderoso software de monitoramento de redes, pode ser usado tanto para pequenas empresas que usam poucos servidores, tanto quando para grandes empresas com um grande número de servidores.

A figura 3 mostra os principais Clientes que usam o Zabbix para monitorar a sua rede.



Figura 3 – Principais clientes do Zabbix

Fonte: www.zabbix.org

O Zabbix oferece (ZABBIX, 2012):

- Suporte para ambos mecanismos de polling⁶ e trapping⁷;
- Servidores para Linux, Solaris, HP-UX, AIX, Free BSD, Open BSD, OS X;
- Agentes de alta performance nativos;
- Monitoramento de servidores sem uma gente instalado; – Autenticação de usuário segura utilizando criptografia
 - dos dados;
- Permissões de usuários flexíveis;
- Interface gráfica web;
- Flexível notificação e predefinidos eventos por e-mail;
- Alto Nível de visualização (Negócios) de recursos;
- A utilização do ZABBIX traz ao administrador alguns

⁶ Cada dispositivo é endereçado num tempo bem definido.

⁷ É usado pelo agente para informar ao servidor algum evento ocorrido.

- benefícios indispensáveis nos dias de hoje, como: Solução de código aberto;
- Alta eficiência para agentes baseados nas plataformas: UNIX e WIN32;
- Baixa curva de aprendizado;
- Alto retorno de investimento através dos dados coletados, diminuindo o tempo gasto com soluções erradas dos problemas;
- Baixo custo de implantação pois é de fácil instalação;
- Muito simples de configurar;
- Sistema de monitoramento centralizado.
- Todas informações (configuração, dados de performance) são armazenadas em uma base de dados relacional;
- Serviço de árvore de alto nível;
- Instalação muito fácil;
- Suporte para o SNMP (v1, v2). Ambos aceitam polling e trapping;
- Procedimento interno de tarefas proprietárias.

O Zabbix é composto de vários componentes (ZABBIX, 2012):

- **Zabbix Server:** O servidor pode verificar remotamente os serviços de rede (como servidores web, Arquivos, atividade de link), utilizando controles simples. Ele é o componente central para o qual os agentes reportam a disponibilidade, integridade de informações e estatísticas dos servidores. Toda a configuração, estatísticas e dados operacionais são armazenados, sendo o componente que participará ativamente alertando os administradores quando surgirem problemas na rede.
- **Zabbix Proxy:** É uma parte opcional da implantação do Zabbix. O Proxy coleta dados de desempenho e disponibilidade, em nome do Zabbix Server. Todos os dados coletados localmente são transferidos para o Zabbix Server Proxy. O Zabbix Proxy é uma solução ideal para um controle centralizado de locais remotos, filiais, não havendo a necessidade dos administradores de redes locais; Muitas vezes precisamos monitorar ambientes remotos, onde podemos ter vários dispositivos que precisam ser monitorados. Se esses dispositivos forem monitorados diretamente, pode ocasionar perda de dados, visto o volume de informações enviadas,

atrasos nas leituras, perda de informação por indisponibilidade do link, etc. Com isso, é comum que o Zabbix apresente gráficos incompletos, triggers⁸ acionadas erroneamente, entre outros problemas.

- **Zabbix Agent:** A fim de acompanhar ativamente recursos e aplicações locais (como discos rígidos, memória, processador, etc.) em sistemas em rede, os sistemas devem executar o Agente Zabbix. O agente vai reunir informações operacionais do sistema em que está em execução, e informar esses dados ao Zabbix para posterior processamento. Em caso de falhas (como um disco rígido estar lotado, ou um processo cair), o servidor Zabbix pode ativamente alertar os administradores da máquina que relatou o problema;



Figura 4 - Projeto de infraestrutura de rede do IFRR

Fonte: <http://projeto.ifrr.edu.br>

Em seguida a lista de itens a serem monitorados (Arquivos, Processos, Execução do Sistema, Ingressos, Servidores, Switches, Roteadores, etc.) para monitorar a rede é o diagrama de rede do IFRR, mostrado como exemplo para a rede de computadores do IFRR, conforme mostrado na Figura 5, que são os elementos da Rede.

⁸ Trigger (Gatilhos): Analisam os itens obtidos e geram alarmes de acordo com condições pré-ajustados – Zabbix (2011).

3 ESTUDO DE CASO

3.1 Implantação do Zabbix

Para o início da implantação do Zabbix, fez-se um levantamento da infraestrutura de rede atual de todos os campi do IFRN. Para isso foi feito uma documentação no Wiki do Redmine⁹ de cada Campus contendo informações de: servidores, Switches, roteadores, links, impressoras de rede, access points como mostra a Figura 4.

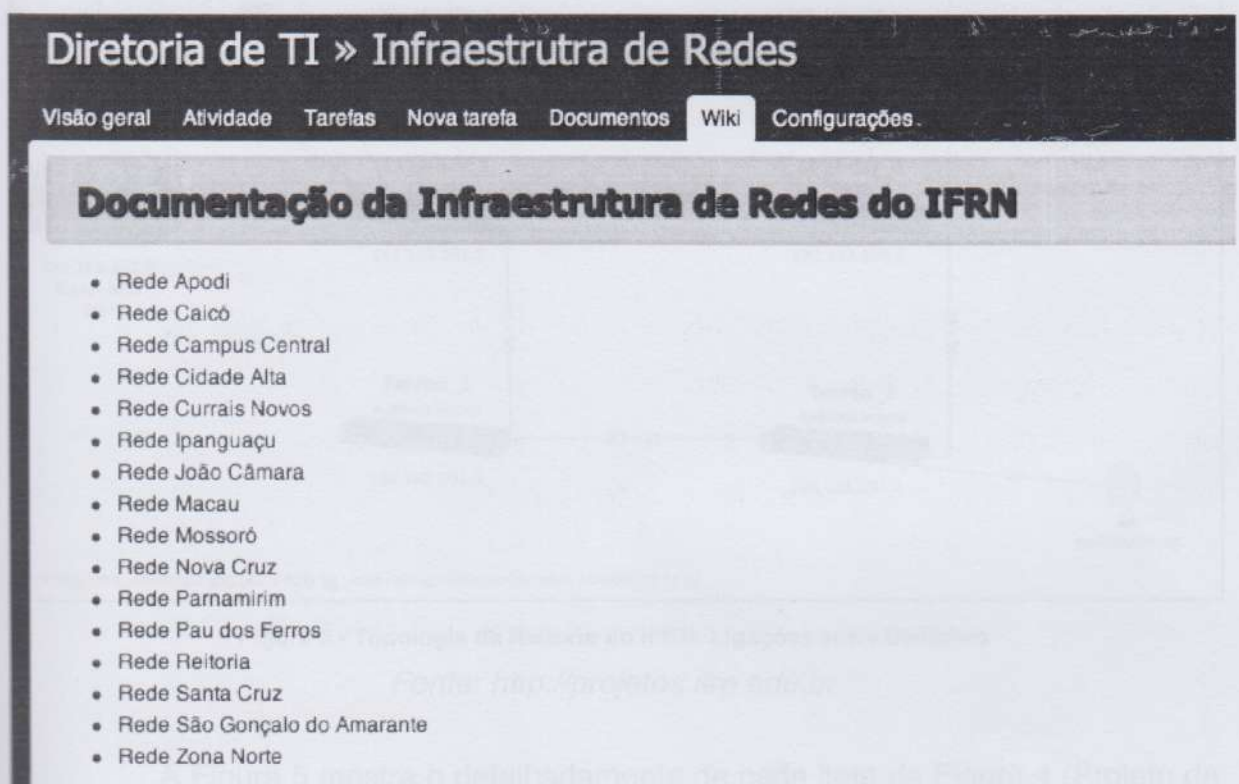


Figura 4 - Projeto de infraestrutura de rede do IFRN

Fonte: <http://projetos.ifrn.edu.br>

Em seguida a listagem de itens a serem documentados (Access Points, Endereçamento do Campus, Impressoras, Servidores, Switches, contato local para eventuais dúvidas e o diagrama de rede feito no Microsoft Visio exportado como imagem para o repositório) dentro de campus do Instituto conforme mostrado na Figura 5, que são os elementos da Reitoria.

⁹ Flexível projeto de aplicação Web de gestão.

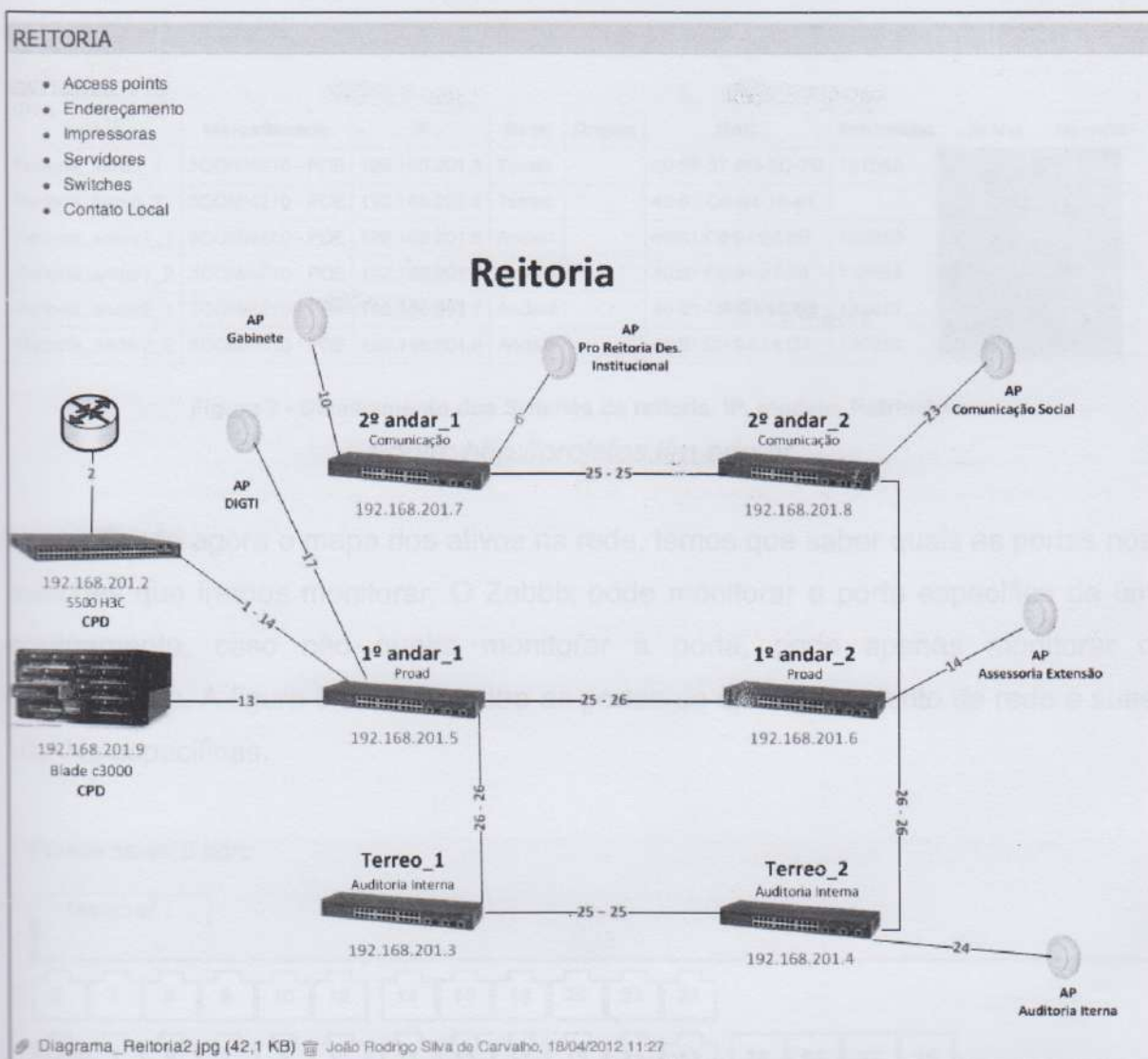


Figura 5 - Topologia da Reitoria do IFRN. Ligações entre Switches

Fonte: <http://projetos.ifrn.edu.br>

A Figura 5 mostra o detalhadamente de cada item da Figura 4 (Projeto de infraestrutura de rede do IFRN), onde damos os nomes as ativos de rede com sua respectivas referências (marca, IP, Rack).

REITORIA

SWITCHES

Switch	Marca/Modelo	IP	Rack	Origem	MAC	Patrimonio	Senha	Usuario
Reitoria_terreo_1	3COM/4210 - POE	192.168.201.3	Terreo		00-22-57-BD-5C-7D	121559		
Reitoria_terreo_2	3COM/4210 - POE	192.168.201.4	Terreo		40-01-C6-94-1F-84			
Reitoria_andar1_1	3COM/4210 - POE	192.168.201.5	Andar1		40:01:C6:94:22:5D	132653		
Reitoria_andar1_2	3COM/4210 - POE	192.168.201.6	Andar1		40:01:C6:94:21:19	132655		
Reitoria_andar2_1	3COM/4210 - POE	192.168.201.7	Andar2		40-01-C6-94-15-B5	132657		
Reitoria_andar2_2	3COM/4210 - POE	192.168.201.8	Andar2		40:01:C6:94:18:C4	132654		

Figura 2 - Detalhamento dos Swiches da reitoria. IP, modelo, Patrimônio

Fonte: <http://projetos.ifrn.edu.br>

Tendo agora o mapa dos ativos na rede, temos que saber quais as portas nos switches que iremos monitorar. O Zabbix pode monitorar a porta específica de um equipamento, caso não queira monitorar a porta, pode apenas monitorar o equipamento. A figura 6 abaixo mostra as portas de um equipamento de rede e suas VLANs específicas.

Please select a port:

Member 1

2 4 6 8 10 12 14 16 18 20 22 24

1 3 5 7 9 11 13 15 17 19 21 23 25 26 27 28

Select All Select None

Port	Untagged Membership	Tagged Membership
1/0/1	1	5,20,30,40,50,60,70,110,130,500

Figura 6 – Configurações das portas de ativo de rede

Fonte: <http://projetos.ifrn.edu.br>

3.2 Informações para o Monitoramento

Algumas das questões levantadas visando o monitoramento da rede foram:

- Quais as informações que trafegam na rede;
- Quais os horários de maior volume de tráfego;
- Disponibilidade de nossos links com os clientes;
- Tempo de resposta dos clientes monitorados;
- Quais clientes estão desligados;
- Motivos que estão impedindo a comunicação com os nossos clientes;
- Disponibilidade de nossos serviços.

Dentro destas questões discutidas, deu-se total importância ao monitoramento dos equipamentos que suportam a comunicação do cliente com a empresa, os servidores da empresa e os servidores dos clientes.

Os principais dados tiveram uma prioridade essencial de monitorar foram:

- Estado os links
- Uso de CPU
- Memória e disco
- Tráfego na rede
- Atraso de banda
- Monitoramento da porta onde estão os links de internet
- Taxas de upload e download
- Servidores ativos
- Telefonia
- Carga de memória nos roteadores e servidores
- Mapa da rede estado nos links

Na figura 7 abaixo, mostra o monitoramento do firewall interno, mostrando tráfego de rede, uso de CPU, memória utilizada, interface interna (WAN) e interface Interna (LAN).

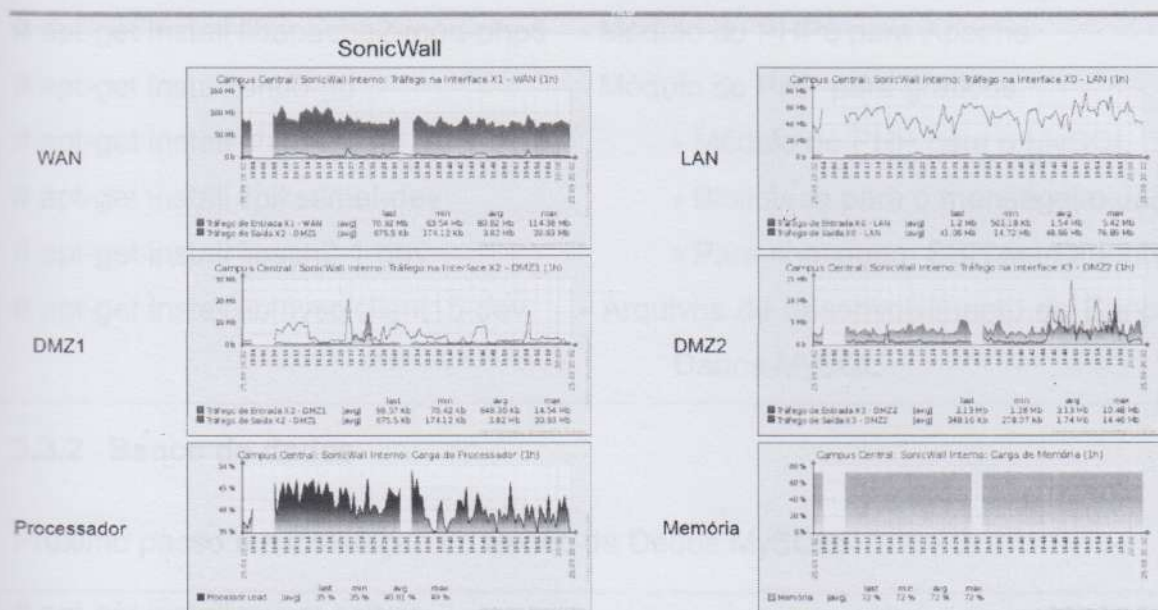


Figura 7 – Tela de monitoramento do Firewall interno.

Fonte: <http://projetos.ifrn.edu.br>

O quanto antes a equipe de TI souber que ele está com problemas, mais rápido pode-se tentar recolocar o serviço ativo.

3.3 Instalação do sistema Zabbix

A instalação do Zabbix Server ou Agent a partir do source requer alguns software adicionais, como visto a seguir.

3.3.1 Preparação do sistema

No quadro a seguir a instalação dos diversos softwares necessários através do utilitário de instalação de pacotes "apt-get".

# apt-get update	
# apt-get install openssh-server	- Proporciona acesso remoto ao servidor
# apt-get install build-essential	- Compilador GCC, bibliotecas, etc
# apt-get install fping	- Fping - teste de conectividade usando o ICMP
# apt-get install apache2	- Apache - servidor WEB
# apt-get install libsnmp-dev	- Bibliotecas Net-SNMP
# apt-get install libcurl4-openssl-dev	- Bibliotecas Curl para monitoramento WEB

```
# apt-get install libapache2-mod-php5 - Módulo do PHP5 para Apache
# apt-get install php5-gd             - Módulo do PHP para gráficos
# apt-get install php5-mysql          - Módulo do PHP para o MySQL
# apt-get install libiksemel-dev      - Biblioteca para o mensageiro Jabber
# apt-get install libssh2-1-dev       - Para checagem SSH sem agente
# apt-get install libmysqlclient15-dev - Arquivos de desenvolvimento do Banco de
                                         Dados MySQL
```

3.3.2 Banco de dados

Próximo passo é a instalação do Banco de Dados MySQL:

```
# apt-get install mysql-server
    <senha de root do mysql>
```

3.3.3 Instalação e configuração do Zabbix 1.8.3

Criação do usuário do Zabbix.

• Passo 1 - Criação do usuário

```
~# sudo adduser zabbix
<password>
<confirm>
```

• Passo 2 - Download e Untar do Source

Utilizando o usuário 'zabbix':

```
# su - zabbix
#wget
http://sourceforge.net/projects/zabbix/files/ZABBIX%20Latest%20Stable/1.8.3/zabbix
-1.8.3.tar.gz
~$ tar xfvz zabbix-1.8.3.tar.gz
```

Lembrando que será criado um diretório chamado **zabbix-1.8.3** após a extração do arquivo comprimido.

• Passo 3 - Criar o Banco de Dados Zabbix

```
~$ mysql -p
<senha de root do MySQL>

mysql> create database zabbix character set utf8;
Query OK, 1 row affected (0.00 sec)

mysql> grant all privileges on zabbix.* to <username>@localhost identified by
'<password>';
Query OK, 0 rows affected (0.01 sec)

mysql> quit;
```

Passo 4 - Configurar, compilar e instalar o servidor

```
~$ su -
<root_password>
~# cd /home/zabbix/zabbix-1.8.3/
~# ./configure --enable-server --enable-agent --with-mysql --with-net-snmp --with-
jabber --with-libcurl --prefix=/usr/local/zabbix
~# make install
```

Por padrão, o comando “make install” irá instalar todos os arquivos em /usr/local/bin, /usr/local/lib, etc. Pode-se usar outro diretório para instalação diferente do /usr/local usando -prefix, como acima. Neste caso, os binários serão instalados em <prefix>/sbin, os utilitários em <prefix>/bin e as Man pages em <prefix>/share

Passo 5 - Configurar o /etc/services

Este passo é opcional. No entanto, é recomendado.

```
~# vim /etc/services
```

Nos clientes, podem ser adicionadas as seguintes linhas final do arquivo:

```
zabbix-agent 10050/tcp # Zabbix Agent
```

```
zabbix-agent 10050/udp # Zabbix Agent
zabbix-trapper 10051/tcp # Zabbix Trapper
zabbix-trapper 10051/udp # Zabbix Trapper
```

Uma boa prática usada é sempre salvar os arquivos antes de sair. Esses números de portas são as oficiais do Zabbix, registrados na IANA.

• Passo 6 - Configurar o agente e servidor

Copiar os arquivos de configuração e alterá-los corrigindo os dados solicitados.

```
~# cd /usr/local/zabbix/
~# mkdir etc
~# cd etc/
~# cp /home/zabbix/zabbix-1.8.3/misc/conf/zabbix_agentd.conf .
~# cp /home/zabbix/zabbix-1.8.3/misc/conf/zabbix_server.conf .
```

Na configuração do cliente:

```
~# cd /usr/local/zabbix/etc
~# vim zabbix_agentd.conf
```

Deve ser certificado que esta configuração aponte corretamente para as definições do servidor. Para o agente que executa no próprio servidor, deve ficar da seguinte forma:

```
Server=127.0.0.1
```

Deve-se descomentar a seguinte opção:

```
PidFile=/tmp/zabbix_agentd.pid
```

Após os procedimentos acima, o arquivo deve ser salvo.

Na configuração do servidor:

```
~# cd /usr/local/zabbix/etc
~# vim zabbix_server.conf
```

Alterar as seguintes linhas com as informações do usuário do banco que foram criadas no Passo 3:

```
# Database user
```

```
DBUser=<username>
```

```
# Database password
```

```
# Comment this line if no password used
```

```
DBPassword=<password>
```

Após os procedimentos acima, o arquivo deve ser salvo.

• Passo 7 - Configurar o Apache

Copiando os arquivos do php do zabbix diretamente para o /var/www/ faz-se desnecessário alterar o Virtual Host default.

```
~# cd /var/www/
```

```
~# cp -r /home/zabbix/zabbix-1.8.3/frontends/php.
```

- Copia os arquivos

```
~# mv php zabbix
```

- Renomea a pasta

```
~# /etc/init.d/apache2 restart
```

- Reinicia o Apache

Finalmente, os serviços podem ser iniciados com comandos abaixo:

```
~# /etc/init.d/zabbix-server start
```

- inicia o serviço

```
~# /etc/init.d/zabbix-agent start
```

- para o serviço

Para verificar se eles estão em execução, o comando abaixo pode ser usado.

```
~# ps aux | grep zabbix
```

3.3.4 Finalizando a configuração via Web

Usando um navegador, o zabbix pode ser acessado e confirme os itens abaixo.

```
http://<nome-do-servidor ou ip/zabbix/
```

1. Introduction

Deve-se ler e clicar em Next.

2. License Agreement

Deve-se marcar a opção "I Agree" e clicar em Next.

3. Check of Pre-Requisites

No servidor, o arquivo de configuração do php deve ser aberto e alterado com as seguintes opções:

```
~# vim /etc/php5/apache2/php.ini

max_execution_time = 300 ; Maximum execution time of each script, in seconds
max_input_time = 300 ; Maximum amount of time each script may spend
parsing request data
post_max_size = 32M
date.timezone =America/Recife
mbstring.func_overload = 7

~# /etc/init.d/apache2 restart
```

Caso o "timezone" não seja esse, deve-se verificar qual aplica-se em <http://us3.php.net/manual/en/timezones.php>, e a atualização da página pode ser feita no navegador e verificar se todos os erros foram corrigidos. Feito isso, deve-se ir para a próxima etapa clicando em Next.

• 4. Configure DB Connection

As informações de usuário e senha devem ser adicionadas no Banco de Dados do Zabbix (as mesmas que foram usadas no `zabbix_server.conf`). Deve-se clicar em Test Connection e verificar se a conexão está OK. Quando estiver, pode-se avançar para a próxima etapa clicando em Next.

• 5. ZABBIX server details

Faz-se a verificação do nome do host e a porta.

• 6. Pre-Installation Summary

Confirmar se todas as configurações estão corretas.

• 7. Install

Nesse ponto, deve-se clicar em "Save configuration file" e salvar o arquivo `zabbix.conf.php` na máquina local. Via SSH, deve-se salvar o arquivo adquirido em

/var/www/zabbix/conf/. Uma forma de realizar esse procedimento é utilizar o scp. Na máquina local:

```
$ scp zabbix.conf.php root@<ip_do_servidor>:/var/www/zabbix/conf/
<root_password>
```

Caso o sistema operacional utilizado seja o Windows, pode-se utilizar o software "winscp" (<http://winscp.net/eng/index.php>) para arrastar e soltar o arquivo dentro do servidor Zabbix.

Agora, clica-se em Next.

• 8. Finish

Clicar em Finish para finalizar a configuração.

Será aberta uma tela de login do servidor Zabbix. Por default, o login é 'Admin' e a senha 'zabbix'.

3.3.5 Zabbix – Cadastrando hosts

Assim que o Zabbix é instalado, ele possui apenas um host cadastrado. O próprio servidor Zabbix. Para poder monitorar seus servidores e ativos de rede, deverá ter um cadastro cada um deles.

Para isso, deve-se clicar no menu Configuração > Hosts e clique no botão Criar Host no canto superior direito. Irá aparecer a seguinte tela:

Figura 8 – Cadastramento de hosts

Fonte: <http://projetos.ifrn.edu.br/wiki>

Nela, as informações mais importantes são o Nome do Host, o Grupo e o Endereço IP. Sem elas, não é possível adicionar o host com sucesso. É nesta tela também, que se poderá associar um template (modelo) a um host.

Para isso, deve-se acessar o menu Adicionar na área Associado aos templates no lado direito da tela, selecione o Grupo Templates no menu drop-down do pop-up que surge, marque o template desejado e clique em Selecionar ao final da janela.

Pode-se observar que o template selecionado agora se encontra dentro da caixa relacionado aos templates. Para dessassociar, marque o template e deve ser pressionado o botão Dessassociar, no mesmo local. Lembrando que, somente dessassociando, todos os itens, antes linkados ao host pelo template, ainda se encontram monitorando o host e agora são nativos do próprio host.

Caso seja necessário dessassociar o template e limpar os itens de monitoramento do host, clique-se em Dessassociar e limpar.

3.3.6 Criando itens

Após cadastrado o host, ele irá aparecer junto aos demais numa lista acessada no menu Configuração > Hosts. Cada linha é um host, e possui informações de Aplicações, Itens, Triggers, Gráficos, DNS, IP, Templates, Status e Disponibilidade.

Os Itens são a forma que o Zabbix possui de coletar os dados. Ou seja, cada item irá coletar um dado, e eles serão a fonte de informações para gerar os gráficos e gatilhos do Zabbix. Para criar um item direto no host, deve-se clicar em Itens na linha do host desejado.

Será aberta uma outra página, com a lista dos itens relacionados a este host.

Para um novo item, clica-se em Criar item no canto superior direito. A tela de novo item é a da figura 9.

Item: Switch de Teste

Host	Switch de Teste	Selecionar
Descrição		
Tipo	Agente ZABBIX	
Chave		Selecionar
Tipo de informação	Numérico (inteiro sem sinal)	
Tipo de dados	Decimal	
Unidades		
Usar multiplicador	Não usar	
Intervalo atualização (em seg)	30	
Intervalos flexíveis (seg)	Não há intervalos flexíveis definidos	
Novo intervalo flexível	Espera 50	Período 1-7,00:00-23:59
	Adicionar	
Manter histórico (em dias)	90	
Manter estatísticas (em dias)	365	
Status	Ativo	
Armazenar valor	Sem alterar	
Mostrar valor <u>throw map</u>	Sem alterar	
Nova aplicação		
Aplicações	-Nenhum-	

Grupo: APs

Salvar Cancelar

Adicionar ao grupo do

Figura 9 – Criando itens

Fonte: <http://projetos.ifrn.edu.br>

3.3.7 Zabbix – Criando Templates

O template nada mais é do que um "modelo" de host, com todos os itens, gatilhos e gráficos necessários para que, quando aplicados a um host, dispensem a criação de tais objetos host a host. Sendo assim, será necessário criar um template para cada modelo de equipamento que se desejar monitorar.

Para monitorar cada host são necessários um conjunto de itens de interesse e cada um desses itens deve ser criado no seu respectivo host.

Para poupar o trabalho de criar todos os itens repetidamente, especialmente se tratarem de hosts similares como switches do mesmo modelo, servidores linux, etc, foram criados os templates.

Assim, caso seja necessário fazer alguma modificação, basta alterar o desejado no template e essa modificação será aplicada a todos os hosts linkados ao template.

Felizmente, o Zabbix já traz alguns templates prontos, normalmente para equipamentos mais "comuns" das marcas Cisco, Dell, HP, máquinas Linux, Windows, FreeBSD, MacOS X, OpenBSD, Solaris, e serviços como Exchange e SQLServer.

Os templates trazidos pelo Zabbix e todos os templates que forem criados poderão ser encontrados no menu Configuração > Hosts escolhendo Templates nos dois menus drop-down presentes no canto superior direito da tela conforme a figura 10.



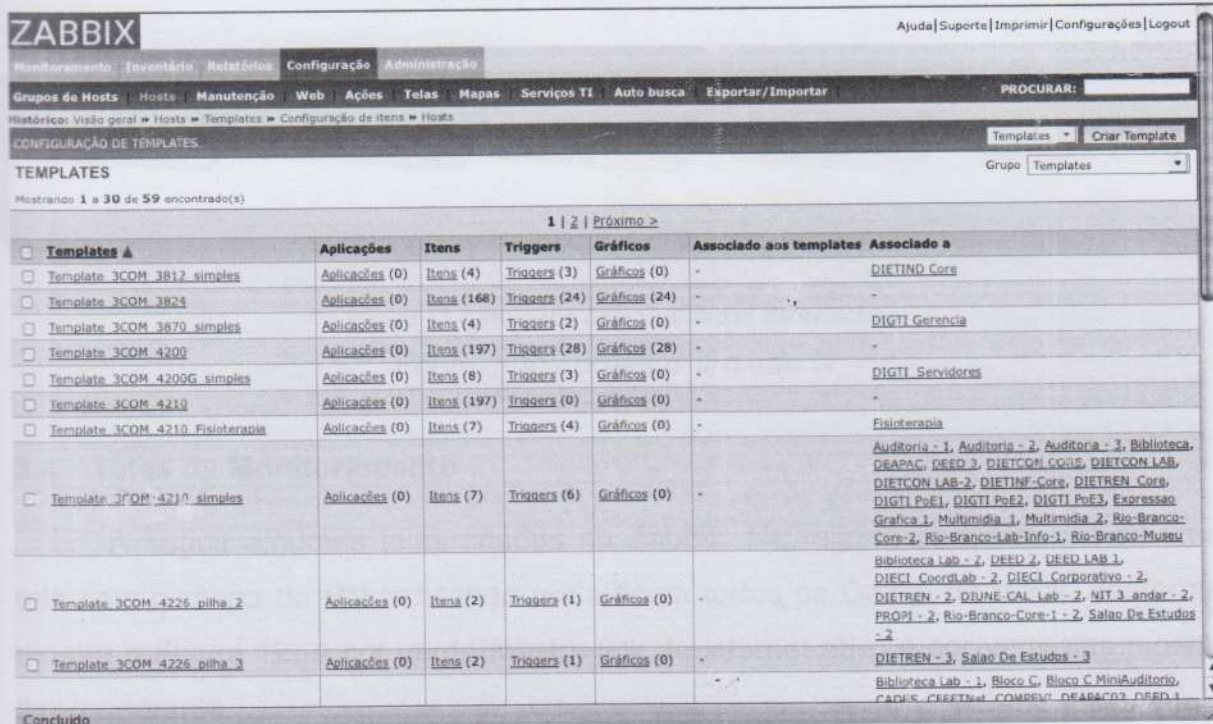


Figura 10 – Criando templates

Fonte: <http://projetos.ifrn.edu.br>

3.3.8 Zabbix – Adicionando imagens personalizadas

Para personalizar e dar seu toque pessoal aos seus mapas, pode-se adicionar imagens diferentes ao Zabbix. Elas podem ser adicionadas como Ícones ou Fundos.

Primeiramente, busca-se e trata a imagem que deseja utilizar, deixando, de preferência, um .PNG com fundo transparente.

O Zabbix possui as seguintes opções de personalização de ícones:

Ícone Padrão	Problema	Desconhecido	Manutenção	Desabilitado
--------------	----------	--------------	------------	--------------

Deve-se salvar as imagens separadamente.

A seguir, um exemplo de um switch 4226t. Depois de tratadas, as imagens ficaram como na figura 11.

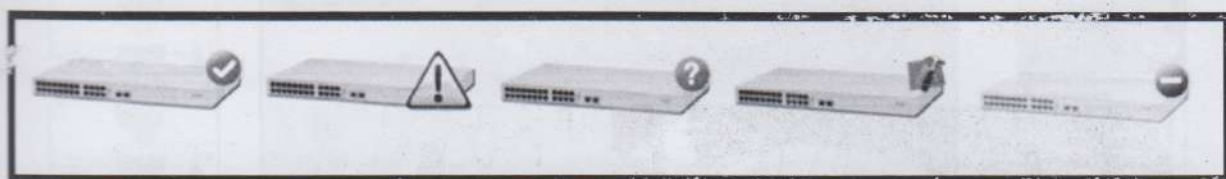


Figura 11 – Imagens personalizadas de switches

Fonte: <http://projetos.ifrn.edu.br>

3.4 Telas de Monitoramento

A seguir algumas telas criadas no Zabbix. Na reitoria do IFRN usa-se uma tela com o mapa do RN indicando onde ficam todos os Campi do IFRN, conforme mostra a Figura 12. A cor verde mostra link de internet ativo e cor vermelha mostra link inoperante.

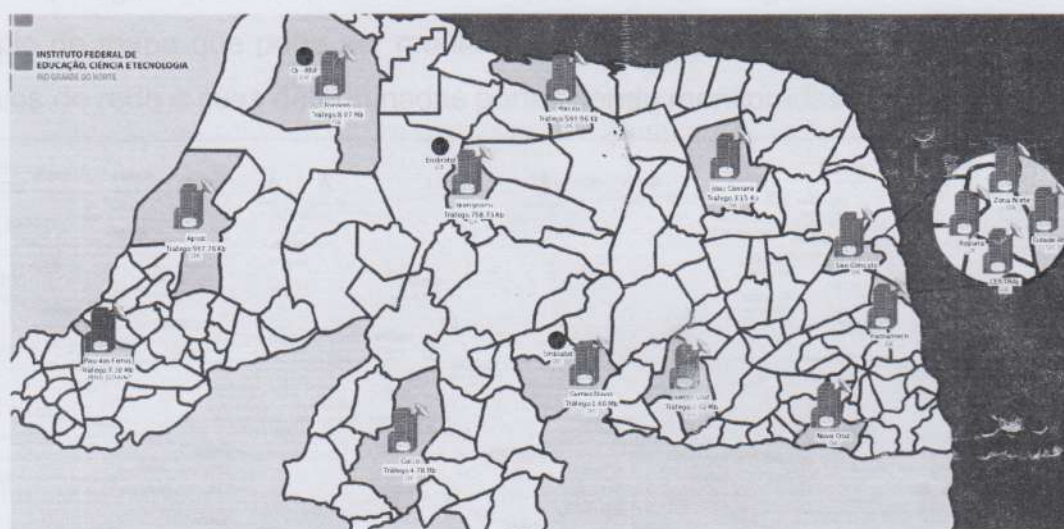


Figura 12 - Mapa IFRN Interior. Mostrando toda a atividade dos links de internet

Fonte: <http://projetos.ifrn.edu.br>

Na topologia da rede VoIP, a Figura 13 mostra como é a topologia adotada para esse projeto de telefonia implantado recentemente no IFRN.

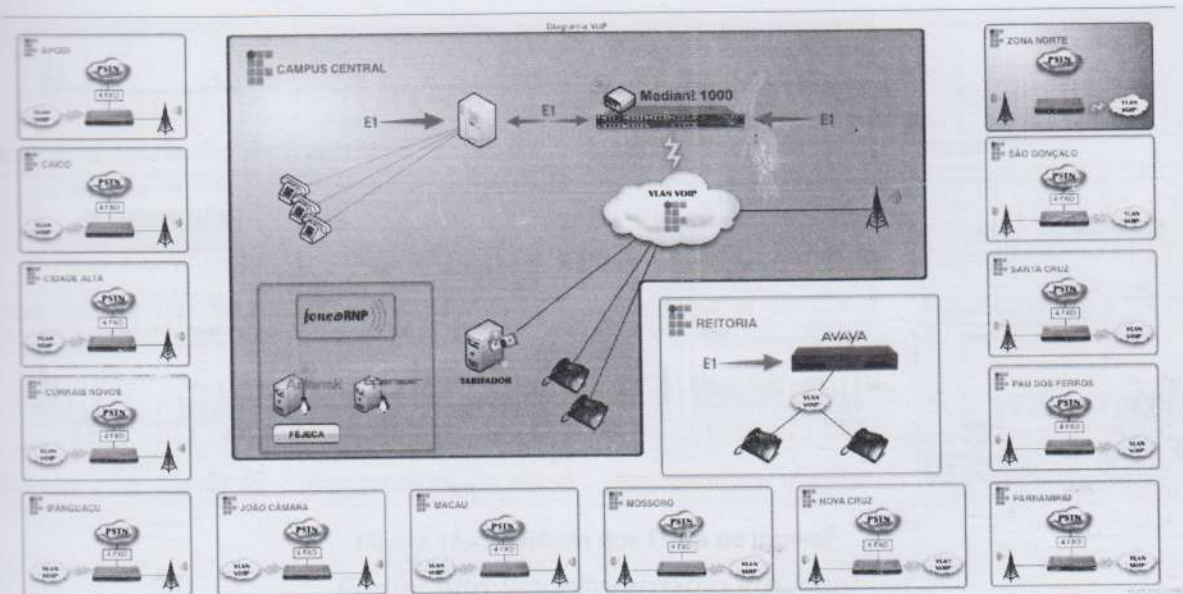


Figura 13 - Diagrama da Rede Voip. Telefonia do IFRN

Fonte: <http://projetos.ifrn.edu.br>

Topologia rede CNAT – Rede Campus Central! A figura 14 mostra um outro exemplo de mapa que pode ser montado dentro do Zabbix. Uma topologia usando os ativos de rede e suas determinadas portas sendo monitoradas.

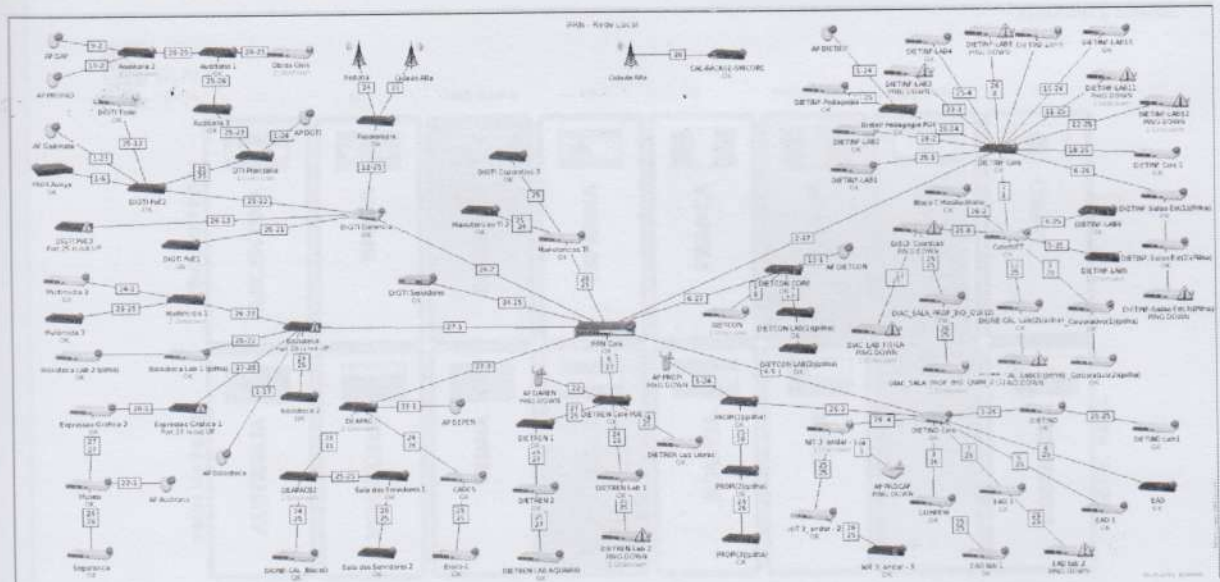


Figura 14 - Rede local CNAT. Campus Natal Central - Topologia dos ativos de rede

Na figura 15, a tela onde o todo tráfego dos links nos Campi do interior é monitorado. As taxas de *upload* e *download* do link de cada local.

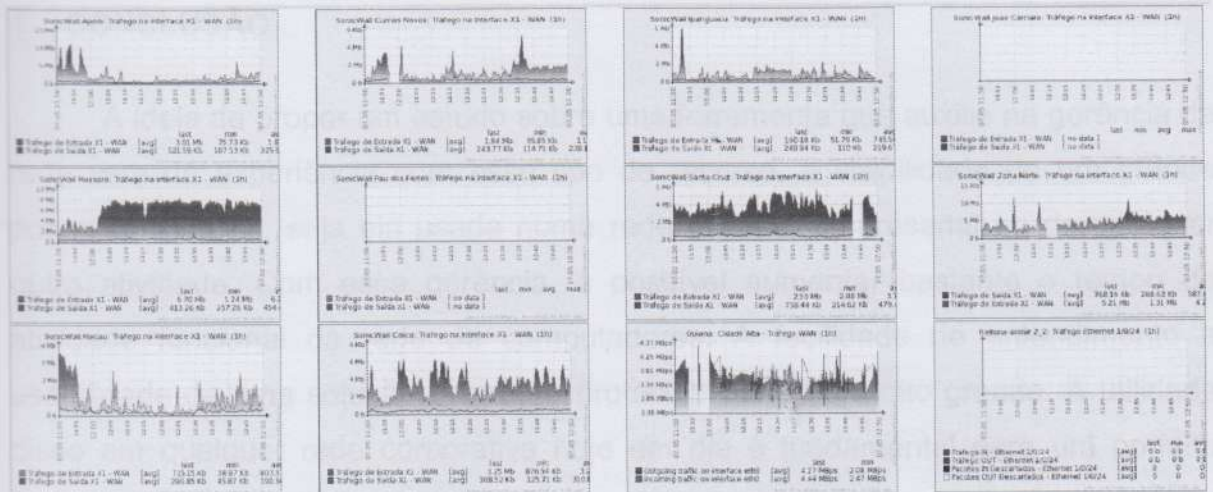


Figura 15 - Atividade dos Links do Interior
Fonte: <http://monitoramento.ifrn.local>

Na figura 16, a tela dos servidores dentro no nosso Datacenter que estão ativos ou não. Em vermelho, os inativos e com o "ok" estão os ativos.

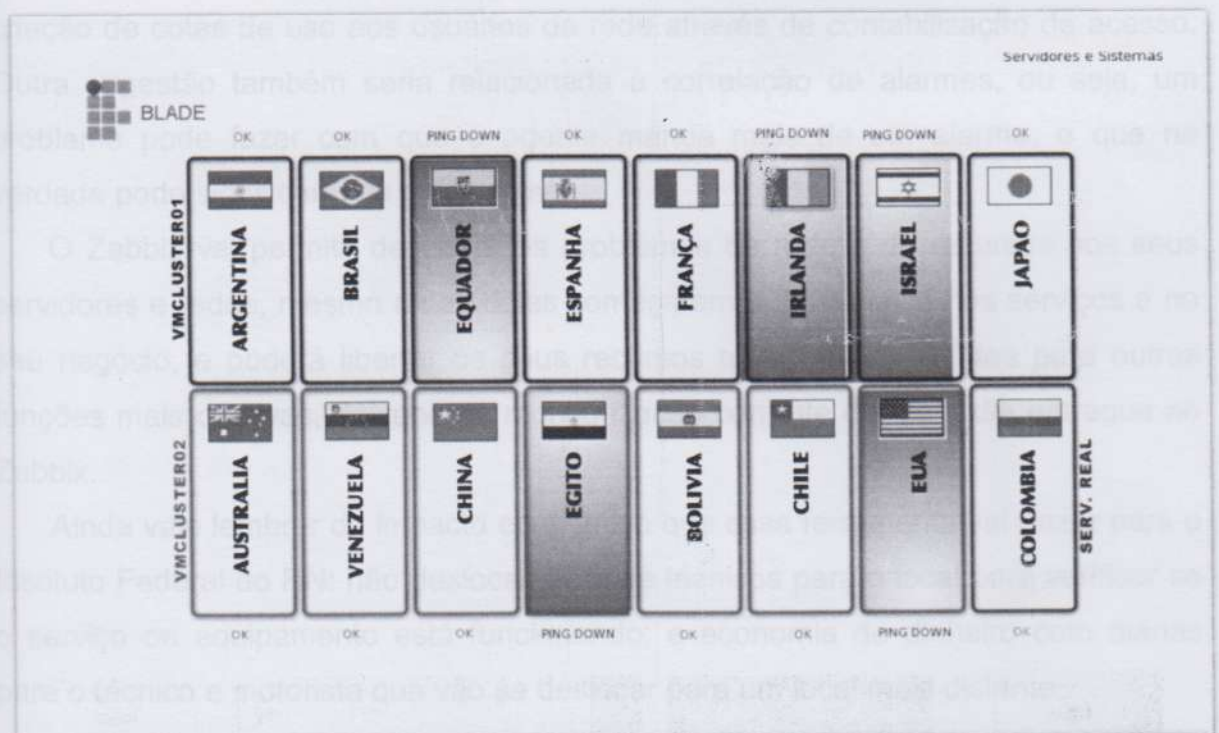


Figura 16 - Servidores Ativos e Inativos.
Fonte: <http://projetos.ifrn.edu.br>

4 CONCLUSÃO

A ideia de propor um estudo sobre uma ferramenta que auxilie na gerência de rede vem da experiência com esse tipo de recurso, a visibilidade de um grande potencial da área, seja ela usada numa rede escolar, empresarial ou de qualquer outra atividade. Com essa gerência, é possível aumentar bastante o tempo de atividade funcional da rede de computadores. A facilidade de entendimento e usabilidade de uma solução usando o protocolo SNMP é muito grande. A utilidade disso em qualquer rede corporativa hoje em dia é fundamental para um perfeito funcionamento da mesma.

Outro ponto forte desta proposta é de estar trabalhando com tecnologias totalmente livres para seu uso, o que condiz muito com o propósito de quem usa a plataforma Linux, não só pela sua robustez, segurança e confiabilidade, mas também por sua liberdade.

Essa é somente uma idéia inicial, que pode crescer muito. Têm muitas áreas para serem abordadas ainda, como por exemplo, a questão de tarifação, ou seja, criação de cotas de uso aos usuários da rede através de contabilização de acesso. Outra sugestão também seria relacionada à correlação de alarmes, ou seja, um problema pode fazer com que o agente mande mais de um alarme, o que na verdade pode significar uma única coisa.

O Zabbix vai permitir descobrir os problemas de rede e de recursos nos seus servidores e redes, mesmo antes deles começarem a ter impacto nos serviços e no seu negócio, e poderá libertar os seus recursos técnicos importantes para outras funções mais criativas, deixando a monitorização corrente do dia-a-dia entregue ao Zabbix.

Ainda vale lembrar do impacto econômico que essa ferramenta vai trazer para o Instituto Federal do RN: não deslocamento de técnicos para o local para verificar se o serviço ou equipamento está funcionando; e economia de dinheiro com diárias para o técnico e motorista que vão se deslocar para um local mais distante.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDREDEO. Monitorando um equipamento via zabbix. Disponível em: <http://andredeo.blogspot.com/2009/03/monitorando-um-equipamento-via-zabbix.html>. Acessado em: 25 setembro de 2012.

CARVALHO, Tereza Cristina Melo de Brito. Gerenciamento de redes: uma abordagem de sistemas abertos. Sao Paulo: Makron Books, 1993. 364p.

CISCO. CCNA Exploration. Disponível em: http://www.cisco.com/web/BR/educacao/netacad/programa/cursos/info_cursos_ccna.html. Acessado em 08 de outubro de 2012.

DEBIAN. Getting Debian. Disponível em: <http://www.debian.org/distrib/>. Acessado em 6 de maio de 2012.

IETF. Request for Comments. (RFC) Disponível em: <http://www.ietf.org/rfc.html>. Acessado em 29 de setembro de 2012.

REDERIO. Nt00601. Disponível em: <http://www.rederio.br/downloads/pdf/nt00601.pdf>. Acessado em: 15 setembro de 2012.

UNDERLINUX. Tutoriais/monitoramento/zabbix . Disponível em: <http://underlinux.org/wiki/Tutoriais/Monitoramento/zabbix>. Acessado em: 27 agosto 2012

VIVAOLINUX. Instalando o zabbix 1.6.6 no debian 5. Disponível em: <http://www.vivaolinux.com.br/artigo/Instalando-o-Zabbix-1.6.6-no-Debian-5/>. Acessado em: 12 de agosto 2012.

VIVAOLINUX. Instalando o zabbix. 2010. Disponível em: <http://www.vivaolinux.com.br/artigo/Instalando-o-Zabbix?pagina=1>. Acessado em: 27 agosto 2012.

VIVAOLINUX. Linux. Disponível em: <http://www.vivaolinux.com.br/linux/>. Acessado em: 18 de setembro 2012.

WIKIPEDIA. Protocolo. Disponível em: <http://pt.wikipedia.org/wiki/Protocolo>. Acessado em 15 de setembro de 2012.

ZABBIX. Zabbix mapas 2. Disponível em: <http://www.zabbix.com/documentation/pt/1.8/manual/sobre>. Acessado em: 12 de setembro de 2012.