

**INSTITUTO FEDERAL GOIANO - CAMPUS MORRINHOS  
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS PARA  
INTERNET**

**JOÃO VICTOR GONÇALVES DE PAULA**

**IMPLANTAÇÃO DO ZABBIX NO IF GOIANO CAMPUS  
MORRINHOS**

**MORRINHOS – GO  
2016**

**JOÃO VICTOR GONÇALVES DE PAULA**

**IMPLANTAÇÃO DO ZABBIX NO IF GOIANO CAMPUS  
MORRINHOS**

Monografia apresentada ao Curso Superior de Tecnologia em Sistemas para Internet do Instituto Federal Goiano - Campus Morrinhos, como requisito parcial para obtenção de título de Tecnólogo em Sistemas para Internet. Área de concentração: Desenvolvimento de Sistemas. Orientadora: MSc. Ana Maria Martins Carvalho.

**MORRINHOS - GO  
2016**

**Dados Internacionais de Catalogação na Publicação (CIP)**  
**Sistema Integrado de Bibliotecas – SIBI/IF Goiano Campus Morrinhos**

P324i Paula, João Victor Gonçalves de.

Implantação do Zabbix no IF Goiano Campus Morrinhos. /  
João Victor Gonçalves de Paula. – Morrinhos, GO: IF  
Goiano, 2016.

122 f. : il. color.

Orientador: M.<sup>a</sup> Ana Maria Martins Carvalho.

Trabalho de conclusão de curso (graduação) – Instituto  
Federal Goiano Campus Morrinhos, Tecnologia em Sistemas  
para Internet, 2016.

1. Zabbix. 2. Monitoramento de rede. 3. Rede de  
computadores I. Carvalho, Ana Maria Martins. II. Instituto  
Federal Goiano. Tecnologia em Sistemas para Internet. III.  
Título

CDU 004.7(043)

# JOÃO VICTOR GONÇALVES DE PAULA

## IMPLANTAÇÃO DO ZABBIX NO IF GOIANO CAMPUS MORRINHOS

Data da defesa: 08 de julho de 2016.

Resultado: \_\_\_\_\_

### BANCA EXAMINADORA

### ASSINATURAS

Ana Maria Martins Carvalho Profº MSc. \_\_\_\_\_  
Instituto Federal Goiano Campus Morrinhos

Antônio Neco de Oliveira Profº MSc. \_\_\_\_\_  
Instituto Federal Goiano Campus Morrinhos

José Pereira Alves Profº Esp. \_\_\_\_\_  
Instituto Federal Goiano Campus Morrinhos

**MORRINHOS - GO  
2016**

## **DEDICATÓRIA**

Dedico este trabalho aos meus pais Fábio e Adriana, à minha namorada Helouíse e a todos meus amigos que colaboraram e incentivaram para que este fosse concluído.

## **AGRADECIMENTOS**

Primeiramente gostaria de agradecer a Deus pela vida, aos meus pais que sempre me incentivaram aos estudos e apoiaram em minhas decisões e a todos os professores que puderam compartilhar parte de seus conhecimentos comigo.

À professora Ana Maria Martins Carvalho, por todo apoio durante o período dentro e fora da orientação, por todos os ensinamentos e conselhos.

## RESUMO

Este trabalho tem como propósito o estudo da ferramenta de monitoramento open source, Zabbix em sua versão 2.4.6, e finalidade de realizar a implantação da mesma no IF Goiano Campus Morrinhos. Busca realizar uma administração de forma centralizada de parte do parque tecnológico que a instituição possui. Contempla a distribuição do Zabbix em quatro servidores distintos, afim de verificar como a ferramenta se comporta, facilitar o gerenciamento e recuperação das informações em caso de algum incidente. Foi verificado, através da ferramenta, status de atividade de serviços e ativos de rede, consumo de recursos como memória ram, hd e tráfego de rede. Também dispôs dos recursos de mapeamento e envio de alertas através do whatsapp e e-mail, na busca de facilitar a identificação dos incidentes na rede. Através do monitoramento via SNMP, ICMP e Agent do Zabbix, foi possível coletar informações de equipamentos como servidores, câmeras de segurança, telefones VoIP, switchs e antenas sem fio nanostations. Conclui que a ferramenta de monitoramento é bastante dinâmica e robusta, abrindo novas possibilidades para sua expansão no Campus, vindo a monitorar novos recursos, buscando maior eficácia na gerencia da estrutura da instituição.

**Palavras-Chaves:** Zabbix, Monitoramento de rede, Redes de computadores.

## SUMMARY

This work aims to study the open source monitoring tool, Zabbix in its version 2.4.6, and purpose of carrying out the implementation of it in the IF Goiano Campus Morrinhos. Seeking to achieve better management of centralized part of the technological park that the institution has. This work includes the distribution of Zabbix in four different servers in order to verify how the tool would behave, and easier management and retrieval of information in the event of disaster. It was verified through the status tool service activity and network assets, consumption of resources as ram, HD and network traffic. And he set the mapping of resources and sending alerts via whatsapp and email, seeking to facilitate the identification and network incidents. By monitoring via SNMP, ICMP and Agent Zabbix, it was possible to collect information from devices such as servers, security cameras, VoIP phones, switches and wireless antennas NanoStation model. Zabbix was effective with the way in its implementation was carried out, proved to be very dynamic and robust, opening up new possibilities for its expansion on the campus, been monitoring new features, seeking greater efficiency in the management structure of the institution.

**Keywords:** Zabbix, Network monitoring, Computer network.

## LISTA DE TABELAS

Tabela 1 Tipos de Mensagem ICMP .....	28
Tabela 2 Requisitos de Hardware do Zabbix Fonte: Ricardo Pinheiro .....	35
Tabela 3 Tabela de Templates Utilizados .....	39
Tabela 4 Tabela ICMP.....	40
Tabela 5 Template S.O. ....	42
Tabela 6 Template SNMP .....	43
Tabela 7 Template Monitoramento WEB.....	44
Tabela 8 Estrutura Template App Zabbix Server e Proxy .....	45
Tabela 9 Template App Mysql.....	46

## LISTA DE FIGURAS

Figura 1 Funcionamento de um sistema de gerenciamento de rede.....	17
Figura 2 Modelo de Referência OSI e TCP/IP .....	24
Figura 3 Cabeçalho UDP .....	26
Figura 4 Componentes SNMP .....	29
Figura 5 Distribuição de Hardwares para os Servidores .....	36
Figura 6 Interfaces de rede e respectivos endereços IPs.....	37
Figura 7 Templates Utilizados .....	38
Figura 8 Componentes dos Templates.....	38
Figura 9 Notificação Trigger ICMP: WhatsApp.....	40
Figura 10 Incidente Trigger ICMP.....	41
Figura 11 Alerta Trigger ICMP: MAPA.....	41
Figura 12 Alerta Trigger ICMP: e-mail.....	41
Figura 13 Dados Coletados dos Switchs via SNMP .....	43
Figura 14 Velocidade e Tempo de resposta site friendzone.net.br .....	44
Figura 15 Velocidade e Tempo de resposta site s2bifgoiano.net.br .....	45
Figura 16 Desempenho Zabbix Proxy .....	46
Figura 17 Desempenho Zabbix Server.....	46
Figura 18 Desempenho de rede Mysql.....	47
Figura 19 Desempenho de consultas Mysql.....	47
Figura 20 Gráfico: Utilização de processador.....	48
Figura 21 Gráfico utilização Memória Ram. ....	48
Figura 22 Gráfico Tráfego de rede .....	48
Figura 23 Gráfico utilização de Disco .....	49
Figura 24 Mapa de status da telefonia do Campus .....	50
Figura 25 Mapa de localização das câmeras de segurança.....	50
Figura 26 Mapa de tráfego das nanostation .....	51
Figura 27 Mapa de tráfego dos switches.....	51
Figura 28 Tela com gráficos das interfaces Eth0 dos servidores .....	52
Figura 29 Tela com gráfico das interfaces do Zabbix .....	52
Figura 30 Tela interfaces do servidor Zabbix Proxy II .....	53
Figura 31 Tela consumo de memória ram dos servidores.....	53

Figura 32 Tela uso de processador dos servidores.....	53
Figura 33 Tela desempenho do serviço zabbix e Mysql.....	54
Figura 34 Tela mapeamento câmeras de segurança.....	54
Figura 35 Tela mapeamento telefonia.....	55
Figura 36 Tela mapeamento tráfego switch.....	55
Figura 37 Tela de mapeamento do tráfego Nanostation.....	56
Figura 38 Tela de Boas Vindas do Zabbix.....	77
Figura 39 Checagem de Pré Requisitos.....	78
Figura 40 Configuração do Banco de Dados.....	78
Figura 41 Detalhes do ZabbixServer.....	79
Figura 42 Resumo da Instalação.....	79
Figura 43 Finalização da configuração no navegador.....	80
Figura 44 Dashboard Zabbix.....	81
Figura 45 Portlet Status do Zabbix.....	81
Figura 46 Portlet Status do Sistema.....	82
Figura 47 Portlet Status do Host.....	82
Figura 48 Portlet Ultimos 20 Incidentes.....	83
Figura 49 Portlet Monirotamento Web.....	83
Figura 50 Portlet Status Auto Busca.....	83
Figura 51 Zabbix Proxy Criando Proxy.....	92
Figura 52 Zabbix Proxy Atividade Proxy.....	92
Figura 53 Zabbix Proxy Criando Host Proxy.....	93
Figura 54 Zabbix Proxy Template.....	93
Figura 55 Zabbix Proxy Status.....	94
Figura 56 Tipo de Midia e-mail.....	99
Figura 57 Criação do grupo de usuário de e-mail.....	100
Figura 58 Criação das ações a serem notificadas via e-mail.....	101
Figura 59 Criação das Condições das ações.....	102
Figura 60 Criação das Ações.....	103
Figura 61 Preparação do envio da notificação via e-mail.....	104
Figura 62 Envio de notificação via e-mail com sucesso.....	104
Figura 63 e-mail de Notificação Trigger: Problema.....	104
Figura 64 e-mail de Notificação Trigger: OK.....	105
Figura 65 Mensagem de Teste do Yumsup.....	108

Figura 66 Criação Mídia Script Whatsapp .....	110
Figura 67 Criação do grupo de notificação do Whatsapp.....	111
Figura 68 Permissão do grupo notificação WhatsApp.....	112
Figura 69 Criação de usuário .....	113
Figura 70 Mídia WhatsApp usuário Joao.....	114
Figura 71 Permissão de usuário do grupo WhatsApp .....	114
Figura 72 Ação notificação WhatsApp.....	115
Figura 73 Notificação WhatsApp em Andamento .....	116
Figura 74 Notificação WhatsApp enviada.....	116
Figura 75 Notificação de problema e OK via e-mail .....	116
Figura 76 Notificação de Problem e OK no WhatsApp.....	117
Figura 77 Serviço Zabbix Agente Windows.....	119
Figura 78 Regras de entrada Firewall Windows.....	120
Figura 79 Criação de Grupo de Hosts .....	121
Figura 80 Escolha do ZabbixProxy Fonte: Autor .....	122
Figura 81 Hosts Servidores Windows OK .....	122
Figura 82 Hosts Windows 7 Problema .....	122

## LISTA DE ABREVIATURAS

APP	<i>Application</i>
ADSL	<i>Asysmmetric Digital Subscriber Line</i>
ARPANET	<i>Advanced Research Projects Agency Network</i>
CPU	<i>Unidade Central de Processamento</i>
FTP	<i>File Transfer Protocol</i>
GPIv2	<i>General Public License version 2</i>
GTI	<i>Gerência de Tecnologia da Informação</i>
HD	<i>Hard Disk</i>
HTTP	<i>Hypertext Transfer Protocol</i>
ICMP	<i>Internet Control Message Protocol</i>
IF	<i>Instituto Federal</i>
IP	<i>Internet Protocol</i>
IPv4	<i>Internet Protocol version 4</i>
IPv6	<i>Internet Protocol version 6</i>
Mbps	<i>Megabits por segundo</i>
MIB	<i>Management Information Base</i>
OSI	<i>Open System Interconnection</i>
RAM	<i>Random Acess Memory</i>
RNP	<i>Rede Nacional de Pesquisa</i>
S.O.	<i>Sistema Operacional</i>
SMTP	<i>Simple Mail Transfer Protocol</i>
SNMP	<i>Simple Network Management Protocol</i>

TCP	<i>Transmission Control Protocol</i>
TI	<i>Tecnologia da Informação</i>
UDP	<i>User Datagram Protocol</i>
UEPB	<i>Universidade Estadual da Paraíba</i>
URL	<i>Uniform Resource Locator</i>
VLAN	<i>Virtual Local Área Network</i>

## SUMÁRIO

<b>1.</b>	<b>INTRODUÇÃO</b> .....	<b>16</b>
<b>2.</b>	<b>REVISÃO BIBLIOGRÁFICA</b> .....	<b>19</b>
<b>3.</b>	<b>GERENCIAMENTO DE REDE</b> .....	<b>23</b>
<b>4.</b>	<b>ARQUITETURA TCP/IP</b> .....	<b>24</b>
<b>5.</b>	<b>PROTOCOLO TCP</b> .....	<b>25</b>
<b>6.</b>	<b>PROTOCOLO UDP</b> .....	<b>26</b>
<b>7.</b>	<b>PROTOCOLO IP</b> .....	<b>27</b>
<b>8.</b>	<b>PROTOCOLO ICMP</b> .....	<b>28</b>
<b>9.</b>	<b>PROTOCOLO SNMP</b> .....	<b>29</b>
<b>10.</b>	<b>IF GOIANO - CAMPUS MORRINHOS</b> .....	<b>31</b>
<b>11.</b>	<b>A FERRAMENTA DE MONITORAÇÃO ZABBIX</b> .....	<b>33</b>
<b>12.</b>	<b>PARTE EXPERIMENTAL</b> .....	<b>34</b>
<b>13.</b>	<b>ESTRUTURA E APRESENTAÇÃO DOS DADOS</b> .....	<b>37</b>
	13.1. TEMPLATE SIMPLE CHECK ICMP.....	40
	13.2. TEMPLATE S.O.....	41
	13.3. TEMPLATES SNMP .....	42
	13.4. TEMPLATE SERVIÇO .....	44
	13.5. GRÁFICOS .....	47
	13.6. MAPAS .....	49
	13.7. AGRUPAMENTO DE GRÁFICOS .....	52
	13.8. APRESENTAÇÃO DE SLIDS .....	56
<b>14.</b>	<b>CONCLUSÃO</b> .....	<b>57</b>
<b>15.</b>	<b>REFERÊNCIAS</b> .....	<b>58</b>
<b>16.</b>	<b>APÊNDICE A - INSTALAÇÃO DO ZABBIXDB MYSQL</b> .....	<b>61</b>
	14.1. PREPARAÇÃO .....	61
	14.2. INSTALAR AS DEPENDÊNCIAS.....	62
	14.3. INSTALANDO O FPING .....	62
	14.4. REPOSITÓRIO OFICIAL ZABBIX.....	63

14.5.	REPOSITÓRIO OFICIAL MYSQL.....	64
14.6.	CRIANDO O SCHEMA MYSQL ZABBIX .....	66
14.7.	CONFIGURAÇÃO ZABBIX-AGENT.....	67
<b>15.</b>	<b>APÊNDICE B - ZABBIX SERVER.....</b>	<b>69</b>
15.1.	PREPARAÇÃO .....	69
15.2.	INSTALAR AS DEPENDÊNCIAS / REPOSITÓRIOS .....	70
15.3.	INSTALANDO O FPING .....	70
15.4.	INSTALANDO IKSEMEL.....	70
15.5.	Repositório Oficial Zabbix .....	71
15.6.	CONFIGURAÇÃO ZABBIX-SERVER .....	72
15.7.	CONFIGURAÇÃO ZABBIX-AGENT.....	73
15.8.	AJUSTANDO O FRONTEND DO ZABBIX.....	75
15.9.	SERVIÇOS HTTPD.....	76
15.10.	SERVIÇOS DE FIREWALL.....	76
15.11.	CONFIGURAÇÃO NO NAVEGADOR.....	77
<b>16.</b>	<b>APÊNDICE C - INSTALAÇÃO E CONFIGURAÇÃO ZABBIX PROXY</b>	<b>84</b>
16.1.	CONFIGURAÇÃO PROXY AGENTD.CONF .....	86
16.2.	CONFIGURAÇÃO PROXY SERVER.CONF.....	87
16.3.	CRIAÇÃO DO PROXY NO FRONTEND.....	91
16.4.	INSTALAÇÃO DO SEGUNDO SERVIDOR PROXY.....	94
<b>17.</b>	<b>APÊNDICE D - SISTEMAS DE ALERTA VIA E-MAIL E WHATSAPP</b>	<b>95</b>
17.1.	SISTEMA DE ALERTA VIA E-MAIL.....	96
17.2.	CONFIGURAR O POSTFIX.....	96
17.3.	CONFIGURAÇÃO DO E-MAIL NO FRONTEND DO ZABBIX	99
17.4.	CONFIGURAÇÃO DO SISTEMA DE ALERTA VIA WHATSAPP	

17.5. CRIAÇÃO DE UM USUÁRIO PARA NOTIFICAÇÃO DO  
WHATSAPP 112

**18. APÊNDICE E - INSTALAÇÃO DO ZABBIX AGENT EM HOST  
WINDOWS 117**

18.1. CRIAÇÃO DOS GRUPOS DE HOSTS ..... 120

18.2. CRIAÇÃO DOS HOSTS WINDOWS NO FRONTEND ..... 121

## 1. INTRODUÇÃO

Após a criação dos computadores e sua utilização para o gerenciamento de informações surgiu a necessidade de comunicação entre eles, de modo a descentralizar as informações e compartilhar os recursos de forma eficiente. Assim, surgiram as redes de computadores, responsáveis pela troca de informações entre dispositivos.

Segundo Sousa (2005, p. 37) uma rede de computadores é um conjunto de equipamentos interligados de maneira a trocarem informações e compartilhem recursos, como arquivos de dados gravados, impressoras, modems, softwares, e outros equipamentos.

Pode-se observar o grande crescimento das redes de computadores, pois no início ligava, universidades e grandes corporações, todavia, desde meados da década de 80 passou a conectar todo o globo, ou seja, essa rede se expandiu de tal forma que é possível conectar à rede através de computadores, notebooks, smartphones, tablets, smartwatches, televisores, veículos, e dessa forma surgiu a internet.

Com esse grande crescimento da quantidade de redes se comunicando, surgiu uma estrutura muito complexa, fazendo com que os problemas que eram encontrados anteriormente e resolvidos com pequenos passos se tornassem complexos.

De acordo com Comer (2007, p. 34), a complexidade da Internet é tão grande por conta das diversas tecnologias de diversas empresas no mercado, que criam seus produtos com características específicas, dificultando a padronização ou referência a uma determinada tecnologia que pode ser interpretada erroneamente, fazendo com que os inexperientes na área tenham dificuldade.

Para tanto, na tentativa de evitar problemas ou corrigir os mesmos e garantir a qualidade da estrutura da rede existe o administrador de rede.

O administrador de rede é a pessoa responsável pela monitoração e controle dos sistemas de hardware e software que compreendem uma inter-rede. Um administrador trabalha para detectar e corrigir problemas que tornam a comunicação ineficiente ou impossível e eliminar as condições que produzirão o problema novamente. Porque falhas de hardware e de software podem causar problemas, mas, um administrador de rede deve monitorá-las. (Comer, 2007, p. 539).

É necessária uma ferramenta capaz de monitorar e apresentar ao administrador de rede o status de sua estrutura, auxiliando a gerência de seu trabalho.

Segundo Comer (2007, p. 540), o software de gerenciamento de rede irá permitir que o administrador da rede monitore a comunicação dos dispositivos de rede, como hosts, roteadores e switches, de forma a identificar seus status e obter estatísticas sobre os mesmos.

A Figura 1 apresenta o diagrama de funcionamento de um sistema de gerenciamento de rede. Esses sistemas funcionam em três partes, em sua primeira, há uma coleta de informações dos dispositivos gerenciados, na segunda etapa ocorre a análise dessas informações, verificando a atividade e o que está ocorrendo em cada dispositivo, possibilitando a análise na busca de alguma anormalidade ou problema, e na terceira etapa dispara alertas ou realiza uma tarefa pré-configurada, possibilitando à gerência agir com base nas informações coletadas e no histórico de problemas anteriormente ocorridos. Déo; Pires (2010, p.69).



Figura 1 Funcionamento de um sistema de gerenciamento de rede

Fonte: Revista Espírito Livre, 2010. P.70

### Objetivo geral:

- Implantar uma ferramenta de monitoramento de tráfego e ativos de rede, *open source*, no Instituto Federal Goiano-Campus Morrinhos, para detectar problemas de forma mais eficaz e encontrar soluções mais rapidamente evitando que a estrutura fique indisponível por determinado momento.

**Objetivos específicos:**

- Implantar a ferramenta *open source* Zabbix para o monitoramento de tráfego e ativos de rede;

Zabbix é uma ferramenta moderna. *Open Source* e multiplataforma, livre de custos de licenciamento, pois sua licença é a GPLv2 (*GNU General Public License*), utilizada para monitorar a disponibilidade e o desempenho de aplicações, ativos e serviços de rede por todo o mundo. Spínola Horst et. Al, p.19 (2015).

- Implantar dois servidores contendo o Zabbix Proxy, responsáveis por realizar a coleta de toda a informação de tráfego de rede e controle de ativos, conseqüentemente ocorrerá a distribuição da carga entre as redes corporativas e livre;
- Criar Scripts para automatizar tarefas de gerência de redes;
- Monitorar a banda da rede em seguimentos estruturados com o IPv6 "*Internet Protocol Version 6*", o IPv4 "*Internet Protocol Version 4*";
- Monitorar ativos da rede, dentre eles câmeras, roteadores e serviços WEB.

## 2. REVISÃO BIBLIOGRÁFICA

Moraes (2008) apresenta o estudo da base de informações de gerenciamento MIB "*Management Information Base*" e a arquitetura do protocolo SNMP "*Simple Network Management Protocol*", utilizando a ferramenta Zabbix na versão 1.4.5 para a implantação em um ambiente de testes.

Possui o objetivo de coletar informações de tráfego dos enlaces de dados em redes Ethernet entre um modem ADSL "*Asymmetric Digital Subscriber Line*" e uma máquina virtual e calcular a taxa de bits trafegadas entre esse enlace.

Com uma limitação de hardware para montar sua estrutura de estudo, o autor utilizou a tecnologia do VmWare para virtualizar um host e fazer o gerenciamento da rede. Foram feitos quatro estágios de testes, onde alterava-se a velocidade da interface dos hosts para verificar o que era coletado pelo Zabbix e calcular a quantidade de bits trafegados pelos enlaces.

Conclui-se que através de uma ferramenta automatizada, como Zabbix, é possível aplicar o gerenciamento de rede e obter maior controle sobre os tráfegos dos enlaces, podendo evitar lentidão em toda rede.

O estudo realizado por Fachini; Timm (2010) apresenta a implantação do Zabbix na versão 1.8.3 em um ambiente corporativo e demonstra a utilização da ferramenta na automatização de recuperação de serviços.

Demonstra a necessidade de a corporação utilizar uma outra ferramenta de monitoramento que facilite mais seu controle interno e externo, visto que outras ferramentas utilizadas pela empresa mostram falhas em alguns aspectos, como a descentralização e no envio de alertas.

Como proposta, o autor utilizou um dos pontos fortes da ferramenta, que é a utilização de templates, para configurar apenas um parâmetro e aplicar a diversos hosts de forma simultânea. Assim o autor pôde capturar informações sobre seus hosts e criar ações quando a ferramenta analisasse os dados coletados, podendo automatizar tarefas.

Conclui-se que foi realmente eficaz a utilização do Zabbix, pois apresentou total integração com seu ambiente, facilitando o gerenciamento de recursos e possibilitando a automatização de tarefas, gerando maior rapidez na solução de problemas.

Andrey (2011), apresenta a utilização de um software livre, para realizar o monitoramento de rede e servidores, monitorar alguns serviços através da utilização do Zabbix Proxy na sua versão 1.8.8, e com seus agentes gerar relatório dos dados coletados.

Em seus testes o autor avalia a solução na forma que ocorrem as medições, o envio e apresentação dos alarmes e a forma que são apresentados os dados coletados. Como infraestrutura, o autor dispôs de um ambiente real sediado por uma empresa, assim seu período de coleta foi durante o período comercial, das 8 às 18 horas. Os dados coletados durante esse período foram os mesmos utilizados para os testes de mostra de dados. Através de simulações foram feitos testes de como a ferramenta se comporta no envio de alerta e na execução de ações na tentativa de resolução de erro de forma autônoma.

Apesar de observar complexidade na criação de triggers para o disparo de alertas, devido a forma de criação das expressões O autor conclui que a ferramenta apresenta o processo de configuração de forma fácil, possui alto desempenho na apresentação dos dados coletados, e agilidade no disparo de alertas quando um problema é detectado. Possui diversas funções e serviços que possibilitam o monitoramento ativo ou passivo de diversos dispositivos.

De acordo Ernando (2013), o grande avanço da necessidade das redes de computadores ampliou a quantidade de problemas encontrados, como indisponibilidade de aplicação e indisponibilidade de capacidade de servidores. Assim, gerando a necessidade de um monitoramento em tempo real de toda estrutura de serviço e hardware, de modo a obter informações confiáveis para facilitar a tomada de decisões no momento de planejamento da estrutura de rede.

Com isso o autor apresenta uma arquitetura baseada em um modelo gerente – agente, utilizando o Zabbix, uma ferramenta com vasto suporte de instalação a diversos sistemas operacionais e com diversas formas de notificações de alertas. Afim de conhecer a ferramenta, utilizou o “Zabbix server” como central de monitoramento e “Zabbix agente” nos servidores e o protocolo SNMP nos equipamentos a serem monitorados.

Após a implantação do Zabbix no campus Capivari, o autor descreve a importância de uma ferramenta eficiente de monitoramento. Com a implantação do Zabbix ele encontrou benefícios na automatização de processos realizados nas

impressoras, reduzindo a atenção de suporte técnico por parte da equipe de TI. A facilidade de diagnosticar e identificar problemas com os backups realizados dos servidores virtuais facilitou para a equipe gerenciar melhor o espaço visto que é uma limitação da estrutura, facilitando também o estudo de aquisição para a ampliação dos equipamentos de armazenamento.

Eder (2013) apresenta uma ferramenta gratuita capaz de gerenciar redes que trabalham com IPV6 e pode ser implantada com baixo custo utilizando o raspberry. Com propósito, o trabalho analisa o desempenho em um pequeno ambiente de estudo, utilizando o computador raspberry e o Zabbix em sua versão 2.2.1 como servidor, e monitorar recursos de hardware de outras máquinas utilizando os protocolos IPv4 e IPv6.

Após a análise de diversos cenários foram detectados problemas com o banco de dados utilizado e houve a necessidade da troca do mesmo. O Zabbix se apresentou eficiente e robusto, apesar de apresentar pequena lentidão no acesso da interface web ocasionada pelo baixo recurso de hardware do raspberry. Foi comprovado que para ambientes de teste e redes de pequeno porte é possível implantar uma ferramenta poderosa e com baixo custo.

O estudo realizado por Vieira (2014), aborda o conceito de gerenciamento de rede implantando a ferramenta Zabbix, com monitoramento através do protocolo de gerenciamento SNMP, tendo como caso de uso o Instituto Federal Goiano-Campus Urutaí. De acordo com a necessidade da instituição que foi utilizada como estudo de caso, há uma vasta gama de equipamentos e serviços a serem monitorados. O ambiente, possui ferramentas que monitoram e gerenciam alguns recursos, porém mostram falhas em alguns aspectos. Dessa forma, não obtendo o controle e gerenciamento de toda sua estrutura. Foi utilizado a ferramenta de monitoramento Zabbix afim de obter um melhor gerenciamento de todos os serviços e ativos das redes que o Campus dispõe.

Toda a problemática foi solucionada com a ferramenta, essa que se encontra em utilização com alto grau de adaptação ao ambiente, tornando positivo sua implantação.

O trabalho apresentado por Batista (2014), apresenta a importância de um sistema de gerenciamento de redes e utiliza o Zabbix como ferramenta de monitoramento baseado em uma arquitetura centralizada. Apresentou como objetivo implantar uma solução open-source na rede da UEPB “*Universidade Estadual da Paraíba*”, Campus VII e estruturar a ferramenta para realizar a coleta de dados da infraestrutura do Campus e apresentar de forma funcional.

Utilizando o Zabbix, criou um mapa de sua estrutura monitorada, apresentando a topologia e os hosts e ativos que estavam sendo monitorados, conseguindo coletar a utilização de CPU “*Unidade Central de Processamento*”, tráfego de entrada e saída das interfaces de rede dos dispositivos monitorados, analisar o tempo de resposta e se há gargalo na rede ou se o tráfego está em níveis aceitáveis.

Concluiu-se que com o Zabbix o administrador da rede poderia planejar melhor a expansão de sua estrutura, verificar a demanda de recursos pelos usuários e resolver os problemas em um tempo mais hábil.

O trabalho apresentado por Sateles (2015), contempla o estudo de caso do software gratuito de monitoramento de rede, Zabbix em sua versão 2.4, buscando a avaliação de recursos, flexibilidade e apresentação dos dados capturados pela ferramenta. Seu ambiente de testes, composto por apenas três máquinas virtuais, dentre uma servidora e duas clientes, serviu de estrutura para coletar informações da utilização de hardware utilizado pelas mesmas e testar o sistema de alerta via e-mail que a ferramenta oferece. Com esses dados coletados, a autora pôde verificar a forma de apresentação das informações pela ferramenta e seus relatórios.

### 3. GERENCIAMENTO DE REDE

De acordo com Luiz (2012) gerenciamento de rede “É um conjunto de ferramentas, procedimentos, técnicas e políticas usadas para manter a eficiência e o funcionamento de uma rede de computadores. Independentemente de seu tamanho.”

A gerência de redes é responsável por garantir que tudo funcione corretamente, que a informação esteja sempre disponível ao cliente. Esses resultados são obtidos através de monitoramento, gerenciamento, detecção e correção de falhas, análise das informações dos componentes e serviços que compõem a rede.

Segundo Elaine; Aguiar (2006), existem no mercado alguns guias de controle de gestão como Cobit. E trazem como proposta grupos de controles divididos das seguintes formas: Gerência de desempenho, gerência de falhas, gerência de configuração e documentação, gerência de problemas e incidentes e gerenciamento de logs. A seguir apresenta-se uma breve descrição dessas gerências:

- Gerenciamento de desempenho: tem como funções quantificar, apresentar uma forma de medir e apresentar o desempenho. Como exemplo um gráfico que apresente a taxa de download e upload de um link. O protocolo SNMP tem um importante papel para o gerenciamento de desempenho. KUROSE; ROSS p.557 (2013);
- Gerenciamento de falha: tem como funções detectar, registrar e reagir às falhas de rede. Não possui uma divisão tão definida em relação ao gerenciamento de desempenho, que trata de interrupção de serviços em enlaces, hosts, hardware e software. O gerenciamento de falha apresenta a relação de longo prazo do desempenho da rede. O SNMP “*Simple Network Management Protocol*”, também é importante para esse gerenciamento. KUROSE; ROSS p.557 (2013);
- Gerenciamento de configuração: responsável pelo controle de versões dos elementos de hardware e software na rede, verificando o modo de operação dos dispositivos e suas conexões. Pode ser dividida em três categorias: inventário, configuração e provisão. Luiz p.27 (2012);
- Gerência de contabilização: planeja a forma de crescimento da rede e gerencia a utilização de todos os meios e recursos disponíveis. Luiz p.29 (2012);
- Gerenciamento de segurança: planeja a forma de acesso aos recursos da rede de forma a garantir a integridade de todas as informações, gerenciar os acessos

conforme as definições de cada organização, além disso, pretende proteger as informações, controlar o acesso aos sistemas, monitorar a utilização de recursos, e analisar arquivos de log. Luiz p.29 (2012).

#### 4. ARQUITETURA TCP/IP

Segundo Tanenbaum p.28 (2011), o modelo de referência TCP/IP “*Transmission Control Protocol*”, “*Internet Protocol*”, surgiu logo após a criação da ARPANET, que foi uma rede de pesquisa criada pelo departamento de defesa dos Estados Unidos. Com o passar do tempo, empresas públicas e universidades passaram a fazer parte dessa rede, mais tarde incluiu-se as redes de rádio e satélite, e assim os protocolos existentes começaram a ter problemas na intercomunicação, surgindo a necessidade de uma outra referência de gerenciamento.

Em comparação ao modelo de referência OSI “*Open System Interconnection*”, o TCP/IP não possui as camadas de apresentação, sessão e física, tendo apenas as camadas de aplicação, transporte, Internet e enlace. A Figura 2 apresenta a diferença entre o modelo de referência OSI e a arquitetura TCP/IP. A Tabela 1 apresenta uma breve descrição da arquitetura TCP/IP.

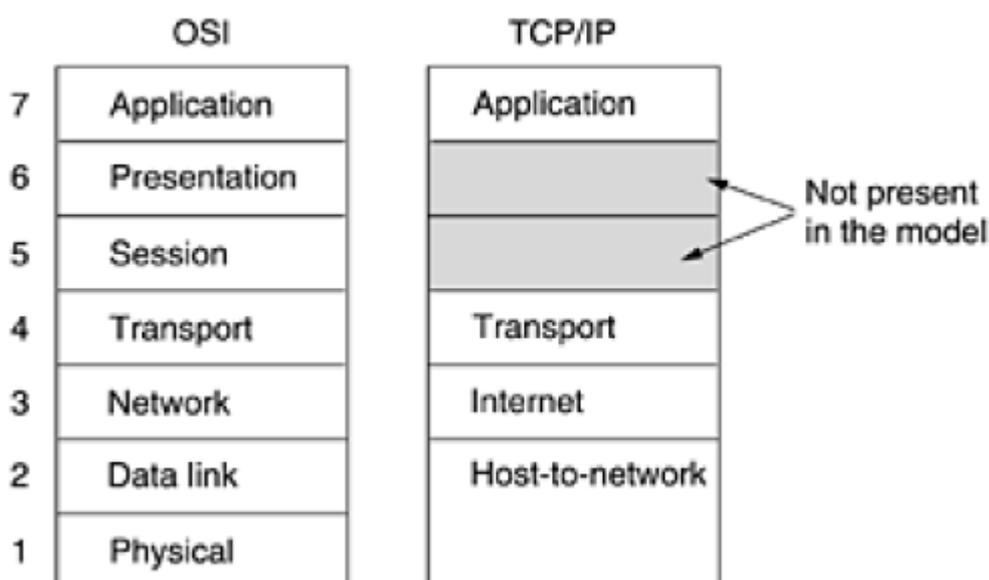


Figura 2 Modelo de Referência OSI e TCP/IP

Fonte: Tanenbaum 2011

## 5. PROTOCOLO TCP

O protocolo TCP é orientado a conexão porque antes da aplicação realizar o envio de um dado a outro os processos precisam estabelecer a conexão entre si, se “apresentar”. A conexão com o TCP é sempre ponto a ponto, entre um remetente e um único destinatário. Se houver uma conexão TCP entre dois processos, os dados poderão fluir em ambos os sentidos. KUROSE; ROSS p.169 (2013);

Segundo Tanenbaum p.410 (2011), o protocolo TCP estabelece suas conexões através de três vias do *handshake*, entre os hosts onde eles se identificam e confirmam que estão prontos para iniciar a transferência de dados. Para efetuar o processo de comunicação um dos hosts aguardam uma conexão de entrada executando as primitivas *LISTEN* e *ACCEPT*, o outro host executa uma primitiva *CONNECT* informando o IP *Internet Protocol* e a porta que irá conectar, o tamanho do seguimento TCP e opcionalmente algum dado como por exemplo uma senha. A primitiva *CONNECT* envia um segmento TCP com o bit *SYN* ativado e um bit *ACK* desativado e fica aguardando resposta.

Quando chega no host de destino, o TCP desta estação verifica se existe um processo de primitiva *LISTEN* em execução na porta informada no campo de porta de destino, se não existir ele retorna uma resposta com bit *RST* ativado para rejeitar a conexão. Se existir algum processo o segmento TCP de entrada será recebido, assim poderá aceitar ou rejeitar a conexão, se for aceito é enviado ao outro host um segmento de confirmação, Tanenbaum p.410 (2011).

## 6. PROTOCOLO UDP

“Assim como o IP, o protocolo UDP *“User Datagram Protocol”*, também é um protocolo não confiável e não orientado à conexão” Torres. p.33 (2013).

O protocolo UDP permite maior flexibilidade ao programador, porém maior complexidade de programação. Na sua transmissão, o protocolo solicita uma porta ao sistema operacional, após, identifica o IP do destinatário e envia o pacote, sem haver nenhuma conexão prévia entre os hosts. Caso não localizar a máquina de destino é gerado uma mensagem IMP de porta não atingida. Torres. p.33 (2013).

O UDP definido na RFC 768, faz pouco do que um protocolo de transporte pode fazer. Sua multiplexação e demultiplexação não apresenta nenhuma verificação de erros simples e não adiciona nada ao datagrama IP. Se algum desenvolvedor optar por utilizar o UDP como protocolo de transporte, a aplicação estará comunicando quase diretamente com o protocolo IP, pois o UDP pega as informações da camada de aplicação, acrescenta o número da porta de origem e de destino para o serviço de multiplexação e demultiplexação e encapsula em um datagrama IP e realiza a entrega do segmento ao receptor. KUROSE; ROSS p.169 (2013).

Segundo Tanenbaum p.400(2011), o protocolo UDP encapsula segmentos com cabeçalhos de tamanho de 8 bytes seguidos por sua carga útil, duas pontas responsáveis por identificar o host de origem e destino. Quando o segmento UDP chega ao destino, sua carga útil é entregue à porta de destino. O UDP tem valor a mais que o IP de forma bruta pois ele possui os campos de porta de origem e destino, caso contrário a camada de transporte não saberia o que fazer com o pacote e graças a elas a camada consegue entrega-los corretamente. A Figura 3 apresenta o cabeçalho do protocolo UDP.

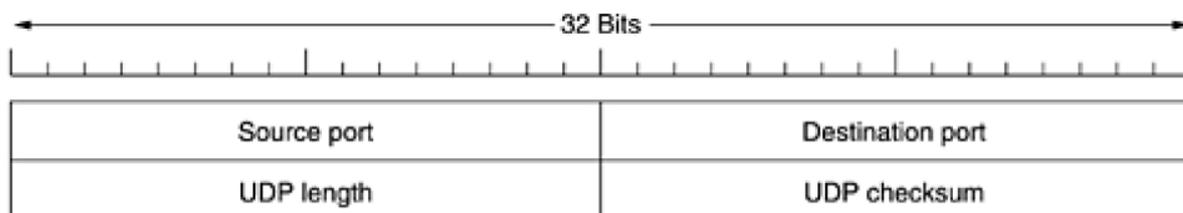


Figura 3 Cabeçalho UDP

Fonte: Tanenbaum p.400 (2011)

## 7. PROTOCOLO IP

“Na Internet, cada host e cada roteador tem um endereço IP que codifica seu número de rede e seu número de host. A combinação é exclusiva: em princípio, duas máquinas na Internet nunca tem o mesmo endereço IP”. Tanenbaum p.337 (2011).

Atualmente dispomos de duas versões deste protocolo a IPv4 e IPv6. A versão 4 do protocolo é composta por 32 bits, gerando no total de  $2^{32}$  de endereços IPs possíveis. Com cerca de 4 bilhões de endereços, que são escritos em notação decimal e separados por pontos, cada conjunto é composto de 8 bits. Como exemplo: 192.168.0.1. KUROSE; ROSS p.250 (2013).

Partindo do princípio que nenhum outro host na Internet pode ter o mesmo endereço IP que outro, e, com o avanço atual da tecnologia, esses endereços IPs disponíveis estão se tornando escassos, e dessa forma foi criado o IPV6, de forma a buscar a garantia que não haverá falta de IPs em algum futuro próximo.

O protocolo IPv6 não veio para substituir o IPv4 de uma hora para outra, mas trazer melhorias, principalmente no seu número de endereçamentos. Essa nova versão requisitará comutadores e hosts mais potentes, uma vez que seu modo de operar será diferente do anterior. O IPv6 aumentou seu tamanho, enquanto o IPv4 é composto por 32 bits, o IPv6 é composto por 128bits, aumentando exponencialmente o suporte hierárquico de endereçamentos e o número de hosts a serem endereçados. Naugle G. p.281 (1998).

Enquanto o IPv4 é composto por quatro conjuntos de 8 bits, o IPv6 é composto por oito conjunto de 16 bits, escritos em hexadecimal e separados por dois pontos. Como exemplo: 8000:0000:0000:0000:0123:4567:89AB:CDEF. Para facilitar sua escrita, visto que ele apresente muitos zeros, é autorizado sua representação em três formas:

- 8000::123:4567:89AB:CDEF: Os zeros que contém a esquerda podem ser omitidos permitindo ficar mais limpo o endereço como por exemplo em 123: .Tanenbaum p.360 (2011);
- Quando um grupo de 16 bits forem compostos por apenas zeros este pode ser representado apenas por (::) como no exemplo anterior. Tanenbaum p.360 (2011);

- ::192.31.20.46 : Podem ser representado também sendo escritos com um conjunto de dois pontos (::) e seguido do número decimal tradicional, como o exemplo acima. Tanenbaum p.360 (2011).

## 8. PROTOCOLO ICMP

O protocolo ICMP "*Internet Control Message Protocol*" é utilizado para comunicar informações da camada de rede entre hosts e computadores. Por exemplo quando é executado uma tentativa de acesso remoto utilizando o TELNET e há um erro com retorno "rede de destino inalcançável", quer dizer que a aplicação não conseguiu conectar ao destino, e em algum local na rede um roteador IP não conseguiu localizar o host final e retornou através do ICMP esta mensagem de erro. KUROSE; ROSS p.261 (2013).

Se não fosse o protocolo ICMP não seria possível utilizar o programa ping para realizar testes de conexão entre hosts, pois o ping envia um pacote ICMP do tipo 8 código 0, e o receptor ao receber responde um pacote ICMP do tipo 0 com código 0. O traceroute também é um programa que utiliza o protocolo para realizar o acompanhamento de rote entre dois hosts. KUROSE; ROSS p.261 (2013).

O protocolo ICMP possui alguns retornos de mensagens que possibilitam identificar algumas informações de um determinado host, como apresenta a Tabela 1.

Tabela 1 Tipos de Mensagem ICMP

Fonte: Tanbaum 2011

Tipo de mensagem	Descrição
Destination unreachable	Não foi possível entregar o pacote
Time exceeded	O campo Time to live chegou a 0
Parameter problem	Campo de cabeçalho inválido
Source quench	Pacote regulador <sup>9</sup> Redirect Ensina geografia a um roteador
Echo	Pergunta a uma máquina se ela está ativa
Echo reply	Sim, estou ativa
Timestamp request	Igual a Echo, mas com timbre de hora
Timestamp reply	Igual a Echo reply, mas com o timbre de hora

## 9. PROTOCOLO SNMP

Segundo Rodrigues (2005), o SNMP “*Simple Network Management Protocol*” é um protocolo de rede que utiliza serviços do protocolo UDP e é responsável por gerenciar, de forma simples, os equipamentos em uma rede.

“É o padrão mais popular para o protocolo de gerência de rede. É um padrão aberto adotado por vários fabricantes e operadoras, definindo o funcionamento da arquitetura de gerenciamento de redes TCP/IP”. Tapajos et al. p.72 (2015).

O protocolo SNMP tem suas interações sem conexão, utiliza os protocolos UDP/IP nas portas 161 e 162 e possui pacotes com tamanhos variáveis. Se tornou padrão para o gerenciamento da Internet, pois é simples sua implementação e amplamente difundido. Déo p.31 (2012).

Segundo Déo p.28 (2012), o gerente SNMP é o responsável por receber as informações coletadas do agente SNMP e através de aplicações gerar funcionalidades como criação de gráficos, armazenamento em banco de dados e disparar alertas. Os agentes SNMP são os dispositivos dos quais os dados serão coletados e enviados ao gerente, como apresenta a Figura 4.

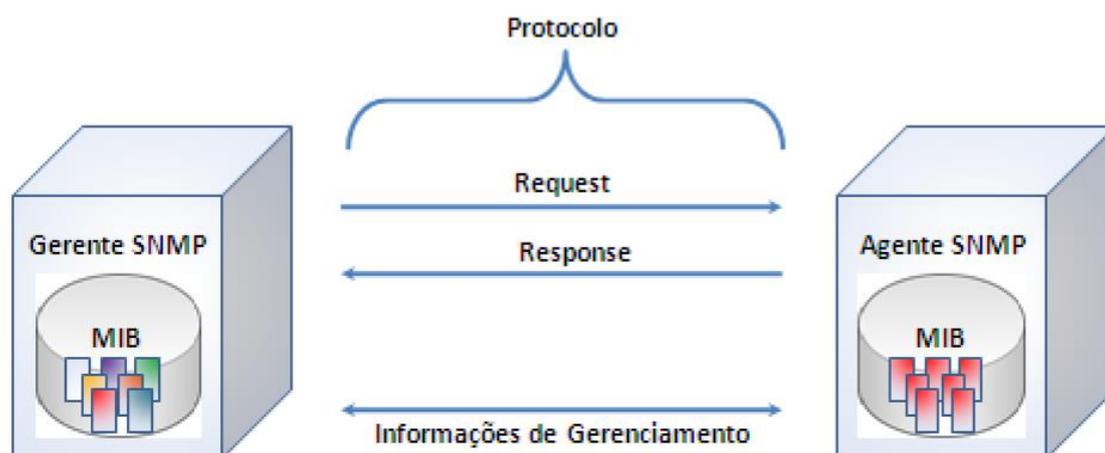


Figura 4 Componentes SNMP

Fonte: Déo p31(2012)

A MIB “*Management Information Base*” é uma base de informações gerenciadas que apresentam informações relevantes à gerência de redes, ela não possui objetos reais, apenas os organiza. Déo p.45 (2012).

O SNMP está em sua terceira versão, porém apenas equipamentos mais novos tem suporte a este protocolo. Ele passou por um processo de evolução ganhando algumas melhorias.

Versões:

- SNMPv1:
  - Padrão histórico IETF;
  - RFC 1157 de 1990;
  - Segurança baseada em comunicações;
  - Troca de informações baseada em textos simples.
- SNMPv2:
  - RFC Principais 3416, 3417, 3418;
  - Amplia as operações definidas na versão 1;
  - Unificação dos PDU (Protocol Data Unit);
  - Possui variantes.
- SNMPv3:
  - RFC 3410 à 3418 e 2576;
  - Avanço em segurança e privacidade.

## 10. IF GOIANO - CAMPUS MORRINHOS

Em atividade desde 1997, o IF Goiano – Campus Morrinhos é referência na região Sul de Goiás como instituição pública federal promotora de Educação Profissional, Científica e Tecnológica nas áreas de Ciências Agrárias, Alimentos, Pedagogia e Informática. (IF Goiano).

Atualmente a infraestrutura do IF Goiano Campus Morrinhos possui algumas obras em construção, outras em reforma, o que mostra a necessidade de um sistema de monitoramento de rede para gerir melhor os recursos de tecnologia da informação da instituição.

A instituição dispõe hoje de um link de 100Mbps fornecido pela *Rede Nacional de Ensino e Pesquisa*, que provê a integração global e a colaboração apoiada em tecnologias de informação e comunicação para a geração do conhecimento e a excelência da educação e da pesquisa, sustentando toda a rede administrativa e pública. O setor de TI possui um projeto de implantação que engloba a interligação guiada entre todos os departamentos através de fibra óptica, retirando de funcionamento o sistema de comunicação não guiado que atende os setores mais distantes com até dois quilômetros. Essa estrutura é apresentada na Figura 5.

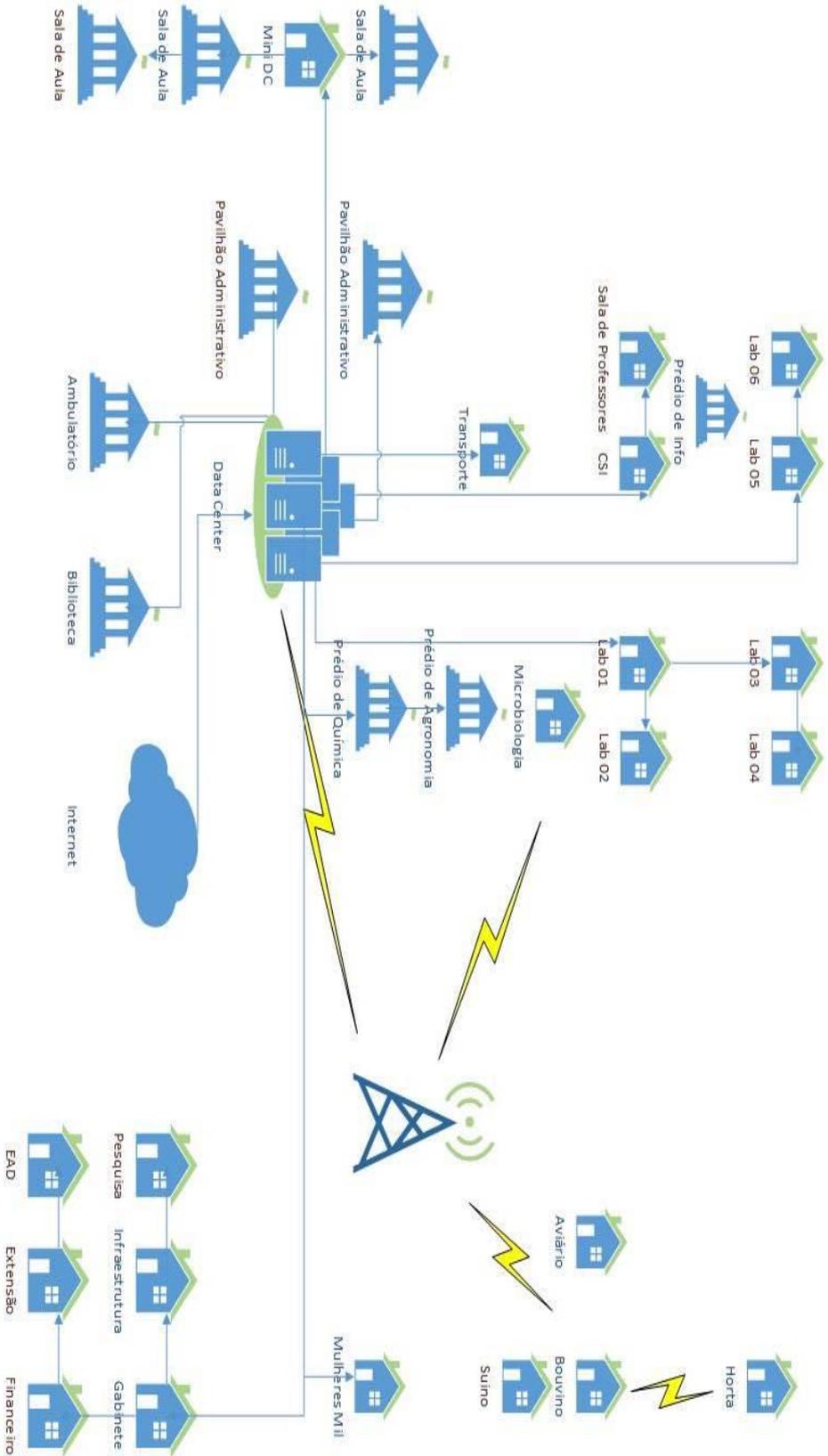


Figura 5 Infraestrutura do IF Goiano - Campus Morrinhos

## 11. A FERRAMENTA DE MONITORAÇÃO ZABBIX

O Zabbix foi criado por Alexei Vladishev em 2001, e atualmente é mantido e suportado pela Zabbix SIA. É uma solução de nível *enterprise*, de código aberto e com suporte a monitoração distribuída. Zabbix SIA. (2016).

O Zabbix é uma ferramenta de monitoramento de redes, servidores e serviços, pensada para monitorar a disponibilidade, experiência de usuário e qualidade de serviços. A arquitetura Zabbix e a flexibilidade dos módulos permitem que a ferramenta seja utilizada para o monitoramento convencional (vivo/morto - on/off), acompanhamento de desempenho de aplicações, análise de experiência de usuário e análise de causa raiz em ambientes complexos, através do servidor Zabbix e das regras de correlacionamento. 4LINUX. (2016).

O Zabbix possui como vantagem a facilidade de manipulação dos objetos, o que facilita o dia a dia do administrador de redes. Com ele é possível criar um item de um host que pode ser utilizado como modelo e replicado para outros hosts, de forma fácil, rápida e intuitiva, da mesma forma para gráficos. Zabbix Brasil. (2016).

Zabbix é uma solução de monitoração completa, que provê diversos recursos de monitoração em um único pacote.

Segundo ZABBIX BRASIL (2016), o Zabbix possui as seguintes funcionalidades:

- Suporte a maioria dos sistemas operacionais: Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, NetBSD, Mac OS X, Windows, entre outros;
- Monitora serviços como http, pop3, imap, ssh sem o uso de agentes;
- Suporte nativo ao protocolo SNMP;
- Interface de gerenciamento Web, de fácil utilização;
- Integração com banco de dados MySQL, Oracle, PostgreSQL ou SQLite;
- Geração de gráficos em tempo real;
- Fácil instalação e customização;
- Agentes disponíveis para diversas plataformas: Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, SCO-OpenServer, 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: e-mail, Jabber, SMS;
- Suporte a execução de scripts personalizados.

## 12. PARTE EXPERIMENTAL

Este capítulo apresenta a parte experimental do trabalho, como o processo de instalação, configuração e resultados obtidos a partir da ferramenta implantada.

Primeiramente, foi definido que todo ambiente seria implantado através da virtualização, que, segundo Carlos et. al (2014) “É o compartilhamento do hardware por um ou mais sistemas operacionais em um mesmo equipamento, funcionando em ambientes independentes e isolados, através de um software que permite a criação de máquinas virtuais”. Por conta da complexidade da infraestrutura da instituição, que utiliza diversas VLANs “*Virtual local área network*”, a qual consiste na segmentação de redes lógicas a partir de um único segmento de rede física, pois tem-se o controle e gerenciamento de toda sua infraestrutura, surgindo a necessidade de virtualizar diversas interfaces de rede para atender todas as redes que o Zabbix monitoraria. Também levando em consideração a praticidade do gerenciamento dos servidores e outras inúmeras vantagens que essa tecnologia possibilita.

Ao escolher o local de implantação da ferramenta, definiu-se o tipo de instalação, que seria apenas uma máquina virtual contendo o servidor Zabbix e o Banco de dados Mysql, que poderiam suprir as necessidades atuais do Campus Morrinhos. Em reunião com a (GTI Gerência de Tecnologia da Informação), definiu-se que seria implantado quatro servidores separados, onde um exerceria o papel do servidor principal (Zabbix Server), outro servidor contendo apenas o banco de dados (Mysql) e dois servidores Proxy (Zabbix Proxy) responsáveis pela coleta de dados de redes distintas.

Atualmente o data center do IF Goiano - Campus Morrinhos conta com a plataforma de virtualização Citrix XenServer que utiliza o *Hipervisor* do projeto Xen de código aberto, capaz de gerenciar plataformas tanto livre quanto proprietária. O Zabbix

possui agentes com compatibilidade com qualquer plataforma, porém seu servidor requer um sistema operacional livre.

A distribuição utilizada foi a Cent OS 7, que é uma distribuição livre enterprise derivada do red hat. A versão utilizada neste trabalho foi a versão 7.1.1503 core, versão mínima do sistema, pois assim é dispensado pacotes que não são necessários para o funcionamento deste projeto. Necessitando apenas de 1024MB de memória RAM e de 12GB de espaço em disco. É uma distribuição que requer poucos recursos, podendo variar da sua versão e pacotes a serem instalados.

Ela pode ser encontra através do link:

[http://mirror.nbtelecom.com.br/centos/7/isos/x86\\_64/CentOS-7-x86\\_64-Minimal-1503-01.iso](http://mirror.nbtelecom.com.br/centos/7/isos/x86_64/CentOS-7-x86_64-Minimal-1503-01.iso)

A versão do Zabbix utilizada foi a 2.4.6. O Zabbix não requer tanto poderio de hardware, segundo Pinheiro. (2011), apenas 128MB de memória RAM, 256MB de espaço em disco são suficientes para colocar o Zabbix em funcionamento, e a quantidade de processador pode variar conforme a quantidade de requisição e qual banco de dados será utilizado. Tendo como exemplo a Tabela 2:

*Tabela 2 Requisitos de Hardware do Zabbix  
Fonte: Ricardo Pinheiro*

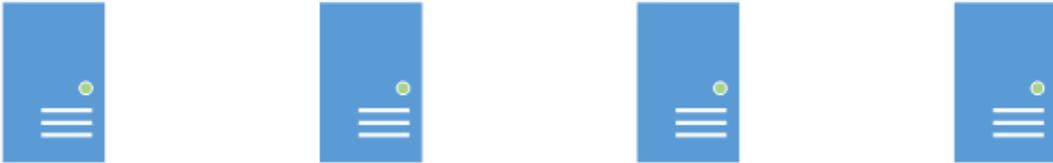
*Disponível em <http://www.cooperati.com.br/2011/10/04/monitoramento-de-servidores-com-Zabbix/>*

<b>Tipo</b>	<b>Plataforma</b>	<b>CPU/Memoria</b>	<b>Base de Dados</b>	<b>Hosts Monitorados</b>
Pequeno	Ubuntu 64	PII 350MHz 256MB	MySQL MyISAM	20
Medio	Ubuntu 64	Athlon 3200+ 2GB	MySQL InnoDB	500
Grande	Ubuntu 64	Intel Dual Core 6400 4GB	RAID10 MySQL InnoDB ou PostgreSQL	>1000
Enorme	RedHat Enterprise	Intel Xeon 2xCPU 8GB	Fast RAID10 MySQL InnoDB ou PostgreSQL	>10000

O Zabbix em si, seja o Server, Agent ou Proxy possuem dois métodos de instalação, via source, que é a compilação dos códigos fontes e via pacotes. Optou-se pela instalação via pacotes, por diminuir a quantidade de movimentação de arquivos dentro do sistema.

O banco de dados Mysql Server foi utilizado em sua versão 5.6.26, escolhido por ter um bom desempenho com o Zabbix e seu processo fácil de instalação e utilização. Optou-se por utilizar o banco em um servidor separado na busca de obter maior desempenho do serviço e manter a integridade das informações caso haja algum problema com o Zabbix Server, assim, se necessário, realizar a reinstalação do server sem o risco de perda de informações.

Foram alocados recursos bem acima do mínimo requerido, para que possa atender todas as necessidades do Cent OS, Mysql, Zabbix Proxy e Server, recursos esses, capaz de atender até mesmo uma grande quantidade de requisições de cada aplicação, podendo manter a qualidade do serviço conforme a expansão da infraestrutura. Abaixo na Figura 5, apresenta cada servidor virtualizado e o hardware alocado a eles.



<b>Zabbix Server</b> Processador: 4 Núcleos Memória Ram: 4GB HD: 50Gb	<b>Zabbix Mysql</b> Processador: 4 Núcleos Memória Ram: 3GB HD: 100GB	<b>Zabbix Proxy I</b> Processador: 4 Núcleos Memória Ram: 3Gb HD: 30GB	<b>Zabbix Proxy II</b> Processador: 4 Núcleos Memória Ram: 3Gb HD: 30GB
--	--	---	--

*Figura 5 Distribuição de Hardwares para os Servidores*

Por questões de segurança todo endereçamento IP presente neste trabalho não corresponde com a atual estrutura do Campus afim de preservar a integridade de sua estrutura de rede.

A Figura 6 apresenta as interfaces de rede de cada servidor e seus respectivos endereços IP que serão necessários para o acesso e configuração dos serviços. Todos os servidores necessitam estar conectados à Internet, para efetuar os downloads e atualizações necessárias e comunicando entre si para poderem realizar a troca de informações coletadas e armazenadas nos bancos de dados.

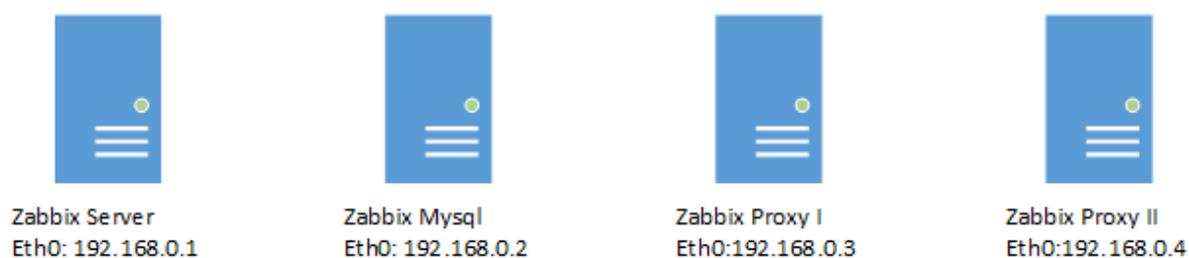


Figura 6 Interfaces de rede e respectivos endereços IPs

Todo o processo de instalação, configuração do Zabbix Server, Zabbix Mysql, Zabbix Proxy I, Zabbix Proxy II e os recursos de envio de alerta via whatsapp e e-mail serão apresentados detalhadamente no apêndice no final deste trabalho.

### 13. ESTRUTURA E APRESENTAÇÃO DOS DADOS

Este capítulo apresenta o processo realizado para executar o monitoramento das informações desejadas, e como elas foram organizadas para a melhor apresentação e gerenciamento.

Após os servidores instalados, configurados juntamente com os agentes, foi realizado o processo de criação e adaptação dos *templates* responsáveis por coletar as informações que eram necessárias para o monitoramento, não priorizando a criação dos hosts, evitando criar o esquema de monitoração da forma mais cara, em gasto de tempo e de gerenciamento, conforme apresenta Spínola Horst et. Al. p.87 (2015).

Para a execução deste trabalho foram utilizados 16 templates, dentre eles alguns padrões do Zabbix e outros criados para melhor atender as necessidades do projeto.

É possível acessar o menu de template em Configuração > Templates. Por padrão, o Zabbix traz diversos templates que já são aptos a realizar as coletas, necessitando vincular apenas o host desejado. É possível criar novos templates, tal como importar, exportar e editar. Para a proposta deste trabalho houve a necessidade de criação e edição de alguns templates padrões. Abaixo na Figura 7 é apresentado alguns dos templates utilizados.

Templates ↑	Aplicações	Itens	Triggers	Gráficos	Telas	Autobusca	Web	Associado aos templates
001-Disponibilidade via ICMP Cameras	Aplicações (1)	Itens (1)	Triggers (1)	Gráficos (0)	Telas (0)	Autobusca (0)	Web (0)	-
002-Monitoracao WEB	Aplicações (1)	Itens (0)	Triggers (2)	Gráficos (0)	Telas (0)	Autobusca (0)	Web (2)	-
003-Disponibilidade via ICMP Telefonia	Aplicações (1)	Itens (1)	Triggers (1)	Gráficos (0)	Telas (0)	Autobusca (0)	Web (0)	-
004-Template App MySQL	Aplicações (1)	Itens (14)	Triggers (1)	Gráficos (2)	Telas (1)	Autobusca (0)	Web (0)	-
005-Template App Zabbix Proxy	Aplicações (1)	Itens (21)	Triggers (19)	Gráficos (4)	Telas (1)	Autobusca (0)	Web (0)	-
006-Template App Zabbix Server	Aplicações (1)	Itens (30)	Triggers (26)	Gráficos (5)	Telas (1)	Autobusca (0)	Web (0)	-
007-Template OS Linux	Aplicações (10)	Itens (32)	Triggers (15)	Gráficos (5)	Telas (1)	Autobusca (2)	Web (0)	Template App Zabbix Agent
008-Template OS Windows	Aplicações (9)	Itens (18)	Triggers (9)	Gráficos (2)	Telas (1)	Autobusca (2)	Web (0)	Template App Zabbix Agent
009-Template SNMP Device SNMPv1	Aplicações (2)	Itens (6)	Triggers (1)	Gráficos (0)	Telas (0)	Autobusca (1)	Web (0)	010-Template SNMP Generic SNMPv1, 011-Template SNMP Interfaces SNMPv1
010-Template SNMP Generic SNMPv1	Aplicações (1)	Itens (5)	Triggers (0)	Gráficos (0)	Telas (0)	Autobusca (0)	Web (0)	-
011-Template SNMP Interfaces SNMPv1	Aplicações (1)	Itens (1)	Triggers (0)	Gráficos (0)	Telas (0)	Autobusca (1)	Web (0)	-
012-Template SNMP Device SNMPv2	Aplicações (2)	Itens (6)	Triggers (1)	Gráficos (0)	Telas (0)	Autobusca (1)	Web (0)	013-Template SNMP Generic SNMPv2, 014-Template SNMP Interfaces SNMPv2
013-Template SNMP Generic SNMPv2	Aplicações (1)	Itens (5)	Triggers (0)	Gráficos (0)	Telas (0)	Autobusca (0)	Web (0)	-
014-Template SNMP Interfaces SNMPv2	Aplicações (1)	Itens (1)	Triggers (0)	Gráficos (0)	Telas (0)	Autobusca (1)	Web (0)	-
015-Disponibilidade via ICMP Switch	Aplicações (1)	Itens (1)	Triggers (1)	Gráficos (0)	Telas (0)	Autobusca (0)	Web (0)	-
016-Disponibilidade via ICMP Nano Station	Aplicações (1)	Itens (1)	Triggers (1)	Gráficos (0)	Telas (0)	Autobusca (0)	Web (0)	-

Figura 7 Templates Utilizados

Os templates são estruturados através de alguns componentes como pode ser observado na Figura 8.

Templates ↑	Aplicações	Itens	Triggers	Gráficos	Telas	Autobusca	Web	Associado aos templates	Associado a
001-Disponibilidade via ICMP Cameras	Aplicações (1)	Itens (1)	Triggers (1)	Gráficos (0)	Telas (0)	Autobusca (0)	Web (0)	-	Adm_Corredor_Esino; Adm_Corredor_GAE; Adm_Corredor_Secretaria; Adm_Corredor_TI; Adm_Entrada_01; Adm_Entrada_02; Adm_Sitoficado_01; Camara_Biblioteca_Esterna; Camara_Centro_Convivencia; Camara_Corredor_Alimentos_Interno; Camara_Datocentro; Camara_Estacionamento; Camara_GAE; Corredor_Verde_direito; Server_Camara; Storage_Camara_01; Storage_Camara_02; Ultimo_Pavilhao_Corredor_Verde_Quimica; ZabbixProxyCamara

Figura 8 Componentes dos Templates

- **Template:** o nome de identificação do *template* e o vínculo com outros *templates* são configurados nesse componente. Para este trabalho foi acrescentado uma numeração ao nome dos *templates* utilizados, para melhor organização e visualização dos mesmos;
- **Aplicações:** componente responsável por realizar o agrupamento de vários itens;
- **Itens:** responsável por agrupar os itens cadastrados, que são os dados que realizam o monitoramento das informações;
- **Triggers:** são os alertas condicionais que serão informados quando um item estiver em um valor predeterminado;
- **Gráficos:** armazenam os gráficos que apresentam as informações coletadas pelos itens;

- Telas: é possível criar um conjunto de gráficos em uma única tela, facilitando a apresentação das informações;
- Auto busca: permite criar um sistema que realizará uma consulta de determinadas informações nos hosts vinculados;
- *Web*: permite criar um sistema de monitoramento web;
- Associado aos *templates*: é possível criar *templates* que podem coletar informações específicas e através de um vínculo ter a apresentação dessas informações mesmo que elas não estejam no mesmo *template*;
- Associado a: apresenta os hosts que fazem parte deste *template*.

Para uma melhor visualização os *templates* foram categorizados pelo seu tipo, como pode ser visto na Tabela 3.

Tabela 3 Tabela de Templates Utilizados

<b>ICMP</b>	<b>S.O.</b>	<b>SNMP</b>	<b>SERVIÇO</b>
001-Disponibilidade via ICMP Cameras	007-Template OS Linux	009-Template SNMP Device SNMPv1	002-Monitoracao WEB
003-Disponibilidade via ICMP Telefonia	008-Template OS Windows	010-Template SNMP Generic SNMPv1	004-Template App MySQL
15-Disponibilidade via ICMP Switch		011-Template SNMP Interfaces SNMPv1	005-Template App Zabbix Proxy
016-Disponibilidade via ICMP Nanostation		012-Template SNMP Device SNMPv2	006-Template App Zabbix Server
		013-Template SNMP Generic SNMPv2	
		014-Template SNMP Interfaces SNMPv2	

### 13.1. TEMPLATE SIMPLE CHECK ICMP

Esse template foi criado e replicado para os grupos de Câmeras, Telefonia, Switchs e Nanostation. O template contempla uma aplicação que é vinculada a um item, conta com os parâmetros do monitoramento do tipo simples, é utilizada uma chave no valor (icmpping[,,60,]) que irá enviar pacotes de 60 bytes e verificar se o valor de resposta será: 0 = quando não houver e 1: = quando houver. Caso não haja resposta o template possui uma trigger que será acionada através da expressão (`{001-Disponibilidade via ICMP Cameras:icmpping[,,60,].last()}=0`) e alertará no dashboard e em todos sistemas de notificações configurados, e em mapas, através de uma macro interna do zabbix `{HOSTNAME}`. A trigger é capaz de dizer qual HOST em específico apresenta problemas.

A Tabela 4 apresenta estrutura do *template* ICMP e nas Figuras 9,10,11 e 12, todas as formas de alertas que foram disparadas devido à configuração do *template*.

Tabela 4 Tabela ICMP

Aplicações	Itens	Triggers
Disponibilidade ICMP	Disponibilidade ICMP	Equipamento <code>{HOSTNAME}</code> não responde ao (PING)

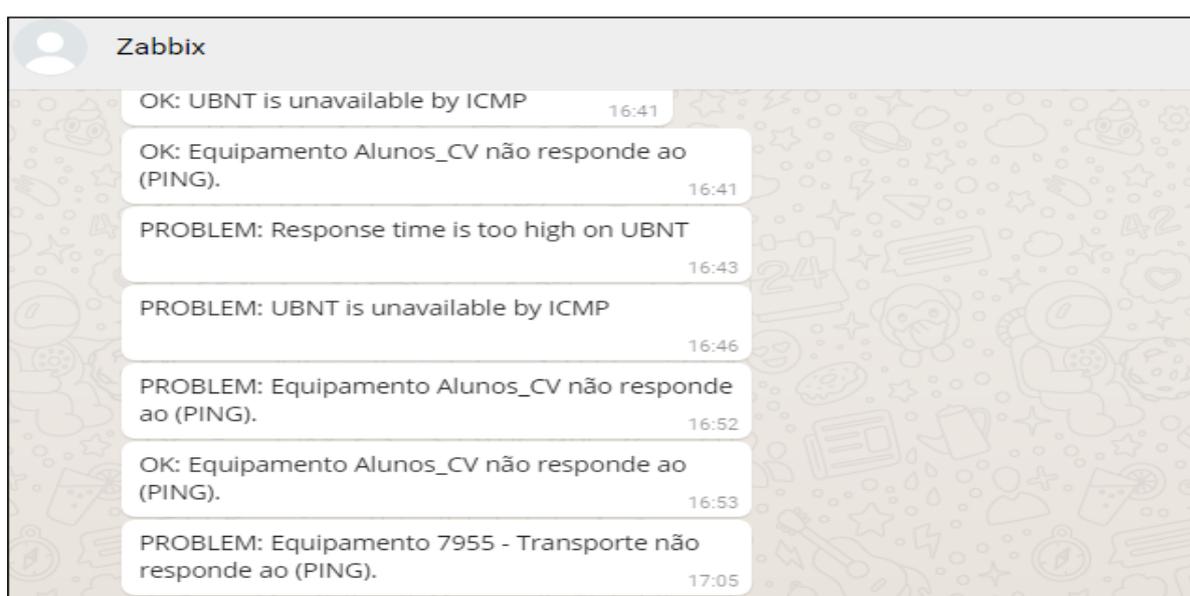


Figura 9 Notificação Trigger ICMP: WhatsApp

Últimos 20 incidentes						
Host	Assunto	Última alteração	Idade	Informação	Reconhecido	Ações
UBNT	UBNT is unavailable by ICMP	16-12-2015 17:25:44	5h 1m 3s		Não	2
7955 - Transporte	Equipamento 7955 - Transporte não responde ao (PING).	16-12-2015 17:04:28	5h 22m 19s		Não	3

Figura 10 Incidente Trigger ICMP



Figura 11 Alerta Trigger ICMP: MAPA

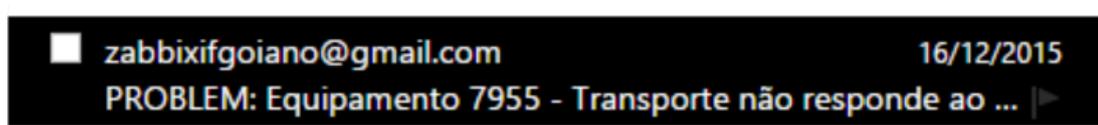


Figura 12 Alerta Trigger ICMP: e-mail

## 13.2. TEMPLATE S.O.

Neste *template* não houve alterações, suas configurações padrões atenderam as necessidades deste trabalho e será apresentado apenas o que foi utilizado pois o mesmo apresenta muitas informações. O *template* de S.O. é constituído por dois *templates* que coletam informações de sistemas operacionais como o Cent OS 7 e Windows Server 2012 utilizados neste trabalho. Para realizar a coleta é necessário configurar os Agent Zabbix em todos os hosts.

Com esses parâmetros é possível coletar informações de sistema livre ou proprietário como: uso de processador, quantidade total de memória livre e em uso, quanto de armazenamento o host possui. Visualizar essas informações em gráficos, e por conta da autodescoberta, o Zabbix consegue identificar a quantidade de unidades de disco e interfaces que cada host possui. A Tabela 5 apresenta toda estrutura do *template*.

Tabela 5 Template S.O.

Aplicações	Itens	Triggers	Gráficos	Regras de Descoberta
CPU	Processor	Processor load is too high on {HOST.NAME}	CPU load	
Filesystems	Total Memory	Lack of free swap space on {HOST.NAME}		Mounted filesystem discovery
MEMORY	Used Memory	Lack of free memory on server {HOST.NAME}	Memory usage	
Network Interfaces				Network interface discovery

### 13.3. TEMPLATES SNMP

Ele é composto por seis *templates*, três deles para a versão 1 do protocolo que é utilizado para monitorar as *Nanostation*, que não possuem suporte para outra versão do protocolo, e a versão 2 que está associado aos *switchs*. Para realizar o monitoramento foi necessário habilitar o SNMP nos equipamentos e, foi utilizada comunidade pública.

Por padrão, o Zabbix possui o *template* SNMP v2, mas como as antenas sem fio *Nanostation* suportam apenas o protocolo v1, foi necessário realizar uma cópia dos *templates* SNMPv2 e trocar a variável do agente em cada item. Para cada versão do SNMP há um *template*: *generic*, *interfaces* e *device*. O *template generic* irá coletar informações como nome, tempo de atividade do *switch*. O componente *interfaces* irá buscar as *interfaces* que o *switch* possui, independente do mesmo ser de 24 ou 48 portas. E o *device* irá agrupar os *templates* anteriores e assim é possível vincular ele a um host e obter todas as informações coletadas pelos outros dois *templates*.

A Tabela 6 apresenta a estrutura do *template*, e a Figura 13 apresenta os dados coletados de um switch após a configuração do *template*.

Tabela 6 Template SNMP

Aplicações	Itens	Regras de Descoberta
013-Template SNMP Generic SNMPv2: General	010-Template SNMP Generic SNMPv2: Device contact details 010-Template SNMP Generic SNMPv2: Device description 010-Template SNMP Generic SNMPv2: Device location 010-Template SNMP Generic SNMPv2: Device name 010-Template SNMP Generic SNMPv2: Device uptime	
014-Template SNMP Interfaces SNMPv2: Interfaces	011-Template SNMP Interfaces SNMPv1: Number of network interfaces	011-Template SNMP Interfaces SNMPv1: Network interfaces

SW-DIST01		General (5 Itens)				
<input type="checkbox"/>	Device contact details	17-12-2015 21:02:15	ifgoiano	-	<a href="#">Histórico</a>	
<input type="checkbox"/>	Device description	17-12-2015 21:02:16	HP V1910-48G Switch Software Version ...	-	<a href="#">Histórico</a>	
<input type="checkbox"/>	Device location	17-12-2015 21:02:15	ti	-	<a href="#">Histórico</a>	
<input type="checkbox"/>	Device name	17-12-2015 21:02:15	SW-DIST01	-	<a href="#">Histórico</a>	
<input type="checkbox"/>	Device uptime	17-12-2015 21:09:14	3 dias, 03:12:17	+00:01:00	<a href="#">Gráfico</a>	

Figura 13 Dados Coletados dos Switchs via SNMP

## 13.4. TEMPLATE SERVIÇO

Os templates de serviços contemplam medidas de desempenho de serviços web, proxy, server e mysql.

O template Monitoração WEB foi criado com intuito de monitorar a disponibilidade de dois sites que estão em servidores do Instituto, sem a necessidade de monitorar o serviço web diretamente, mas monitorar o site em si. É apresentado sua estrutura na Tabela 7. Para isso o Zabbix possui um recurso chamado WEB, que através de códigos de status que as URLs retornam é possível saber se o site está ativo ou não. Foi criada uma trigger para cada site, que é disparada quando o Zabbix não recebe o retorno esperado. Também é possível receber notificações visuais no *dashboard*, no *whatsapp* e via e-mail quando qualquer site fica inacessível.

Tabela 7 Template Monitoramento WEB

Aplicações	Trigger	Cenários Web
Internet	Atividade do Site FriendZone.net	Servico de monitoramento da FriendZone.net.br
	Atividade do Site S2BIFGoiano.net	Servico de monitoramento do S2BIFgoiano.net.br

Através do menu Monitoração > WEB é possível visualizar a última checagem feita nos sites determinados e analisar, através de gráficos, a velocidade e tempo de resposta dos mesmos como é apresentado nas Figuras 14 e 15.

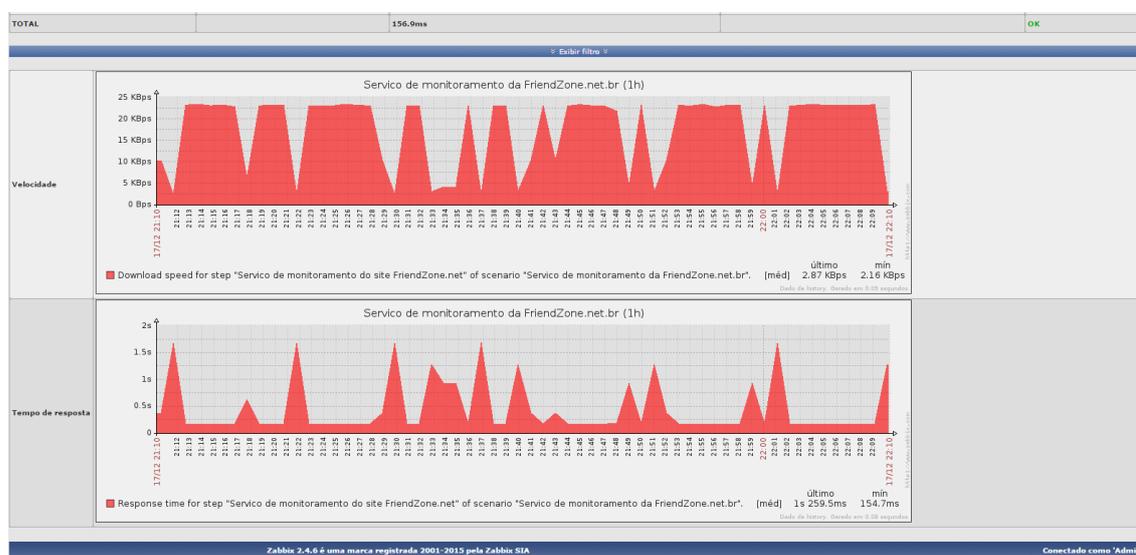


Figura 14 Velocidade e Tempo de resposta site friendzone.net.br

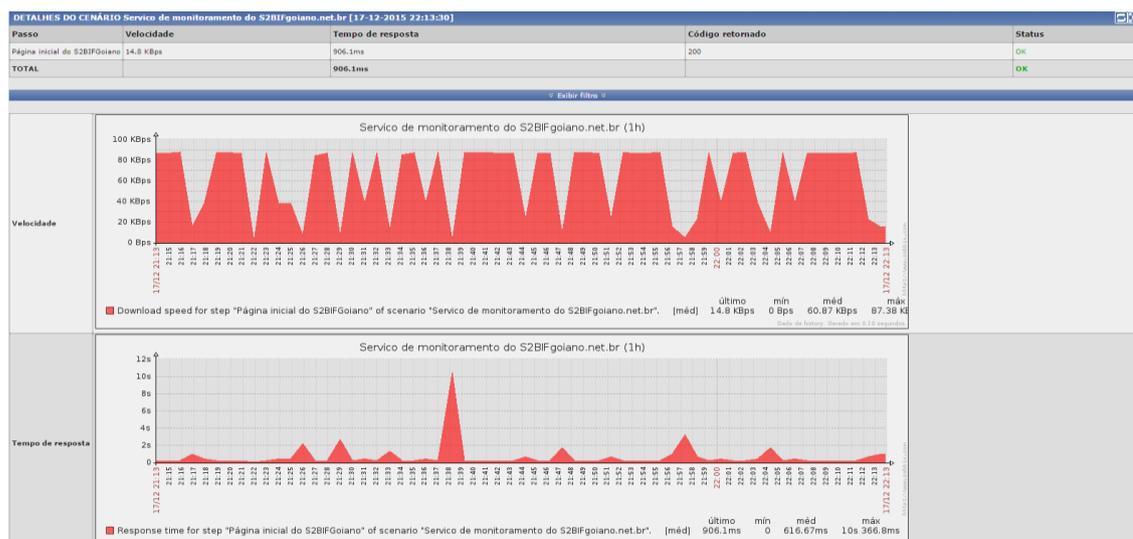


Figura 15 Velocidade e Tempo de resposta site s2bifgoiانو.net.br

Os templates App Zabbix Proxy e Server são padrões do Zabbix e são representados na Tabela 8. São responsáveis por coletar informações de desempenho desses serviços, como valores processados por segundo. Há uma trigger que é disparada ao chegar a valor de atraso de sincronismo dos processos, e um gráfico que apresenta o desempenho em tempo real de cada serviço.

Tabela 8 Estrutura Template App Zabbix Server e Proxy

Aplicações	Itens	Triggers	Gráficos
Zabbix proxy	Values processed by Zabbix proxy per second	Zabbix configuration syncer processes more than 75% busy	Zabbix proxy performance
Zabbix server	Values processed by Zabbix server per second	Zabbix configuration syncer processes more than 75% busy	Zabbix server performance

É possível acessar o gráfico de desempenho dos Servidores no menu monitoramento > gráficos, selecionar o grupo Zabbix Server, o host Zabbix Proxy ou Zabbix Server e o gráfico Zabbix Proxy ou Zabbix Server performance. Pode ser observado a coleta de informações nas Figuras 16 e 17.

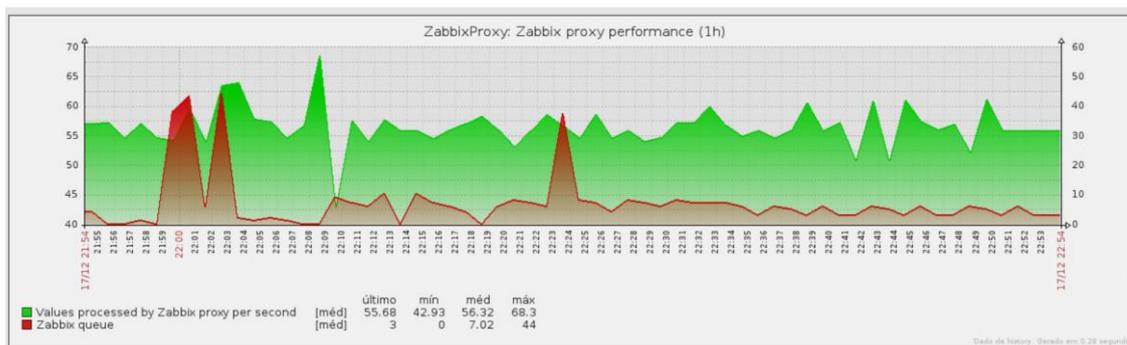


Figura 16 Desempenho Zabbix Proxy

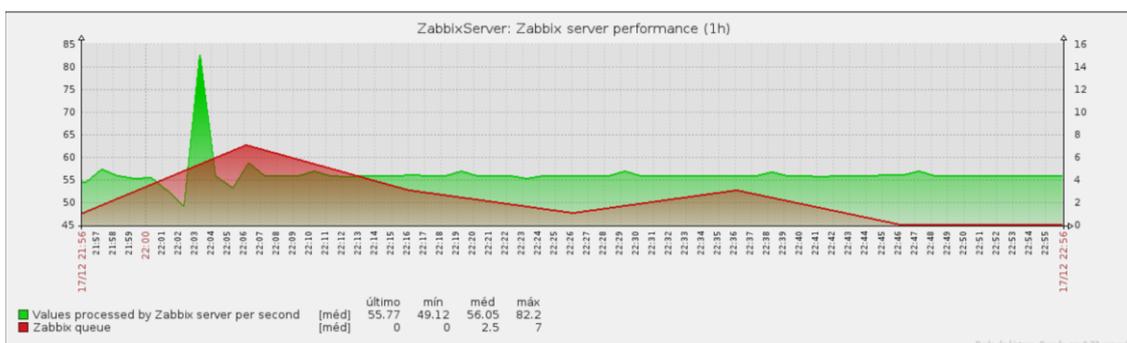


Figura 17 Desempenho Zabbix Server

O Template App Mysql também é um dos padrões que o Zabbix possui. Ele permite coletar informações sobre o serviço do Mysql, tais como quantidade de operações por segundo, tráfego no servidor, receber alertas quando o banco estiver fora de operação, e obter gráficos de tráfego e desempenho do serviço. O mesmo é apresentado na Tabela 9, e o desempenho do servidor nas Figuras 18 e 19.

Tabela 9 Template App Mysql

Aplicações	Itens	Triggers	Gráficos
MySQL	MySQL begin perations per second MySQL bytes received per second MySQL bytes sent per second	MySQL is down	MySQL bandwidth MySQL operations

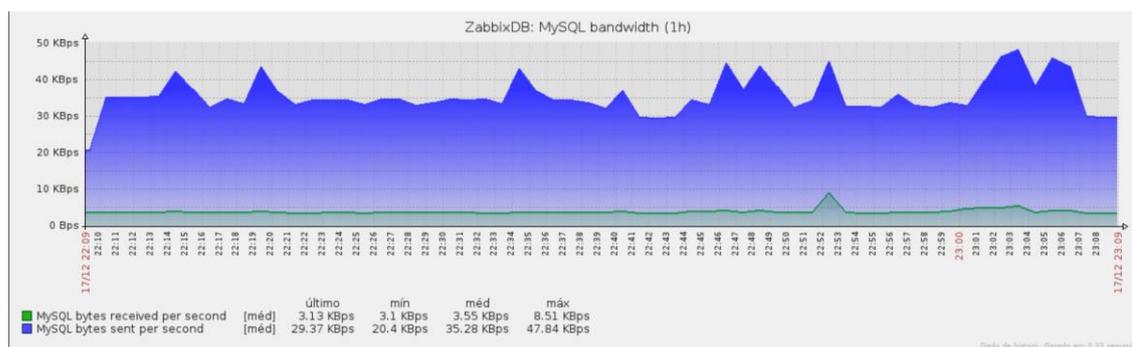


Figura 18 Desempenho de rede Mysql

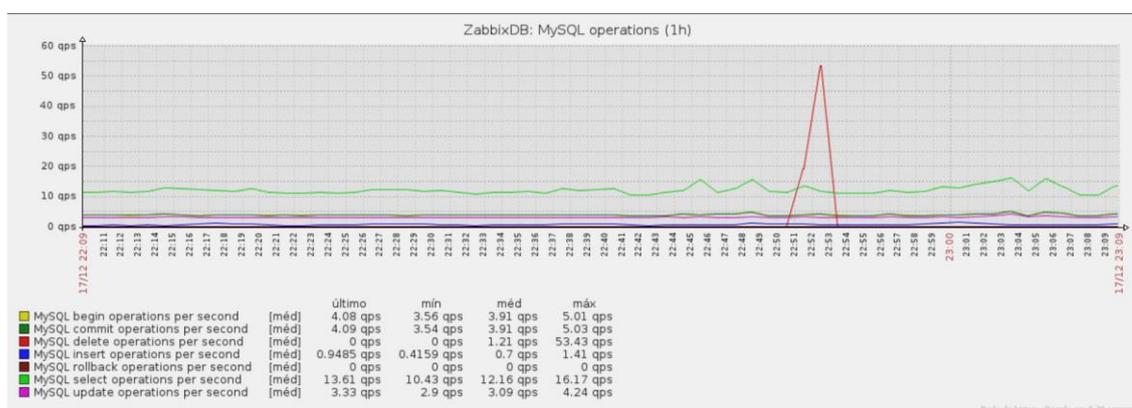


Figura 19 Desempenho de consultas Mysql

## 13.5. GRÁFICOS

O Zabbix possui esse recurso onde as informações coletadas, através de todos os agentes, podem ser exibidas de forma gráfica, facilitando a visualização de informações e seu histórico.

Foram criados gráficos que apresentam informações relevantes para a análise e gerenciamento dos hosts monitorados. Os gráficos são compostos pelos itens que fazem parte dos templates apresentados anteriormente. Além dos gráficos anteriores, seguem abaixo nas Figuras 20 e 21, consumo de memória ram “*Random Access Memory*”, processador, disco e rede. São apresentadas as informações coletadas do host Zabbix server, porém essas informações estão disponíveis também em todos os hosts que contém os agentes instalados e configurados, como todos os servidores zabbix, Windows, computadores do laboratório 2, nanostation e switches.

A apresentação da informação é em tempo real e é possível filtrar o período de tempo de apresentação das informações, variando de 1 hora, como padrão, até um mês atrás ou todo período em que o host está cadastrado no Zabbix.

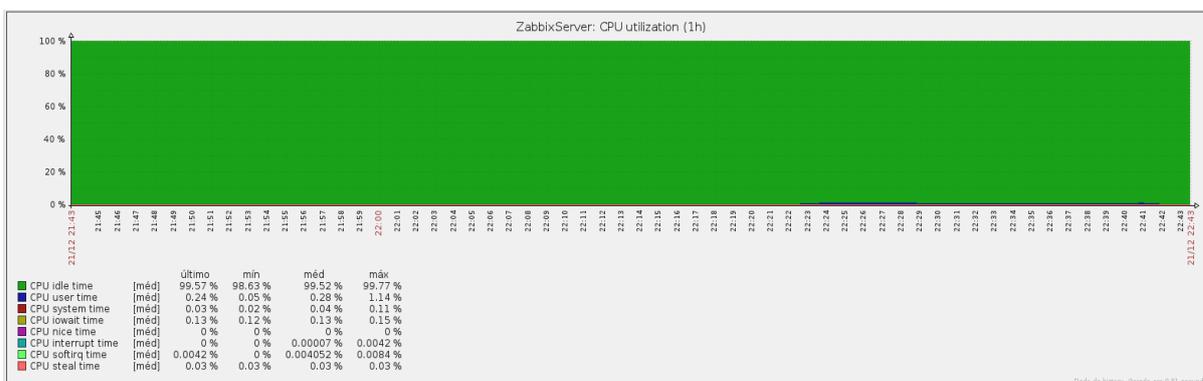


Figura 20 Gráfico: Utilização de processador

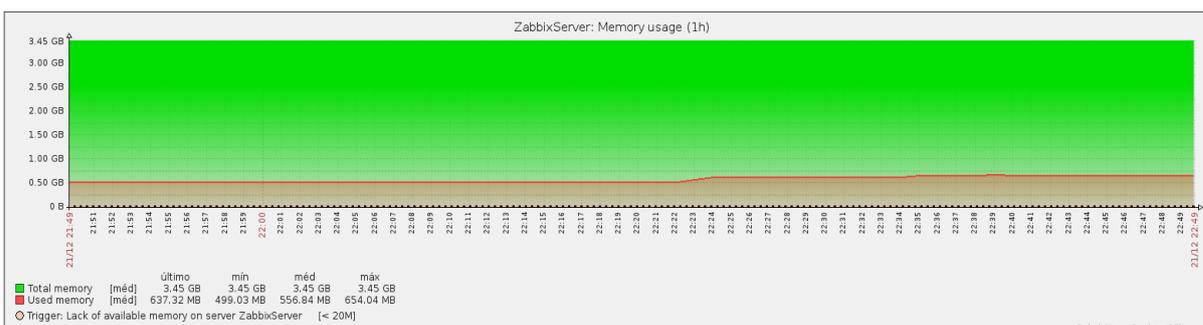


Figura 21 Gráfico utilização Memória Ram.

Independentemente da quantidade de interfaces de rede e discos de um host, o Zabbix é capaz de identificar automaticamente essas interfaces e discos, coletar e apresentar seus tráfegos como é apresentado nas Figuras 22 e 23.

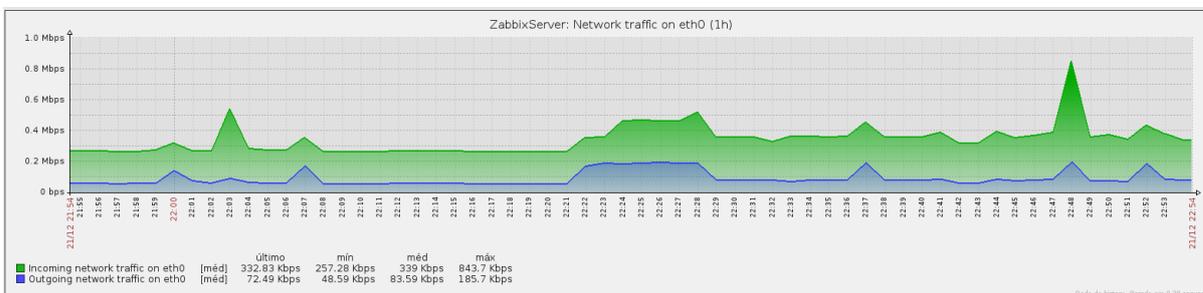


Figura 22 Gráfico Tráfego de rede

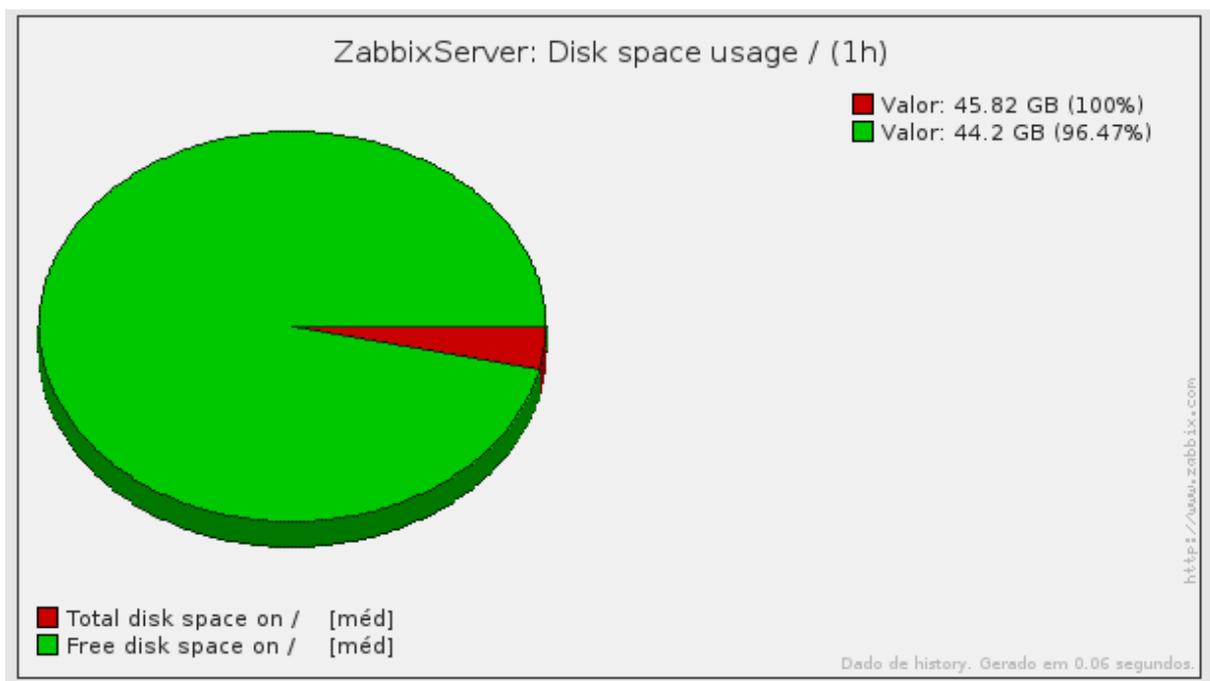


Figura 23 Gráfico utilização de Disco

## 13.6. MAPAS

Os mapas criados no Zabbix são ótimos para visualização de informações. Através deles é possível mapear a localidade dos equipamentos e também, o tráfego entre os equipamentos.

Foram criados quatro mapas. Dois contemplam a localização dos equipamentos de acordo com a estrutura do Campus Morrinhos, apresentados nas Figuras 24 e 25, e os outros dois apresentam o tráfego entre os ativos que são mostrados nas Figuras 26 e 27. Todos os mapas são dinâmicos. Se houver algum problema em um determinado host, o Zabbix irá apresentar no mapa, disparar as triggers e realizar todo processo de alerta. Desta forma, o administrador da rede poderá ter maior precisão de onde está o problema em sua estrutura e tomar as medidas necessárias para solução do problema.



Figura 24 Mapa de status da telefonia do Campus



Figura 25 Mapa de localização das câmeras de segurança

Os mapas que apresentam tráfego realizam a busca dos dados encontrados através dos itens, e é criado links entre os ícones, esses que representam os hosts. Assim é possível apontar no mapa a interface de comunicação entre eles, pelo último valor coletado, detalhes do status dos hosts e o tráfego entre eles.

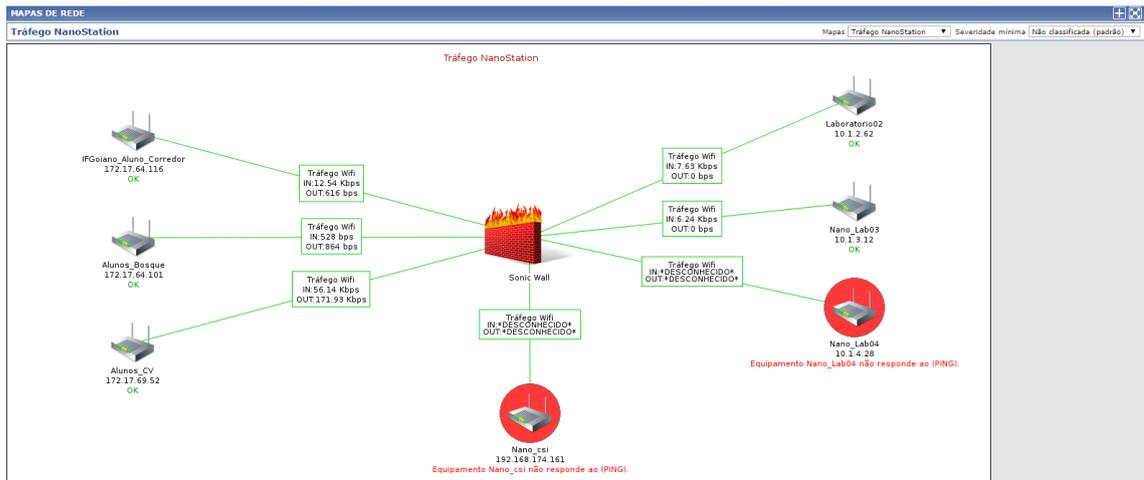


Figura 26 Mapa tráfego Nanostation

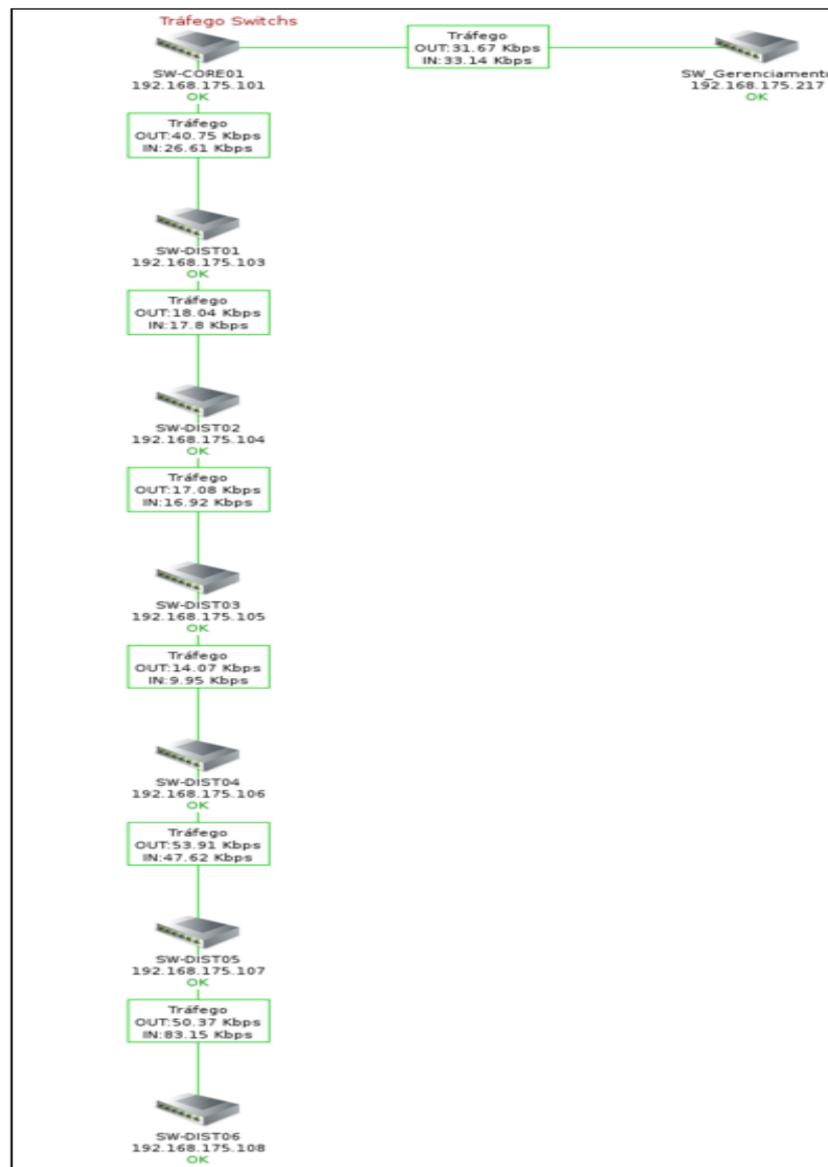


Figura 27 Mapa tráfego Switch

## 13.7. AGRUPAMENTO DE GRÁFICOS

O Zabbix possui um recurso que torna a visualização das informações mais fácil. A possibilidade de criar telas torna possível realizar o agrupamento de vários gráficos e mapas ao mesmo tempo, possibilitando o administrador de rede realizar comparativos entre o consumo de recursos e detectar problemas de forma mais eficiente.

Foram criadas 10 telas, que agrupam os gráficos de desempenho dos servidores: Zabbix Server, Zabbix Proxy I, Proxy II e Zabbix DB. Os itens de desempenho avaliados foram: consumo de memória ram, tráfego de suas interfaces e mapas criados. Todas as telas são apresentadas nas Figuras 28 a 37.

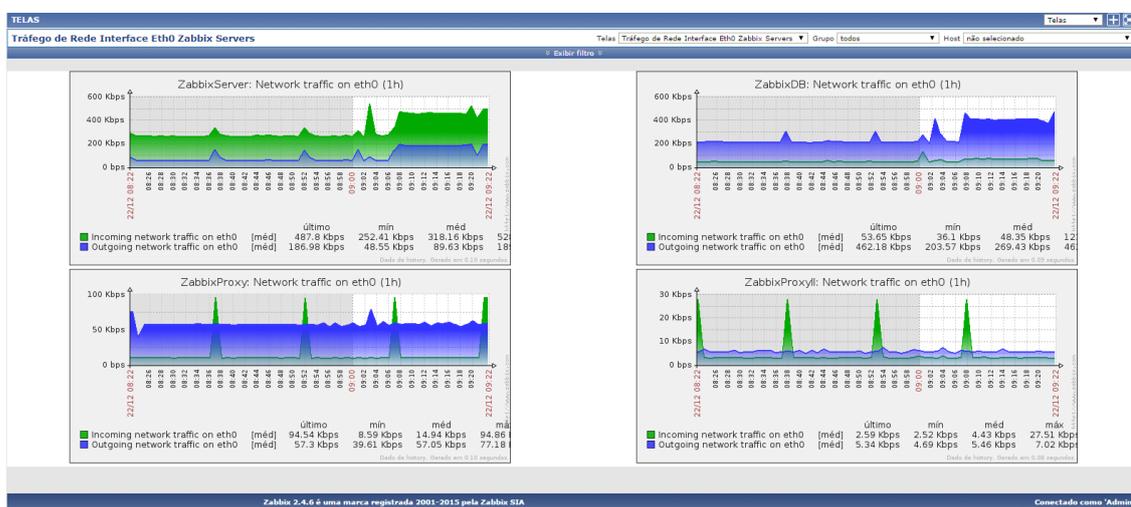


Figura 28 Tela com gráficos das interfaces Eth0 dos servidores

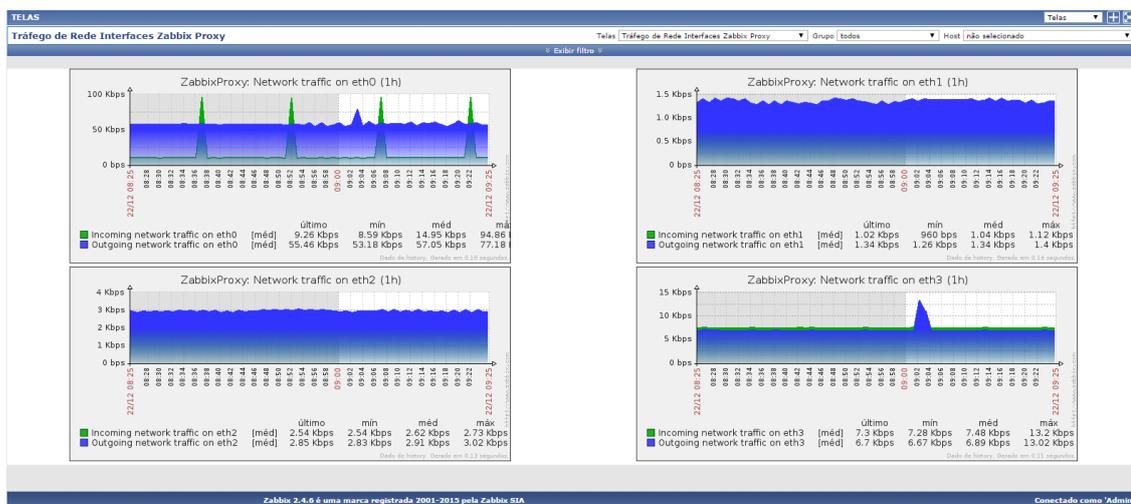


Figura 29 Tela com gráfico das interfaces do Zabbix



Figura 30 Tela interfaces do servidor Zabbix Proxy II

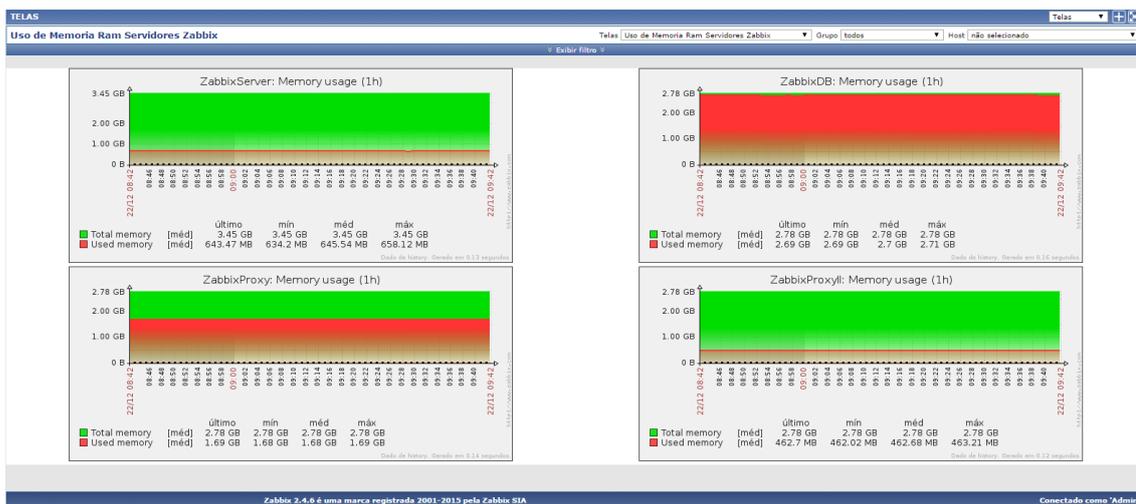


Figura 31 Tela consumo de memória ram dos servidores

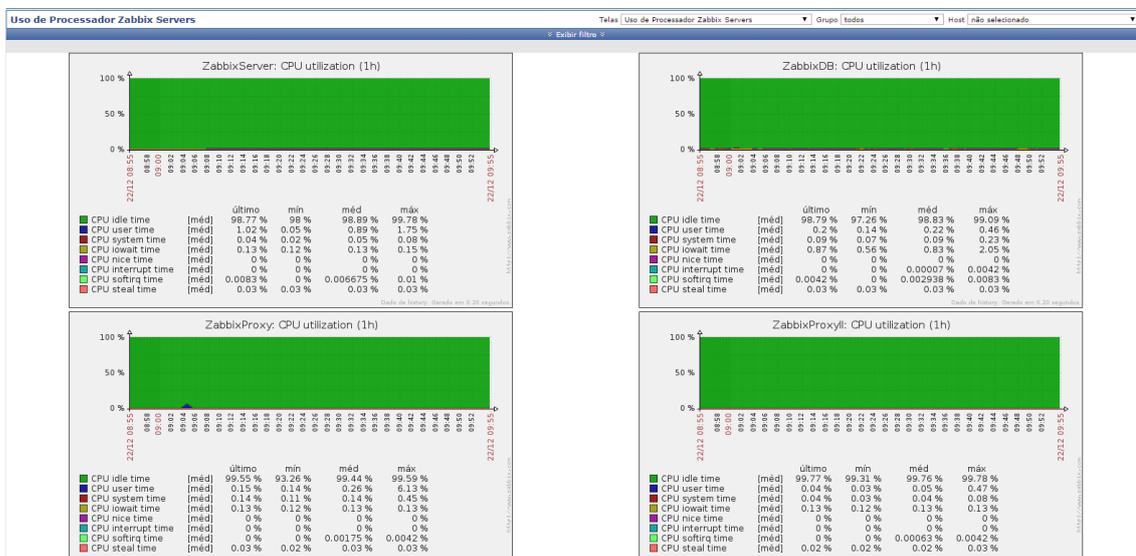


Figura 32 Tela uso de processador dos servidores

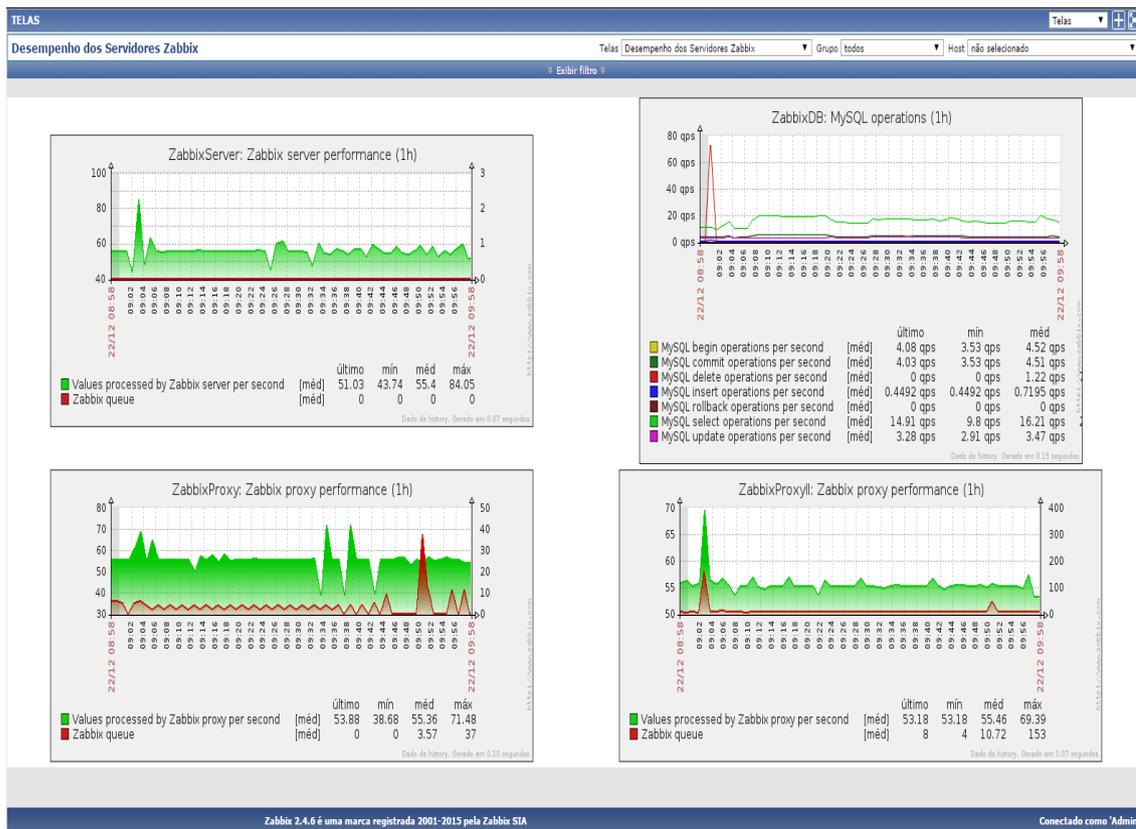


Figura 33 Tela desempenho do serviço zabbix e Mysql



Figura 34 Tela mapeamento câmeras de segurança



Figura 35 Tela mapeamento telefonia

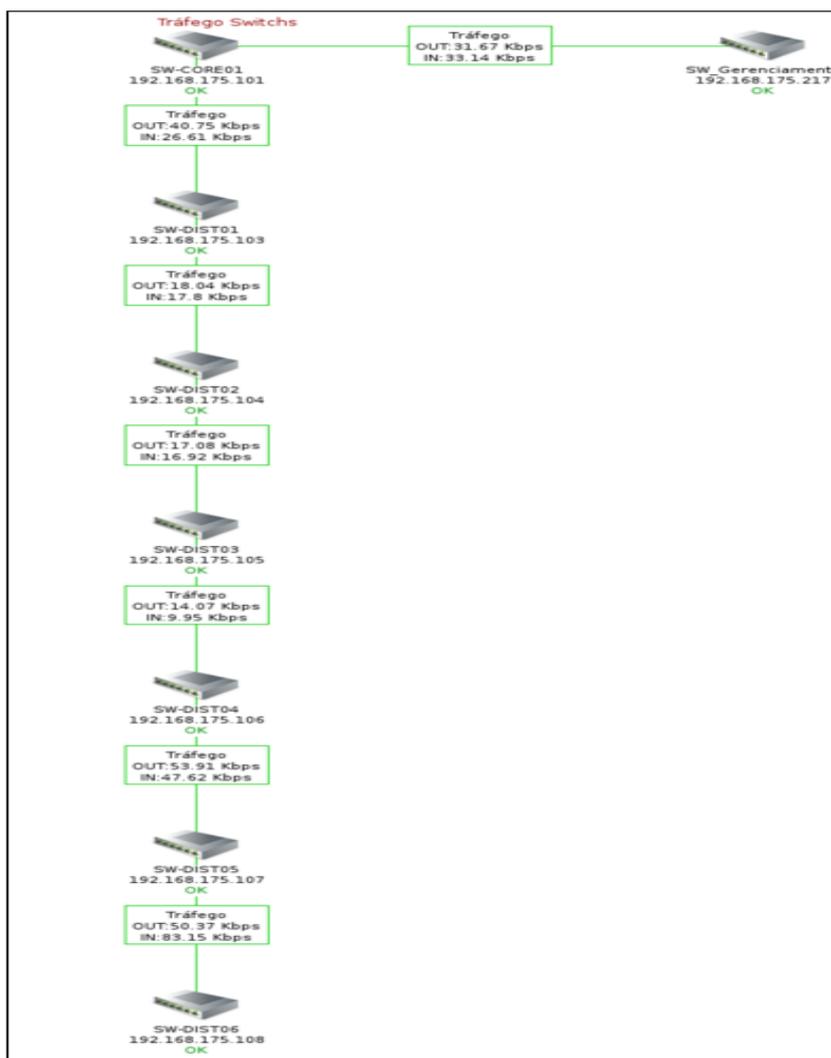


Figura 36 Tela mapeamento tráfego switch

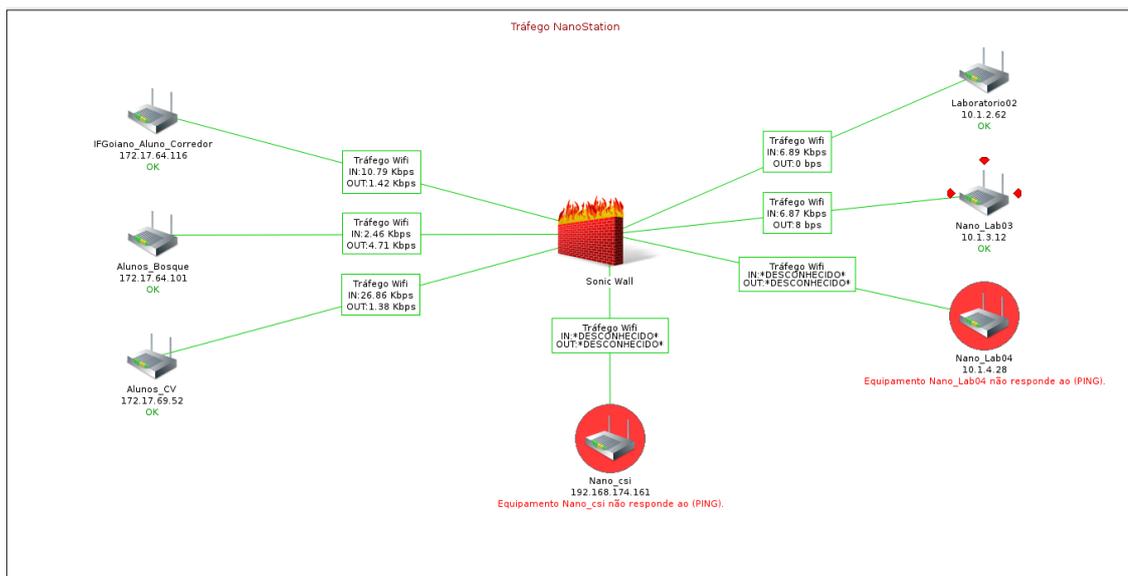


Figura 37 Tela de mapeamento do tráfego Nanostation

## 13.8. APRESENTAÇÃO DE SLIDS

Os slids são responsáveis por apresentar todas as telas criadas com os gráficos e mapas de forma dinâmica. Assim, bastou criar um slid com todo conteúdo apresentado anteriormente. Na coordenação de TI do campus, foi instalada uma televisão, e ligada a um computador. Com a apresentação do recurso de slid a equipe de TI tem todas as informações coletadas apresentadas em gráficos e organizadas em telas sendo apresentadas, atualizando a apresentação de trinta em trinta segundos.

O recurso de slid pode ser apresentado no menu Configuração > SlidShow e para visualizar em Monitoramento > telas, no canto superior direito é necessário colocar a opção SlidShow.

## 14. CONCLUSÃO

Este trabalho apresenta a instalação, configuração e dados obtidos através das coletas realizadas pelo Zabbix em parte dos equipamentos e serviços do IF Goiano - Campus Morrinhos, compostos por servidores, câmeras de segurança, switches, antenas nanostations, telefones VoIP, dois sites que estão hospedados no Campus e recursos de hardware dos servidores e hosts do laboratório dois de informática. Descreve toda fundamentação teórica necessária para a instalação e configuração do Zabbix e a realização do monitoramento.

O Zabbix é uma ferramenta *open source* que possui uma comunidade bastante ativa, que buscam dispor de novos recursos em um curto prazo de tempo. Devido à forma que foi projetada sua implantação no campus morrinhos, e devido a utilização do Cent OS, gerou uma pequena dificuldade para conseguir estabilizar toda intercomunicação de servidores e realizar as configurações da ferramenta e na tentativa de utilizar pluguins.

De acordo com a execução deste trabalho, observa-se que a ferramenta Zabbix é capaz de atender diversos tipos de infraestruturas, de pequeno, médio e grande porte. Para o processo de monitoramento não possui complicação, atende usuários com conhecimentos básicos à usuários avançados que podem pretender lançar novos desafios, possibilitando novas formas de coletas e novas apresentações de dados.

Conclui-se que a implantação do Zabbix no IF Goiano Campus Morrinhos se mostrou eficaz e atendeu as expectativas, com ele é possível obter status, coletar informações de atividade de equipamentos como os telefones, câmeras de segurança, servidores, switches, nanostations. Ele é capaz de realizar a detecção quase imediata da parada de algum equipamento ou serviço, e emitir alertas visualmente, por e-mail ou whatsapp. Ainda permite realizar a análise das informações de tráfego nas portas de todos switches, antenas, servidores e hosts, que foram dispostos a serem monitorados.

## 15. REFERÊNCIAS

4LINUX. **O Que É Zabbix.** Disponível em: <https://www.4linux.com.br/o-que-e-zabbix>. Acesso em: 12 de abr. 2016.

Andrey, Alisson. **Solução De Gerenciamento De Redes Utilizando O Sistema De Código Aberto: Zabbix.** Universidade Tecnológica Federal do Paraná, 2011.

Carlos, Antonio; et. Al (2014). **Virtualização De Servidores: Uma Prática Que Proporciona Benefícios Ao Meio Ambiente E À Gestão Empresarial.** Disponível em: <http://www.aedb.br/seget/arquivos/artigos14/40520509.pdf>>. Acessado em: 02 de fev. 2016.

Batista, Leonardo. **Gerenciamento De Uma Rede De Computadores Em Um Ambiente Corporativo (Uepb/Campus Vii) utilizando O Software Zabbix.** Universidade Estadual da Paraíba, 2014.

Comer, Douglas E. **Redes de computadores e Internet.** 4. ed. Porto Alegre: Bookman, 2007.

Déo, André. **Implementando Zabbix 2.X Proxy Em Ambiente Centos.** Disponível em: <<http://zabbixbrasil.org/wiki/tikiindex.php?page=Implementando+Zabbix+2.x+Proxy+em+Ambiente+CentOS>>. Acesso em: 22 de dez. 2015.

Déo, André; Pires, Aécio. **Gerência de Redes com Zabbix.** p.69 Disponível em: <[http://revista.espiritolivres.org/pdf/Revista\\_EspiritoLivre\\_018\\_setembro2010.pdf](http://revista.espiritolivres.org/pdf/Revista_EspiritoLivre_018_setembro2010.pdf)>. Acesso em: 6 de jul. 2015.

Eder, João. **Monitoramento Em Redes Ipv6 Com Zabbix E Raspberry Pi.** Universidade Tecnológica Federal Do Paraná, 2014.

Elaine, Carla; Aguiar, Jerônimo. **Aumentando A Segurança Da Informação Com Softwares Livres Em Uma Universidade.** Ponto de Presença da RNP na Bahia (PoP-BA), 2006.

Ernando, Washington. **Monitoramento E Gerenciamento de Redes Utilizando Zabbix.** Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – Câmpus Capivari, 2015.

Fachini, Thiago; Timm, Alexandre. **Implementação Da Ferramenta Zabbix Para Monitoramento Reativo.** Universidade Luterana do Brasil, 2010.

Martins,Hernandes. **Zabbix 2.4 Cent Os 7 Tutorial De Instalação.** Disponível em: <<http://hernandesmartins.blogspot.com.br/2015/03/zabbix-2-4-centos-7-tutorial-portugues.html>>. Acesso em: 22 de dez. 2015.

IF Goiano. **Histórico.** Disponível em: <<https://www.ifgoiano.edu.br/home/index.php/historico-morrinhos>> Acesso em: 01 de fev. 2016.

Kurose, James F; Ross Keith W. **Redes de Computadores e a Internet**. 6. ed. São Paulo: Pearson Prentice, 2013.

Luiz, André. **Gerenciamento de redes com snmp**. Unicamp, 2012.

Medeiros, Marcelo. **Notificações Zabbix via whatsapp**. Disponível em: <<http://www.blogdomedeiros.com.br/notificacoes-zabbix-via-whatsapp/>>. Acesso em: 22 de dez. 2015.

Moraes, Márcio. **Gerenciamento De Redes Tcp/Ip: Monitoramento Da Taxa De Utilização De Enlaces Em Redes Ethernet Usando A Ferramenta Zabbix**. Universidade Católica de Goiás, 2008.

Naugle, Mattheu G. **Illustrated TCP/IP**. Wiley Computer Publishing, 1998.

Martellota, Pedro. **Enviando Alertas De e-mail Pelo Zabbix Usando Gmail, Centos E Postfix**. Disponível em: <<https://www.vivaolinux.com.br/dica/Enviando-alertas-de-e-mail-pelo-Zabbix-usando-Gmail-CentOS-e-Postfix>>. Acesso em: 22 de dez. 2015.

Pinheiro, Ricardo. **Monitoramento De Servidores Com Zabbix**. Disponível em: <<http://www.cooperati.com.br/2011/10/04/monitoramento-de-servidores-com-zabbix/>>. Acesso em: 22 de dez. 2015.

RNP. **Cultura**. rnp.br. Disponível em: <<https://www.rnp.br/solucoes/cultura>>. Acesso em: 12 de abr. 2016.

Rodrigues, Benedito. **Gerência E Monitoramento de Redes De Computadores Com O Software Livre Nagios**. Instituto de Estudos Superiores da Amazônia, 2005.

Sateles, Sueli. **Monitoramento De Redes: Análise E Configuração Do Software Zabbix**. IFSP, 2015.

Sousa, Linderberg. **Redes de computadores: dados, voz e imagem**. 5. Ed. São Paulo: Érica, 2005.

Spinola, Adail Horst Et al. **De A a Zabbix** 1. ed. São Paulo: Novatec, 2015.

Tanenbaum, Andrew S; Wetherall David. **Redes De Computadores**. 5. ed. São Paulo: Pearson Prentice, 2011.

Tapajos, Mauro et al. **Gerência De Redes De Computadores**. 2. ed. Rio de Janeiro: Escola Superior de Redes, 2015.

Torres, Pedro R. et al. **Redes E Segurança**. 1. ed. Rio de Janeiro: Escola Superior de Redes, 2013.

Vieira, Wênio. **Gerenciamento De Redes Com A Ferramenta Zabbix: Caso De Uso Campus Urutaí**. Instituto Federal de Educação Ciência e Tecnologia Goiano, 2014.

Zabbix SIA, **O que é o Zabbix.** Disponível em: <<https://www.zabbix.com/documentation/2.4/pt/manual/introduction/about>>. Acesso em: 12 de abr. 2016.

## 16. APÊNDICE A - INSTALAÇÃO DO ZABBIXDB MYSQL

O processo de instalação criado por Martins. (2015) e adaptado para este trabalho, uma vez que o processo original engloba a instalação do Servidor do Zabbix junto com outros parâmetros. A adaptação feita é totalmente necessária para que se adeque ao nosso ambiente.

Aqui é abordada a instalação e configuração do Mysql Server de forma a atender as consultas do Zabbix. Os servidores conectados devem estar se comunicando de acordo com os endereçamentos citados anteriormente, e o usuário logado como root.

A versão utilizada foi a MYSQL: 5.6. Todos os passos executados adiante serão dentro da pasta Zabbix, sendo necessário criar a mesma em /etc/.

### 16.1. PREPARAÇÃO

```
mkdir /etc/Zabbix
```

```
#Realize a atualização dos pacotes do servidor
```

```
yum update -y
```

```
#Acesse o arquivo de configuração do selinux e o desative
```

```
vi /etc/sysconfig/selinux
```

```
SELINUX=disabled
```

```
#Instale o wget, responsável por possibilitar o download de dados pela
```

web

```
yum install -y wget
```

## 16.2. INSTALAR AS DEPENDÊNCIAS

Abaixo segue os comandos necessários para instalar as dependências que o Zabbix utiliza, mesmo o Server não sendo instalado junto com o banco de dados, elas são necessárias para o funcionamento do Zabbix Server e a instalação do Zabbix Agent que irá coletar as informações de hardware e do próprio MySQL.

```

yum install -y OpenIPMI.x86_64 net-snmp.x86_64 unixODBC.x86_64
yum install -y java-1.7.0-openjdk-headless.x86_64 dejavu-sans-fonts
gcc.x86_64 mysql-community-server.x86_64
yum install -y mysql-community-devel.x86_64 libxml2-devel.x86_64 net-
snmp-devel.x86_64 libssh2-devel.x86_64
yum install -y OpenIPMI-devel.x86_64 libcurl-devel.x86_64 java-1.7.0-
openjdk-devel.x86_64 httpd php.x86_64
yum install -y php-mysql.x86_64 php.x86_64 php-mysql.x86_64 php-
devel.x86_64 php-xml.x86_64 php-cli.x86_64 php-bcmath.x86_64 php-
mbstring.x86_64 php-gd.x86_64

```

```

#Instale o iksemel
rpm -ivh ftp://ftp.muug.mb.ca/mirror/fedora/epel/7/x86_64/i/iksemel-1.4-
6.el7.x86_64.rpm

```

## 16.3. INSTALANDO O FPING

O Fping é um utilitário responsável por localizar hosts na rede.

```

#Baixe o pacote do Fping
wget http://pkgs.repoforge.org/fping/fping-3.10-1.el7.rf.x86_64.rpm

```

```

#Instale o pacote
rpm -ivh fping-3.10-1.el7.rf.x86_64.rpm

```

## 16.4. REPOSITÓRIO OFICIAL ZABBIX

Abaixo segue os repositórios necessários para a instalação do agente Zabbix e os pacotes necessário para Zabbix-mysql:

```
wget http://repo.zabbix.com/zabbix/2.4/rhel/7/x86_64/zabbix-server-2.4.6-1.el7.x86_64.rpm
```

```
wget http://repo.zabbix.com/zabbix/2.4/rhel/7/x86_64/zabbix-server-mysql-2.4.6-1.el7.x86_64.rpm
```

```
wget http://repo.zabbix.com/zabbix/2.4/rhel/7/x86_64/zabbix-web-2.4.6-1.el7.noarch.rpm
```

```
wget http://repo.zabbix.com/zabbix/2.4/rhel/7/x86_64/zabbix-web-mysql-2.4.6-1.el7.noarch.rpm
```

```
rpm -ivh http://repo.zabbix.com/zabbix/2.4/rhel/7/x86_64/zabbix-2.4.6-1.el7.x86_64.rpm
```

```
rpm -ivh http://repo.zabbix.com/zabbix/2.4/rhel/7/x86_64/zabbix-agent-2.4.6-1.el7.x86_64.rpm
```

```
rpm -ivh http://repo.zabbix.com/zabbix/2.4/rhel/7/x86_64/zabbix-get-2.4.6-1.el7.x86_64.rpm
```

```
rpm -ivh http://repo.zabbix.com/zabbix/2.4/rhel/7/x86_64/zabbix-sender-2.4.6-1.el7.x86_64.rpm
```

```
rpm -ivh zabbix-server-2.4.6-1.el7.x86_64.rpm zabbix-server-mysql-2.4.6-1.el7.x86_64.rpm
```

```
rpm -ivh zabbix-web-mysql-2.4.6-1.el7.noarch.rpm zabbix-web-2.4.6-1.el7.noarch.rpm
```

## 16.5. REPOSITÓRIO OFICIAL MYSQL

```
#Baixe o pacote do mysql
rpm -Uvh http://dev.mysql.com/get/mysql-community-release-el7-
5.noarch.rpm
```

```
#Instale o pacote
sudo yum -y install mysql-community-server
```

```
#Habilite o serviço mysqld.service
systemctl enable mysqld.service
```

```
#Inicie o serviço mysql.service
systemctl start mysqld.service
```

```
#Cheque status do mysqld.service
systemctl status mysqld.service | grep Active
```

```
#Verifique se o serviço mysqld.service foi habilitado
systemctl list-unit-files --type service | grep mysqld.service
```

```
#Acesse o mysql
mysql -u root
```

Os passos abaixo são muito importantes, são eles que garantiram o acesso do Zabbix ao servidor. Os dados de usuário, nome do banco e senha que serão criados devem ser guardados para uso futuro.

```
#Crie o usuário Zabbixuser no banco de dados
CREATE USER 'Zabbixuser'@'localhost' IDENTIFIED BY 'z@bbixdb';
```

```
#Crie o banco Zabbixdb
create database Zabbixdb character set utf8 collate utf8_bin;
```

#Dê permissão de acesso para o usuário Zabbixuser do servidor com endereço 192.168.0.1 (que irá acessar o banco) de nome Zabbixdb

```
grant all privileges on Zabbixdb.* to Zabbixuser@192.168.180.4 identified by 'z@bbixdb';
```

#Aplique os privilégios

```
FLUSH PRIVILEGES;
```

#Saia do Mysql

```
exit
```

#Agora edite o arquivo de configuração do Mysql, aqui será habilitado a porta do mysql e qual endereço terá acesso ao mysql

```
vi /etc/my.cnf
```

```
port          = 3306
```

```
bind-address  = 192.168.0.1
```

#Tunning do Mysql (Os parâmetros abaixo serão responsáveis por executar um tunning no Mysql possibilitando o aumento de conexões do Zabbix Server ao banco, assim podendo ter menor tempo de resposta na comunicação dos dois).

```
max_connections = 512
```

```
innodb_buffer_pool_size = 500MB
```

## 16.6. CRIANDO O SCHEMA MYSQL ZABBIX

Esse é um processo muito importante, pois é ele que irá criar a base de informações do zabbix. Neste processo é gerado todas as Tabelas primárias, que serão alimentadas a medida que o Zabbix realiza o processo de coleta.

**Obs:** Os passos são executados obrigatoriamente nesta ordem.

```
cd /usr/share/doc/Zabbix-server-mysql-2.4.6/create/
```

#Ao digitar a próxima linha o sistema deve demorar um pouco a lhe permitir digitar novamente, só basta aguardar

```
mysql -uroot Zabbixdb < schema.sql
```

#Crie o schema de imagens

```
mysql -uroot Zabbixdb < images.sql
```

#Crie o shema de dados

```
mysql -uroot Zabbixdb < data.sql
```

#Agora o banco de dados e a base estão prontos, basta adicionar as regras no firewall do sistema para permitir a conexão.

```
firewall-cmd --permanent --zone=public --add-service=mysql
```

#Aplicar as conFigurações

```
systemctl restart firewalld.service
```

## 16.7. CONFIGURAÇÃO ZABBIX-AGENT

Na sequência configura-se o Zabbix agente, responsável por coletar as informações de hardware e serviços do nosso próprio servidor Zabbix.

```
#Habilita os Logs
```

```
LogFileSize=1
```

```
#Habilita quantidade de informação no log
```

```
LogLevel=3
```

```
#Habilita comandos remotos
```

```
EnableRemoteCommands=1
```

```
#Habilita log dos comandos remotos
```

```
LogRemoteCommands=1
```

```
#Endereço IP do servidor Zabbix-Server
```

```
Server=192.168.0.1
```

```
#Habilita porta que o agente irá ouvir
```

```
ListenPort=10050
```

#Define um nome para o Host. Este nome deverá ser informado ao criar um Host no frontend do Zabbix, caso esteja errado o monitoramento não irá ocorrer

```
Hostname=Zabbix Server
```

```
#Inserindo o Zabbix-agentd na inicialização do sistema
```

```
systemctl enable Zabbix-agent.service
```

```
#Iniciando o serviço Zabbix_agentd
```

```
systemctl start Zabbix-agent.service
```

```
#Verificando Status do serviço Zabbix_server.service
systemctl status Zabbix-agent.service | grep Active
```

#Verificando se os serviços do Zabbix foram habilitados, no caso deste servidor contendo apenas o Zabbix-agent habilitado

```
systemctl list-unit-files --type service | grep Zabbix
```

#Agora crie as regras de firewall para que possa haver comunicação do Zabbix agent com o server

```
firewall-cmd --permanent --zone=public --add-port=10050/tcp
firewall-cmd --permanent --zone=public --add-port=10050/udp
firewall-cmd --permanent --zone=public --add-port=10051/tcp
firewall-cmd --permanent --zone=public --add-port=10051/udp
firewall-cmd --permanent --zone=public --add-port=25/udp
firewall-cmd --permanent --zone=public --add-port=25/tcp
```

#Reinicie serviço de firewall para aplicar as configurações

```
systemctl restart firewalld.service
```

#Reinicie o servidor

```
reboot
```

## 17. APÊNDICE B - ZABBIX SERVER

Agora instala-se o Zabbix Server junto com o frontend e todo o processo de instalação e conexão com o banco de dados criado acima.

Os processos de instalação abaixo foram criados por Martins. (2015), e adaptado para este trabalho, onde original consta na instalação do Server junto com o banco de dados, e foi realizada uma atualização para o Zabbix conectar-se em um banco de dados remoto.

Todo o processo de instalação prosseguiu dentro da pasta install criada no diretório raiz /.

### 17.1. PREPARAÇÃO

```
#Para criar a pasta
```

```
mkdir /install
```

```
#Para acessar a pasta
```

```
cd /install
```

```
#Realizar a atualização do sistema com os pacotes mais atuais.
```

```
yum update -y
```

```
#Para proceder com a instalação será necessário desativar o selinux
```

```
vi /etc/sysconfig/selinux
```

```
SELINUX=disabled
```

## 17.2. INSTALAR AS DEPENDÊNCIAS / REPOSITÓRIOS

Abaixo segue os comandos necessários para instalar as dependências que o Zabbix utiliza, elas são necessárias para o funcionamento do Zabbix Server e a instalação do Zabbix Agent que irá coletar as informações de hardware do próprio servidor, instalará dependências que serão utilizadas na implantação do frontend e são responsáveis por realizar a monitoração dos equipamentos.

```
yum install -y wget
```

```
yum -y install OpenIPMI.x86_64 net-snmp.x86_64 unixODBC.x86_64
```

```
yum -y install java-1.7.0-openjdk-headless.x86_64 dejavu-sans-fonts
```

```
gcc.x86_64 mysql-community-server.x86_64
```

```
yum -y install mysql-community-devel.x86_64 libxml2-devel.x86_64 net-  
snmp-devel.x86_64 libssh2-devel.x86_64
```

```
yum -y install OpenIPMI-devel.x86_64 libcurl-devel.x86_64 java-1.7.0-  
openjdk-devel.x86_64 httpd php.x86_64
```

```
yum -y install php-mysql.x86_64 php.x86_64 php-mysql.x86_64 php-  
devel.x86_64 php-xml.x86_64 php-cli.x86_64 php-bcmath.x86_64 php-  
mbstring.x86_64 php-gd.x86_64
```

## 17.3. INSTALANDO O FPING

O Fping é um utilitário responsável por localizar hosts na rede.

```
#Baixe o pacote do fping
```

```
wget http://pkgs.repoforge.org/fping/fping-3.10-1.el7.rf.x86_64.rpm
```

```
#Instale o pacote
```

```
rpm -ivh fping-3.10-1.el7.rf.x86_64.rpm
```

## 17.4. INSTALANDO IKSEMEL

```
rpm -ivh ftp://ftp.muug.mb.ca/mirror/fedora/epel/7/x86_64/i/iksemel-1.4-  
6.el7.x86_64.rpm
```

## 17.5. Repositório Oficial Zabbix

```
#Agora será baixado os pacotes do Zabbix server, Zabbix agente, mysql
php Zabbix-web
    wget http://repo.Zabbix.com/Zabbix/2.4/rhel/7/x86_64/Zabbix-server-2.4.6-
1.el7.x86_64.rpm
    wget      http://repo.Zabbix.com/Zabbix/2.4/rhel/7/x86_64/Zabbix-server-
mysql-2.4.6-1.el7.x86_64.rpm
    wget      http://repo.Zabbix.com/Zabbix/2.4/rhel/7/x86_64/Zabbix-web-2.4.6-
1.el7.noarch.rpm
    wget      http://repo.Zabbix.com/Zabbix/2.4/rhel/7/x86_64/Zabbix-web-mysql-
2.4.6-1.el7.noarch.rpm

#Instale os pacotes baixados anteriormente
rpm -ivh http://repo.Zabbix.com/Zabbix/2.4/rhel/7/x86_64/Zabbix-2.4.6-
1.el7.x86_64.rpm
rpm -ivh http://repo.Zabbix.com/Zabbix/2.4/rhel/7/x86_64/Zabbix-agent-
2.4.6-1.el7.x86_64.rpm
rpm -ivh http://repo.Zabbix.com/Zabbix/2.4/rhel/7/x86_64/Zabbix-get-2.4.6-
1.el7.x86_64.rpm
rpm -ivh http://repo.Zabbix.com/Zabbix/2.4/rhel/7/x86_64/Zabbix-sender-
2.4.6-1.el7.x86_64.rpm
rpm -ivh Zabbix-server-2.4.6-1.el7.x86_64.rpm Zabbix-server-mysql-2.4.6-
1.el7.x86_64.rpm
rpm -ivh Zabbix-web-mysql-2.4.6-1.el7.noarch.rpm Zabbix-web-2.4.6-
1.el7.noarch.rpm
rpm -ivh http://repo.Zabbix.com/Zabbix/2.4/rhel/7/x86_64/Zabbix-java-
gateway-2.4.6-1.el7.x86_64.rpm
```

## 17.6. CONFIGURAÇÃO ZABBIX-SERVER

Agora será configurado o arquivo do Zabbix Server, onde será habilitado para realizar logs, a conexão com o banco de dados, a autodescoberta de rede, que será visto futuramente, e alguns parâmetros de tuning do Zabbix Server.

Observe que algumas linhas podem estar comentadas, basta retirar a # e ajustar o parâmetro conforme abaixo.

#Edite o arquivo de configuração do Zabbix server localizado em /etc/Zabbix

```
vi /etc/Zabbix/Zabbix_server.conf
```

#Habilita a porta a ser ouvida

```
ListenPort=10051
```

#Habilita a criação de Logs

```
LogFileSize=3
```

#Habilita a quantidade de informação coletada no log

```
DebugLevel=3
```

#Endereço IP do Servidor Mysql

```
DBHost=192.168.1.2
```

#Banco de Dados Criado no Servidor do Mysql

```
DBName=Zabbixdb
```

#Usuario criado no Servidor do Mysql

```
DBUser=Zabbixuser
```

#Senha criada para o usuário criado no Servidor do Mysql

```
DBPassword=z@bbixdb
```

```
#Processos de Tunning do Zabbix
#Aumenta a quantidade de conexões com o banco
StartPollers= 5
#
StartIPMIPollers=10
#
StartPollersUnreachable=80
#
StartTrappers=20

#Salve o arquivo para que as configurações sejam efetivas.
:wq
```

## **17.7. CONFIGURAÇÃO ZABBIX-AGENT**

É necessário a configuração do Zabbix agente, responsável por coletar as informações de hardware e serviços do nosso próprio servidor Zabbix.

```
#Habilita os Logs
LogFileSize=1

#Habilita quantidade de informação no log
DebugLevel=3

#Habilita comandos remotos
EnableRemoteCommands=1

#Habilita log dos comandos remotos
LogRemoteCommands=1

#Endereço IP do servidor Zabbix-Server
Server=192.168.0.1
```

```
#Habilita porta que o agente irá ouvir  
ListenPort=10050
```

```
#Define um nome para o Host, este deverá ser informado ao criar um Host  
no frontend do Zabbix, caso esteja errado o monitoramento não irá ocorrer
```

```
Hostname=Zabbix Server
```

```
#Habilitando o serviço Zabbix-server.service na inicialização do sistema  
systemctl enable Zabbix-server.service
```

```
#Verificando Status do serviço Zabbix_server.service  
systemctl status Zabbix-server.service | grep Active
```

```
#Habilitando o serviço Zabbix_agentd na inicialização do sistema  
systemctl enable Zabbix-agent.service
```

```
#Iniciando o serviço Zabbix_agentd  
systemctl start Zabbix-agent.service
```

```
#Verificando Status do serviço Zabbix_agent.service  
systemctl status Zabbix-agent.service | grep Active
```

```
#Habilitando o serviço Zabbix-java-gateway.service na inicialização do  
sistema
```

```
systemctl enable Zabbix-java-gateway.service
```

```
#Iniciando o serviço Zabbix-java-gateway.service  
systemctl start Zabbix-java-gateway.service
```

```
#Verificando Status do serviço Zabbix-java-gateway.service  
systemctl status Zabbix-java-gateway.service | grep Active
```

```
#Verificando se os serviços foram habilitados  
systemctl list-unit-files --type service | grep Zabbix
```

## 17.8. AJUSTANDO O FRONTEND DO ZABBIX

Por ter escolhido a instalação via pacotes, não haverá necessidade de muitas configurações para o frontend. Basta editar o arquivo de configuração do apache para o Zabbix frontend que está localizado no diretório / etc/php.ini.

```
#Digite o comando  
vi /etc/php.ini
```

Utilize no caso do editor vim/vi o comando /(nome da palavra) para realizar a busca de uma palavra desejada, evitando ter que ficar lendo o enorme arquivo de configuração do php.

#Pode ser que haja alguma linha comentada neste caso remova a; e ajuste de acordo com as instruções abaixo

```
max_execution_time 300  
post_max_size 16M  
max_input_time 300
```

Antes  
; date.timezone

Depois  
date.timezone = America/Sao\_Paulo

## 17.9. SERVIÇOS HTTPD

```
#Habilitando o serviço httpd.service na inicialização do sistema  
systemctl enable httpd.service
```

```
#Iniciando o serviço httpd.service  
systemctl start httpd.service
```

```
#Verificando Status do serviço httpd  
systemctl status httpd.service | grep Active
```

```
#Verificando se o serviço foi habilitado  
systemctl list-unit-files --type service | grep httpd
```

## 17.10. SERVIÇOS DE FIREWALL

#Liberando acesso pela interface web na porta http e https, junto com as portas usadas pelo Zabbix server e agente 10050 e 10051 e as portas usadas pelo snmp 25.

```
firewall-cmd --permanent --zone=public --add-service=http  
firewall-cmd --permanent --zone=public --add-service=https  
firewall-cmd --permanent --zone=public --add-service=mysql  
firewall-cmd --permanent --zone=public --add-port=10050/tcp  
firewall-cmd --permanent --zone=public --add-port=10050/udp  
firewall-cmd --permanent --zone=public --add-port=10051/tcp  
firewall-cmd --permanent --zone=public --add-port=10051/udp  
firewall-cmd --permanent --zone=public --add-port=25/tcp  
firewall-cmd --permanent --zone=public --add-port=25/udp
```

```
#Validando as configurações do Firewalld reiniciando o serviço  
systemctl restart firewalld.service
```

#Reinicie o Servidor

reboot

É obrigatório reiniciar o servidor para validar as configurações efetuadas nos passos anteriores. Agora já será possível acessar o servidor do Zabbix Server pelo navegador e finalizar sua configuração.

## 17.11. CONFIGURAÇÃO NO NAVEGADOR

Após a reinicialização do Zabbix Server, será possível acessar a ferramenta através de um navegador. Abra qualquer navegador e acesse a url: 192.168.0.1/Zabbix e será exibida as telas de boas-vindas como na Figura 38.



Figura 38 Tela de Boas Vindas do Zabbix

A Figura 39 mostra, caso o processo de instalação do Zabbix server e a configuração do frontend estejam corretas estará OK para a próxima etapa, note que as configurações que fizemos no php.ini estão conforme o necessário.

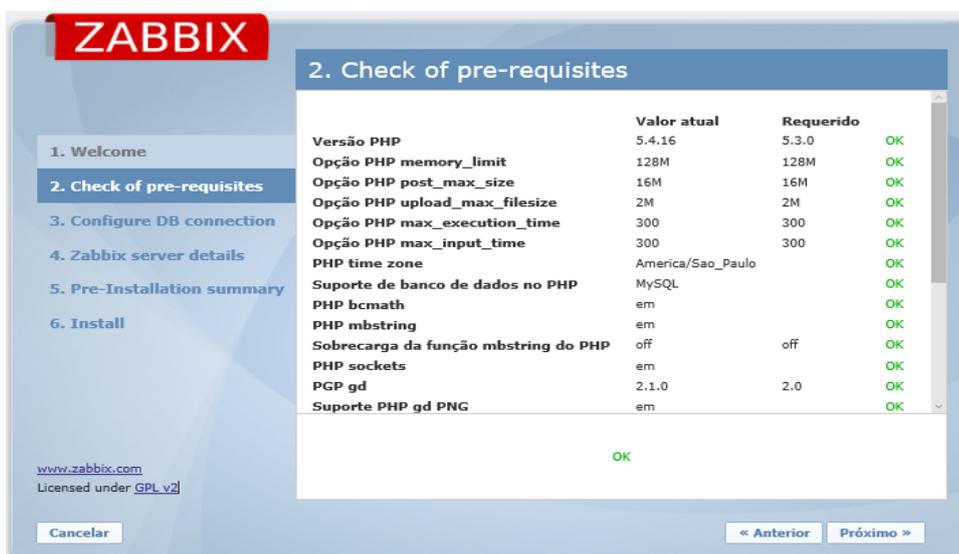


Figura 39 Checagem de Pré Requisitos

Como apresenta a Figura 40, aqui será feita a configuração da conexão com o banco de dados, aqui deverá ser informado em host do banco de dados o IP do servidor de banco de dados (192.168.180.2) o nome do banco criado (Zabbixdb) o usuário (Zabbixuser) e a senha (z@bbixdb) após inserir os parâmetros basta clicar em test connection e se estiver tudo correto receberá um OK e poderá prosseguir.



Figura 40 Configuração do Banco de Dados

A Figura 41 mostra a etapa em que deverá ser informado o IP do host (192.168.0.1) ou o próprio endereço de loopback (127.0.0.1), a porta 10051 e o nome que foi definido no Zabbix agente.conf ZabbixServer que irá funcionar da mesma forma.

**ZABBIX**

### 4. Zabbix server details

Please enter host name or host IP address and port number of Zabbix server, as well as the name of the installation (optional).

**Host**

**Porta**

**Nome**

[www.zabbix.com](http://www.zabbix.com)  
Licensed under [GPL v2](#)

Figura 41 Detalhes do ZabbixServer

A Figura 42 apresentada o resumo da instalação e configuração que foram realizadas na etapa passada do banco de dados e dos dados do Servidor Zabbix

**ZABBIX**

### 5. Pre-Installation summary

Please check configuration parameters.  
If all is correct, press "Next" button, or "Previous" button to change configuration parameters.

<b>Tipo de banco de dados</b>	MySQL
<b>Servidor de banco de dados</b>	192.168.0.2
<b>Porta do banco de dados</b>	padrão
<b>Nome do banco de dados</b>	zabbixdb
<b>Usuário do banco de dados</b>	zabbixuser
<b>Senha do banco de dados</b>	*****
<b>Servidor Zabbix</b>	192.168.0.1
<b>Porta do servidor Zabbix</b>	10051
<b>Nome do servidor Zabbix</b>	ZabbixServer

[www.zabbix.com](http://www.zabbix.com)  
Licensed under [GPL v2](#)

Figura 42 Resumo da Instalação

Se tudo estiver correto será apresentado uma tela igual a Figura 43, esta irá realizar a última configuração necessária para o Zabbix Server entrar em funcionamento. Clique em Fim.

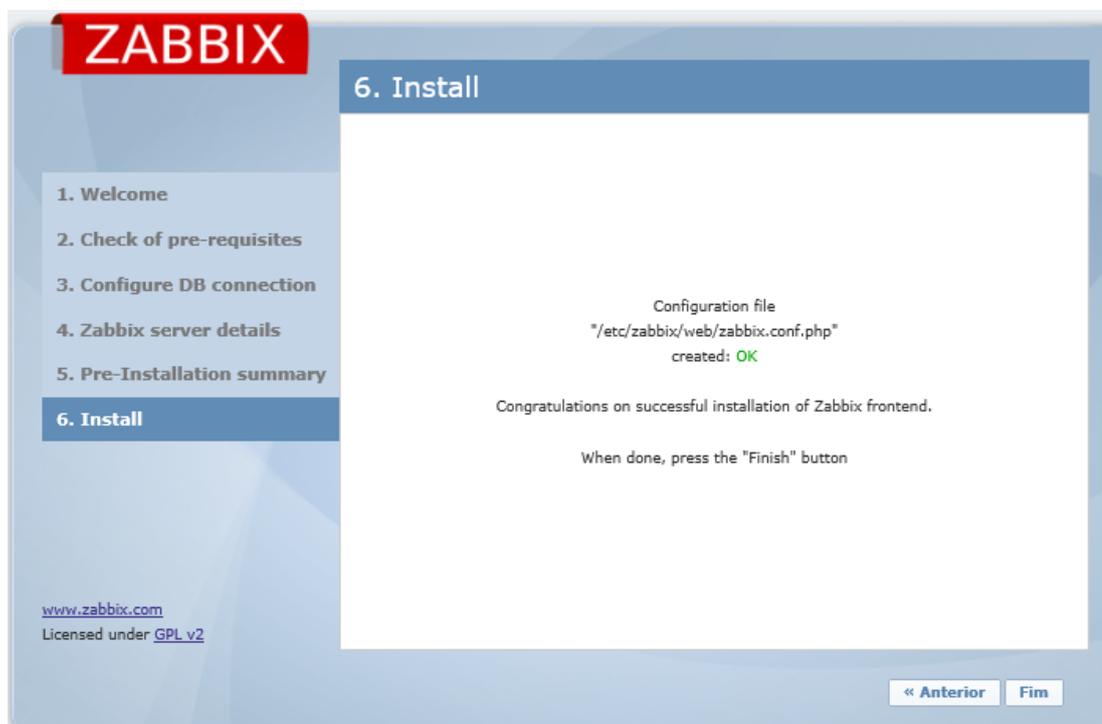


Figura 43 Finalização da configuração no navegador

A Figura 44 apresenta a tela principal do Zabbix, o Dashboard, um quadro geral de informações de tudo o que ocorre com o Zabbix, composto por portlets, componentes independentes que interagem entre si dentro de uma aplicação maior, sendo possível os reorganizar, esconder e configurar da forma que o administrador desejar. Abaixo segue alguns dos portlets compostos no Dashboard do Zabbix.

The screenshot shows the Zabbix web interface. The main navigation bar includes 'Monitoring', 'Inventory', 'Reports', 'Configuration', and 'Administration'. Below this, there are tabs for 'Dashboard', 'Overview', 'Web', 'Latest data', 'Triggers', 'Events', 'Graphs', 'Screens', 'Maps', 'Discovery', and 'IT services'. The 'PERSONAL DASHBOARD' section contains several portlets: 'Favourite graphs', 'Favourite screens', and 'Favourite maps'. The 'Status of Zabbix' portlet is the focus, showing a table of parameters and their values.

Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Number of hosts (enabled/disabled/templates)	39	1 / 0 / 38
Number of items (enabled/disabled/not supported)	62	57 / 0 / 5
Number of triggers (enabled/disabled [problem/ok])	41	41 / 0 [0 / 41]
Number of users (online)	2	1
Required server performance, new values per second	0.83	-

Updated: 22:24:12

The 'System status' portlet shows a table with columns: Host group, Disaster, High, Average, Warning, Information, Not classified. The 'Zabbix servers' row shows 0 in all categories.

The 'Host status' portlet shows a table with columns: Host group, Without problems, With problems, Total. The 'Zabbix servers' row shows 1 Without problems, 0 With problems, and 1 Total.

Figura 44 Dashboard Zabbix

A Figura 45 a acima apresenta o portlet Status do Zabbix, que apresenta o status de seu serviço, a quantidade de hosts, que são os computadores e dispositivos na rede, que podem estar habilitados ou desabilitados. Apresenta a quantidade de itens que são os recursos a serem coletados, como memória, interface de rede e até serviços, como apache e mysql, também é apresentado seu quantitativo como habilitado e desabilitado e caso não seja suportado pelo Zabbix. Abaixo é apresentado as triggers, que são os alertas a serem configurados quando um determinado item coletar uma informação, como por exemplo se um determinado serviço está sem execução ou não, ao receber determinado estado uma trigger pode ser ativada.

Será abordado melhor sobre trigger nos próximos apêndices.

Parâmetro	Valor	Detalhes
Zabbix está rodando	Sim	192.168.180.4:10051
Quantidade de hosts (habilitados/desabilitados/templates)	66	24 / 0 / 42
Quantidade de itens (habilitados/desabilitados/não suportados)	273	259 / 0 / 14
Quantidade de triggers (habilitadas/desabilitadas [incidente/ok])	150	150 / 0 [4 / 146]
Número de usuários (online)	3	1
Desempenho requerido do servidor, novos valores por segundo	4.18	-

Atualizado: 01:00:17

Figura 45 Portlet Status do Zabbix

Abaixo do parâmetro Quantidade de Triggers, o Zabbix apresenta um sistema interno de usuários, onde é possível criar, editar, e alterar permissões de acesso a cada um. E como último parâmetro é apresentado um contador de desempenho, onde mostrará, o desempenho requerido pelo Zabbix para a execução de suas tarefas em valores por segundo.

A Figura 46 é a portlet que apresenta informações a respeito do Status do Sistema Zabbix, aqui será listado todo o conjunto de Grupos de Host que estão no sistema e uma Tabela com as categorias das triggers e irá categorizar cada status de um host conforme sua trigger correspondente.

Status do sistema						
Grupo de hosts	Desastre	Alta	Média	Atenção	Informação	Não classificada
<a href="#">Cameras de Seguranca</a>	0	0	0	0	0	0
<a href="#">Discovered hosts</a>	0	0	4	0	0	0
<a href="#">Zabbix servers</a>	0	0	0	0	0	0

Atualizado: 00:17:17

Figura 46 Portlet Status do Sistema

Nesta portlet, Figura 47, mostra o Status do Host, o Zabbix irá apresentar todos os grupos de hosts presentes, e uma Tabela corresponde ao seu quantitativo de incidentes ocorridos ou não.

Status do host			
Grupo de hosts	Sem incidentes	Com incidentes	Total
<a href="#">Cameras de Seguranca</a>	19	0	19
<a href="#">Discovered hosts</a>	0	2	2
<a href="#">Zabbix servers</a>	4	0	4

Atualizado: 01:15:18

Figura 47 Portlet Status do Host

A Figura 48 apresenta a portlet últimos 20 incidentes, mostra uma lista com os últimos incidentes ocorridos, se algum serviço não responde ou se algum host estiver off-line; vai depender da configuração das triggers. Ele reportará o Host que contém um incidente, tal como o assunto, se ele está fora de alcance ou um serviço não está em execução, tal como sua última alteração, que foi quando o Zabbix obteve sua última consulta de informações, o tempo que já aconteceu a ocorrência, alguma

informação complementar do problema, se houve algum reconhecimento por parte do administrador da rede e a ação tomada pelo Zabbix, que será visto nas próximas etapas.

Últimos 20 incidentes						
Host	Assunto	Última alteração	Idade	Informação	Reconhecido	Ações
WindowsHost	Zabbix agent on WindowsHost is unreachable for 5 minutes	<a href="#">28-08-2015 15:57:00</a>	2d 8h 20m		Não	3
WindowsJV	Zabbix agent on WindowsJV is unreachable for 5 minutes	<a href="#">28-08-2015 15:55:30</a>	2d 8h 21m		Não	3
WindowsHost	WindowsHost is unavailable by ICMP	<a href="#">28-08-2015 15:55:16</a>	2d 8h 22m		Não	3
WindowsJV	WindowsJV is unavailable by ICMP	<a href="#">28-08-2015 15:53:20</a>	2d 8h 23m		Não	3

4 de 4 incidentes exibidos

Figura 48 Portlet Últimos 20 Incidentes

Essa portlet Monitoramento web, Figura 49, não irá aparecer no dashboard logo que acessar o Zabbix, será necessário configurar o monitoramento web, que será apresentado futuramente. Quando configurado esse monitoramento, a portlet irá mostrar o grupo de host que está realizando a monitoração web, seu status, e se há algum monitoramento que não foi reconhecido.

Monitoramento web			
Grupo de hosts	Ok	Falhou	Desconhecido
<a href="#">Zabbix servers</a>	2	0	0

Atualizado: 00:17:17

Figura 49 Portlet Monitoramento Web

A Figura 50 também não vem por padrão no dashboard. É necessário configurar o serviço de auto busca para a mesma estar visível, nela será relatado quais hosts dentro das regras criadas estão ativos ou não e será melhor apresentada no decorrer do trabalho.

Status autobusca		
Regra de autobusca	Online	Fora
<a href="#">Rede TI</a>	16	9
<a href="#">Rede Wifi ADM</a>	2	9
<a href="#">Telefones</a>	25	1

Figura 50 Portlet Status Auto Busca

## 18. APÊNDICE C - INSTALAÇÃO E CONFIGURAÇÃO ZABBIX PROXY

O processo de instalação e configuração do Zabbix Proxy será baseado no processo criado por Déo (2015), e adaptado para o pleno funcionamento deste trabalho.

O servidor deverá estar conectado à Internet, na mesma rede que os outros servidores e atualizado com os pacotes mais recentes. Por questão de organização todo o processo de instalação será efetuado na pasta install, criada anteriormente no diretório raiz /.

```
#Para acessar a pasta e iniciar o processo de download das dependências.  
cd /install
```

#Será necessário instalar as dependências para que o zabbix proxy consiga realizar as coletas corretamente, utilize os comandos abaixo para realizar o processo de instalação.

```
#Instalação do banco de dados que será utilizado pelo zabbix proxy.  
yum -y install sqlite3 sqlite-devel
```

#Instalação da dependência do snmp, responsável pela coleta de informações via snmp.

```
yum -y install net-snmp net-snmp-devel net-snmp-utils net-snmp-libs
```

#Instalação do pacote traceroute, responsável por traçar rotas e apresentar todo seu caminho.

```
yum -y install gcc gcc-devel gcc-c++ curl curl-devel mlocate traceroute
```

#Instalação do pacote de bibliotecas, responsável pelo funcionamento do zabbix.

```
yum -y install libssh2 libssh2-devel openssh-server openssh-clients install  
libcurl curl libcurl-devel
```

#Instalação do WGET, necessário para instalar outros pacotes de outro tipo  
yum install wget

#Abaixo utilizando o wget será realizado o download do fping, o mesmo instalado no Zabbix Server.

```
wget http://pkgs.repoforge.org/fping/fping-3.10-1.el7.rf.x86_64.rpm
```

#Instalação do pacote do fping

```
rpm -ivh fping-3.10-1.el7.rf.x86_64.rpm
```

#Agora será realizado o download dos pacotes mais atuais do zabbix, a versão 2.4.6

```
wget http://sourceforge.net/projects/zabbix/files/ZABBIX%20Latest%20Stable/2.4.6/zabbix-2.4.6.tar.gz
```

#Crie a conta do usuário zabbix no sistema.

```
adduser zabbix -s /bin/false
```

#Descompacte os pacotes do zabbix

```
tar xzvf zabbix-*.tar.gz
```

#Acesse o diretório do conteúdo descompactado

```
cd zabbix-*
```

#Agora dentro da pasta do zabbix, será instalado a base de dados do sqlite3, o banco de dados escolhido para armazenar as informações que o zabbix proxy coletar. Acesse a pasta do sqlite3

```
cd database /sqlite3
```

#Crie a pasta do sqlite em /var/lib/sqlite

```
mkdir /var/lib/sqlite
```

#Será necessário criar o Schema para o Zabbix Proxy da mesma forma que foi criado para o Zabbix Server, o processo também pode levar um pouco de tempo, dando a impressão de que o sistema travou.

```
sqlite3 /var/lib/sqlite/zabbix.db < schema.sql
```

```
#Dê permissão para o zabbix acessar o sqlite  
chown -R zabbix:zabbix /var/lib/sqlite
```

#Com a base de dados criada agora falta compilar os pacotes do Zabbix Proxy e configurar o ambiente, junto com a compilação dos fontes das dependências instaladas.

```
cd ../../  
./configure --enable-proxy --enable-agent --with-net-snmp --with-sqlite3 --  
with-libcurl
```

```
#Agora falta realizar a instalação.  
make install
```

## 18.1. CONFIGURAÇÃO PROXY AGENTD.CONF

#O Zabbix Proxy já está instalado, só resta realizar a configuração do servidor e agente. Edite o arquivo de configuração do agente do proxy localizado em /usr/local/etc/zabbix\_agentd.conf

```
vi /usr/local/etc/zabbix_agentd.conf
```

#No arquivo poderá conter algumas linhas comentadas, será necessário descomenta-las e realizar as alterações necessárias.

```
#Caminho do local do pid do agente  
PidFile=/tmp/zabbix_agentd.pid
```

```
#Caminho de localização do arquivo de log do agente  
LogFile=/var/log/zabbix/zabbix_agentd.log
```

```
#Tamanho de armazenamento do arquivo de log  
LogFileSize=2
```

```
#Tipo de informação que será armazenada no log  
DebugLevel=3
```

```
#Habilita comandos remotos  
EnableRemoteCommands=1
```

```
#Habilita log dos comandos remotos  
LogRemoteCommands=1
```

```
#Endereço IP do servidor do Zabbix Server que irá coletar os dados do  
proxy
```

```
Server=192.168.0.1
```

```
#Porta em que o agente irá ouvir  
ListenPort=10050
```

```
#Nome do host que deverá ser cadastrado no frontend do Zabbix Server  
Hostname=ZabbixProxy
```

## 18.2. CONFIGURAÇÃO PROXY SERVER.CONF

Com o agente já foi configurado será possível que o Zabbix Server colete as informações de nosso servidor proxy. Foi configurado o arquivo de configurações do Zabbix Proxy localizado em /usr/local/etc

#Edite o arquivo zabbix\_proxy.conf usando o editor de texto vi ou qualquer que tenha preferência.

```
vi /usr/local/etc/zabbix_proxy.conf
```

#Determine o modo em que o zabbix irá trabalhar ativo ou passivo. 0 para ativo.

```
ProxyMode=0
```

#Insira o IP do servidor zabbix server

```
Server=192.168.0.1
```

#Determine o nome do zabbix proxy, deverá ser informado quando for cadastrado no frontend do zabbix server

```
Hostname=ZabbixProxy
```

#Determine o nome do banco de dados, como está sendo utilizado o sqlite3 insira o caminho do banco

```
DBName=/var/lib/sqlite/zabbix.db
```

#Comente a linha que representa o usuário do banco

```
#DBUser=root
```

#Comente a linha que corresponde a senha do banco.

```
#DBPassword=
```

#Determine a quantidade de informação que será armazenada nos logs do zabbix proxy

```
DebugLevel=3
```

#Determina a localização do PID do zabbix proxy

```
PidFile=/tmp/zabbix_proxy.pid
```

#Define o local de armazenamento do arquivo de log do zabbix proxy

```
LogFile=/tmp/zabbix_proxy.log
```

#Determine o tamanho do arquivo de logs gerado

```
LogFileSize=100
```

```
#Determine a quantidade de tentativa de conexões  
Timeout=3
```

```
#Determine o tamanho do armazenamento do buffer local do Zabbix Proxy  
ProxyLocalBuffer=168
```

```
#Determine o tamanho do buffer offline do proxy  
ProxyOfflineBuffer=168
```

```
#Determine a taxa de atualização do sistema interno  
HeartbeatFrequency=60
```

```
#Configure a frequência de atualização do servidor  
ConfigFrequency=900
```

Todos os processos básicos necessários para o funcionamento do Zabbix Proxy e Agent estão configurados, só resta habilitá-los para iniciar junto com o sistema e abrir as portas do firewall.

```
#Utilize os comandos para iniciar o agente e o serviço do proxy  
zabbix_agentd  
zabbix_proxy
```

```
#Verifique se os serviços foram iniciados e estão em execução  
ps aux | grep zabbix
```

```
#Copie os daemons do Zabbix e ajuste as permissões para sua execução  
cp /install/zabbix-2.4.6/misc/init.d/fedora/core/zabbix_agentd /etc/init.d/  
cp /install/zabbix-2.4.6/misc/init.d/fedora/core/zabbix_server /etc/init.d/
```

#Como pode se observar foi copiado o daemon do Zabbix Server, mas ele é igual tanto para o server, quanto para o proxy, no entanto será necessário mudar o nome do arquivo Zabbix\_Server para Proxy\_Server e alterar um parâmetro no arquivo.

#Mudar o nome do arquivo

```
mv /etc/init.d/zabbix_server /etc/init.d/zabbix_proxy
```

#Editar o arquivo que agora contém o nome zabbix\_proxy e alterar o nome a linha que contenha o BINARY\_NAME=zabbix\_server alterando para BINARY\_NAME=zabbix\_proxy

#Dê permissão de execução para o fping apartir do zabbix

```
chown root:zabbix /usr/sbin/fping*
```

```
chmod 710 /usr/sbin/fping*
```

```
chmod ug+s /usr/sbin/fping
```

#Inicialize os novos daemons do serviço do Zabbix

```
/etc/init.d/zabbix_proxy start
```

```
/etc/init.d/zabbix_agentd start
```

#Valide se os processos do Zabbix estão rodando:

```
ps -eux | grep -i zabbix
```

#Adicione o "zabbix\_proxy" e "zabbix\_agentd" para iniciar automaticamente:

```
chkconfig --add zabbix_agentd
```

```
chkconfig --add zabbix_proxy
```

```
chkconfig --level 35 zabbix_agentd on
```

```
chkconfig --level 35 zabbix_proxy on
```

#Verifique os serviços que estão para inicializar automaticamente:

```
chkconfig --list | grep zabbix
```

#Libere as portas 10050, 10051 e 10052 no iptables, para que as comunicações tenham êxito:

```
firewall-cmd --permanent --zone=public --add-port=10050/tcp firewall-cmd -  
-permanent --zone=public --add-port=10050/udp
```

```
firewall-cmd --permanent --zone=public --add-port=10051/tcp firewall-cmd -  
-permanent --zone=public --add-port=10051/udp
```

```
firewall-cmd --permanent --zone=public --add-port=25/udp
```

```
firewall-cmd --permanent --zone=public --add-port=25/tcp
```

#Reinicie o serviço de firewall

```
systemctl restart firewalld.service
```

#Para finalizar configure o SeLinux em modo permissivo.

```
vi /etc/sysconfig/selinux
```

```
SELINUX=permissive
```

### 18.3. CRIAÇÃO DO PROXY NO FRONTEND

Agora está tudo configurado corretamente, basta reiniciar o servidor para que todas as regras sejam aplicadas, e logo após, cadastrar o novo proxy no frontend do Zabbix Server.

Para realizar a integração do Zabbix Proxy com o Zabbix Server basta, realizar o login no Zabbix Server, através do endereço IP do servidor zabbix 192.168.0.1/zabbix. Após o login acesse o menu Administração/Proxies e clique no botão do canto direito superior Criar Proxy. Na tela que abrir preencha conforme a Figura 51.

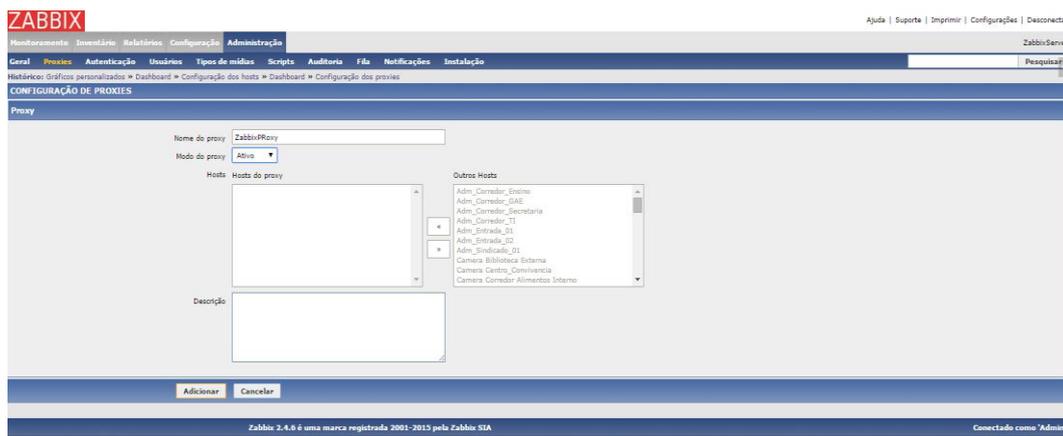


Figura 51 Zabbix Proxy Criando Proxy

Após a criação do Proxy, com todas as configurações realizadas com sucesso, será possível ver quando foi a última checagem do Proxy através do Zabbix Server conforme a Figura 52.

CONFIGURAÇÃO DE PROXIES						
Proxies						
Mostrando 1 para 2 de 2 encontrados						
<input type="checkbox"/>	Nome ↑	Modo	Última vez visto (idade)	Contagem de hosts	Contagem de itens	Performance requerida (vps)
<input type="checkbox"/>	<a href="#">ZabbixProxy</a>	Ativo	7s	19	19	0.63

Figura 52 Zabbix Proxy Atividade Proxy

Com o proxy criado, será necessário criar um host para ele, acesse o menu Configuração/Host e no canto superior direito, Criar Host e preencha as informações conforme a Figura 53.

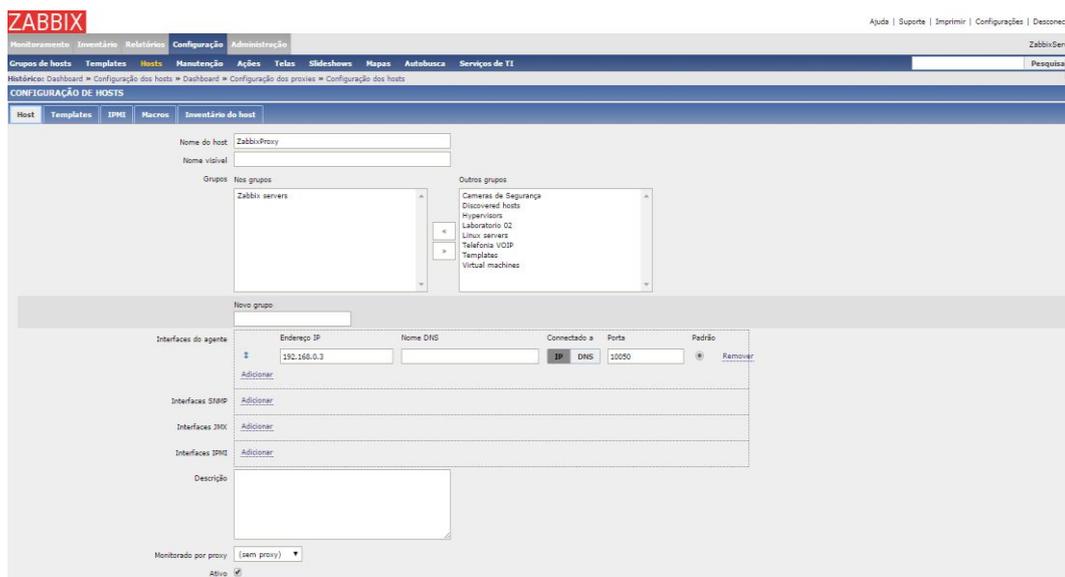


Figura 53 Zabbix Proxy Criando Host Proxy

Antes de salvar o host, clique na aba Templates ou se tiver salvo o novo Host, clique no mesmo e em Templates, configure conforme a Figura 54.

Será utilizado dois Templates padrões do Zabbix, responsáveis por coletar os recursos do Host Criado, o Zabbix Proxy.

- Template App Zabbix Proxy – Responsável por coletar informações de desempenho do proxy
- Template Linux OS – Responsável por coletar informações como memória ram, hd, interfaces de rede, swap entre outras.



Figura 54 Zabbix Proxy Template

Após salvar o novo Host com os Templates, em alguns instantes será possível notar que na coluna Disponibilidade localizada em Host na aba Configurações estará o Host Criado, ZabbixProxy com um Z em verde, simbolizando que a criação do Host do proxy foi feita com sucesso e o Zabbix Proxy/Agent está funcionando corretamente conforme a Figura 55.

<input type="checkbox"/>	ZabbixProxy	Aplicações (12)	Itens (71)	Triggers (40)	Gráficos (15)	Autobusca (2)	Web (2)	192.168.0.3:10050	Template App Zabbix Proxy, Template OS Linux (Template App Zabbix Agent)	Ativo	
--------------------------	-------------	-----------------	------------	---------------	---------------	---------------	---------	-------------------	--	-------	--

Figura 55 Zabbix Proxy Status

## 18.4. INSTALAÇÃO DO SEGUNDO SERVIDOR PROXY.

Como citado anteriormente em nosso trabalho constará a implantação de dois servidores Proxys, realizando a divisão de carga dos servidores e podendo separar as atribuições do que será monitorado a cada um.

Para a configuração do segundo proxy, ProxyII será necessário realizar os mesmos procedimentos para a instalação e configuração do primeiro Proxy criado, sendo necessário apenas adequar algumas configurações para o pleno funcionamento do novo sistema. Tais como:

- Endereço IP conforme na Figura2 deste trabalho.
- Na configuração a ser realizada no agente do proxy, coloque em Hostname o nome deste servidor, ZabbixProxyII, lembrando que esse nome deverá ser informado no Frontend do Zabbix para que funcione corretamente.
- No arquivo de configuração zabbix\_proxy.conf altera a linha do Hostname da mesma forma que no passo anterior.
- Na criação do Proxy e do Host no Frontend deve-se adequar conforme o Hostname criado para este servidor.

## **19. APÊNDICE D - SISTEMAS DE ALERTA VIA E-MAIL E WHATSAPP**

Um dos pontos fortes que a ferramenta Zabbix apresenta é o seu sistema de notificação, ele consegue notificar o Administrador da rede através de diversos recursos, sejam ele via SMS, e-mail e agora é possível também via whatsapp. O whatsapp é um aplicativo de mensagem instantânea que utiliza a lista telefônica do usuário e identifica o usuário que os utilizam, possibilitando a comunicação entre eles através da Internet.

Este trabalho contemplará a implantação do sistema de alerta via e-mail e whatsapp, optando não por utilizar o sistema de envio via SMS, pois o Campus-Morrinhos localiza-se em um local que não possui qualidade de sinal telefônico, tornando assim esse meio de notificação inviável e falho para a solução de problemas. Como atualmente a infraestrutura do Campus-Morrinhos possui redes com meio não guiado que cobrem quase toda sua extensão torna-se efetivo o uso do sistema de alerta via e-mail e whatsapp.

Apesar das duas formas de notificações apresentarem a mesma característica que é a utilização da Internet para a transmissão de suas informações, a decisão de implantação de cada ferramenta foi escolhida por suas características específicas. O e-mail por sua vez pode ser um pouco mais lento em relação ao whatsapp, vendo que pode não ser todo mundo que sincroniza os e-mails com um dispositivo móvel por exemplo, porém a segurança no armazenamento das informações mostra-se mais efetivas em relação ao whatsapp, pois seu sistema de armazenamento é em nuvem e independente do local de acesso às informações são encontradas, podendo ser armazenadas como uma forma de documentação também.

O whatsapp por sua vez se torna mais versátil em relação ao e-mail, trazendo um sistema de apresentação de imagem mais ágil do que o e-mail, porém pode apresentar falha no armazenamento dessas informações, uma vez que a conta é vinculada a um smartphone e o mesmo pode apresentar problemas, ocorrendo a perda dessas informações que podem não conter um backup. Assim utilizando os dois meios de notificações pensando em possíveis falhas e em uma forma rápida e segura de visualizar e armazenar as informações relatadas pelo Zabbix.

## 19.1. SISTEMA DE ALERTA VIA E-MAIL

O processo de instalação e configuração do sistema de alerta via e-mail foi adaptado do artigo de Martelotta. (2015) e adequado para o pleno funcionamento em nosso ambiente.

Nesse processo de instalação e configuração criou-se uma conta no gmail, que será utilizada para enviar os e-mails para o administrador.

## 19.2. CONFIGURAR O POSTFIX

Com o CentOS e o Zabbix devidamente instalados e configurados, instale o Postfix e as dependências necessárias:

```
yum install cyrus-sasl cyrus-sasl-devel cyrus-sasl-gssapi cyrus-sasl-md5  
cyrus-sasl-plain mutt postfix
```

#Em seguida, entre no diretório de configuração do Postfix, faça o backup do arquivo de configuração:

```
cd /etc/postfix/  
mv main.cf main.cf.old
```

#Crie um novo arquivo de configuração para Postfix:

```
vi main.cf
```

#Nele, coloque somente as seguintes linhas:

```
SMTP relayhost  
relayhost = [smtp.gmail.com]:587  
TLS Settings  
smtp_tls_loglevel = 1
```

```
smtp_use_tls = yes
smtpd_tls_received_header = yes
```

```
#TLS
```

```
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
smtp_sasl_tls_security_options = noanonymous
```

#Crie o arquivo "sasl\_passwd", contendo o servidor SMTP do Google e a conta que será utilizada para envio dos e-mails.

```
#Dessa forma:
```

```
vi sasl_passwd
```

```
[smtp.gmail.com]:587 zabbixifgoiano@gmail.com: senha do e-mail
```

#A conta " zabbixifgoiano @gmail.com", eu criei exclusivamente para ser utilizado pelo Postfix, que o Zabbix estará utilizando. Vocês verão como, na próxima etapa.

Já em "Senha", coloque a senha da conta do Gmail que você escolheu para enviar os e-mails.

#Em seguida, rodamos o comando "postmap" no arquivo "sasl\_passwd" e no "main.cf", para que eles possam ser reconhecidos e utilizados pelo Postfix:

```
postmap /etc/postfix/sasl_passwd; postmap /etc/postfix/main.cf
```

```
#Reinicie o serviço do Postfix:
```

```
service postfix restart
```

#Pronto, agora você está com tudo certo para enviar e-mails através do shell. Faça um teste:

```
echo 'Teste.' | mutt -s 'Teste de envio pelo shell' seu_e-mail@gmail.com
```

#O e-mail "seu\_e-mail@gmail.com", é o que receberá o teste. Ou seja, o e-mail será enviado de "zabbixteste-mail@gmail", para "seu\_e-mail@gmail.com". Então, ao seguir as etapas, não esqueça de colocar seu e-mail.

#Cheque a caixa de entrada do seu e-mail, ou o arquivo de log "/var/log/maillog".

#Verificando através da saída do arquivo "/var/log/maillog" da minha máquina de teste (perceba onde tem "status=sent"):

```
tail -f /var/log/maillog
```

```
Jun  1 18:01:29 zabbix-server postfix/smtp[3304]: D902C41349:
to=<prbamartelott@gmail.com>, relay=smtp.gmail.com[74.125.134.108]:587,
delay=7.8, delays=2/0.14/3.6/2, dsn=2.0.0, status=sent (250 2.0.0 OK 1370120491
y24sm78365951yhn.20 - gsmt)
```

```
Jun  1 18:01:30 zabbix-server postfix/qmgr[3292]: D902C41349: removed
```

Se em "status" estiver "status=sent", o e-mail foi enviado com sucesso e acabam aqui as configurações necessárias para enviar seus e-mails através Postfix, usando o Gmail.

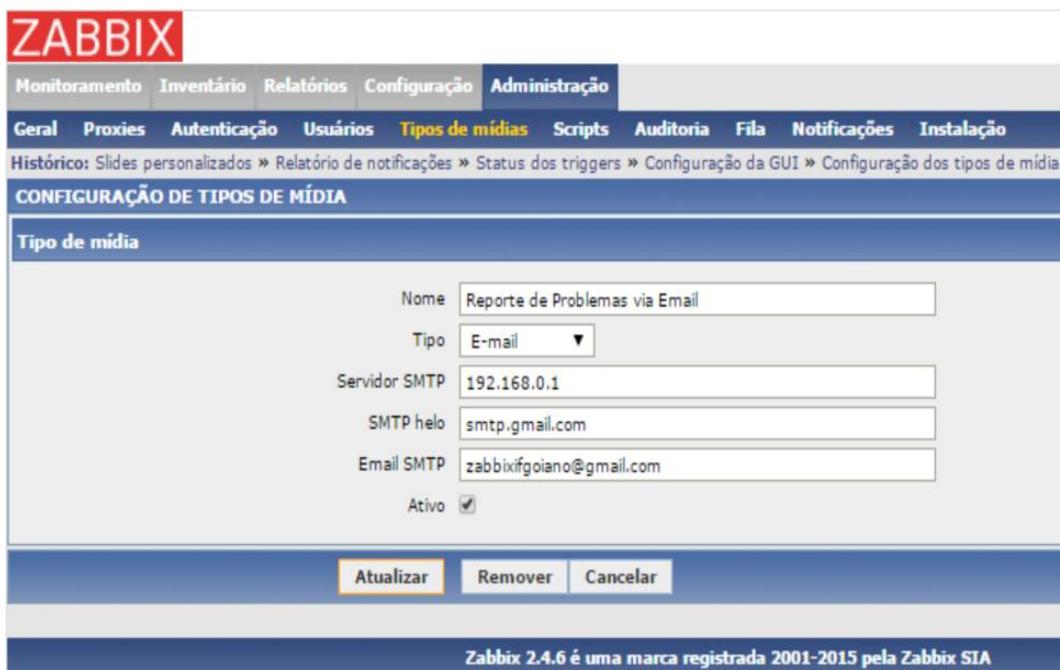
## 19.3. CONFIGURAÇÃO DO E-MAIL NO FRONTEND DO ZABBIX

Ao logar como um usuário com permissões de Administrador do Zabbix acessa o menu Administração > Tipos de Mídias > e-mail, conforme a Figura 56.

Agora será necessário preencher os dados conforme abaixo:

- Tipo: Tipo de notificação no caso e-mail
- Servidor: O IP de onde será enviado o e-mail, no caso o Servidor Zabbix, com IP 192.168.0.1
- SMTP Helo: Informe o servidor de smtp, no caso é utilizado o do gmail: smtp.gmail.com
- E-mail SMTP: A conta de e-mail que enviará os e-mails, a mesma que foi criada anteriormente e realizado os testes de envio.

A configuração deverá ficar conforme a Figura 56.



The screenshot shows the Zabbix web interface. At the top, the ZABBIX logo is visible. Below it, there is a navigation menu with tabs for 'Monitoramento', 'Inventário', 'Relatórios', 'Configuração', and 'Administração'. The 'Administração' tab is selected, and within it, the 'Tipos de mídias' sub-tab is active. A breadcrumb trail reads: 'Histórico: Slides personalizados » Relatório de notificações » Status dos triggers » Configuração da GUI » Configuração dos tipos de mídia'. The main heading is 'CONFIGURAÇÃO DE TIPOS DE MÍDIA'. Underneath, there is a section titled 'Tipo de mídia'. The form contains the following fields: 'Nome' (Reporte de Problemas via Email), 'Tipo' (E-mail), 'Servidor SMTP' (192.168.0.1), 'SMTP helo' (smtp.gmail.com), and 'Email SMTP' (zabbixifgoiano@gmail.com). There is also a checked 'Ativo' checkbox. At the bottom of the form, there are three buttons: 'Atualizar', 'Remover', and 'Cancelar'. A footer at the very bottom states: 'Zabbix 2.4.6 é uma marca registrada 2001-2015 pela Zabbix SIA'.

Figura 56 Tipo de Mídia e-mail

Agora basta clicar em atualizar para finalizar o primeiro processo da configuração no *frontend*. Logo após é necessário vincular a mídia criada a um usuário dentro do Zabbix, para que o sistema dispare as notificações a esse usuário específico.

Como utilizaremos mais de um meio de notificação e mais de um usuário, foi criado um grupo para que facilitasse o envio de notificações aos usuários, evitando a necessidade de vincular o tipo de envio a cada usuário, tendo que, apenas configurar, para enviar ao grupo. Para isso acesse o menu Administração > Usuários.

Na página de usuários clique no botão “Criar grupo de usuários” no canto direito superior e preencha como a Figura 57.

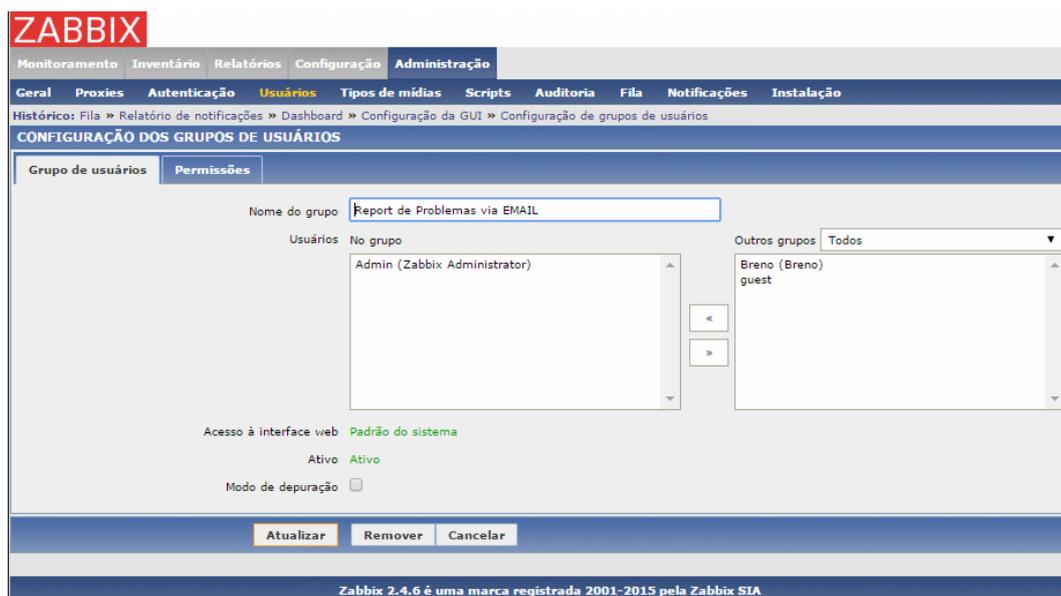


Figura 57 Criação do Grupo de Usuário de E-mail

Fonte: Autor

- Nome do grupo: Report de Problemas via e-mail;
- Usuários do Grupo: Para o grupo criado foi vinculado apenas o usuário Admin, que representa o Gerente de rede, porém é possível adicionar mais usuários a este grupo, de forma que todos eles recebam os e-mails de notificação;
- Para finalizar clique em Atualizar.

Com a mídia de e-mail configurada, e o grupo respectivo, só resta criar as ações, que serão responsáveis por executar o envio das notificações quando uma determinada situação ocorrer.

Para criar as ações é necessário acessar o menu Configuração > Ação. As ações, são responsáveis por executar determinadas tarefas caso ocorra algum disparo de uma *trigger* no sistema. Para criar uma ação basta clicar no botão no canto superior direito “Criar ação”.

Nas ações, Figura 58, poderá ser definido o que será apresentado no conteúdo da notificação, o Zabbix utiliza Macros, que são variáveis do sistema responsáveis por representar vários objetos.

The screenshot shows the Zabbix web interface for configuring an action. The navigation menu includes 'Monitoramento', 'Inventário', 'Relatórios', 'Configuração', and 'Administração'. The main content area is titled 'CONFIGURAÇÃO DE AÇÕES' and contains a form with the following fields and values:

- Nome:** Report problems to Zabbix administrators
- Assunto padrão:** {TRIGGER.STATUS}: {TRIGGER.NAME}
- Mensagem padrão:** Trigger: {TRIGGER.NAME}  
Trigger status: {TRIGGER.STATUS}  
Trigger severity: {TRIGGER.SEVERITY}  
Trigger URL: {TRIGGER.URL}  
Item values:
- Mensagem da recuperação:**
- Assunto da recuperação:** {TRIGGER.STATUS}: {TRIGGER.NAME}
- Mensagem da recuperação:** Trigger: {TRIGGER.NAME}  
Trigger status: {TRIGGER.STATUS}  
Trigger severity: {TRIGGER.SEVERITY}  
Trigger URL: {TRIGGER.URL}  
Item values:
- Ativo:**

Buttons at the bottom include 'Atualizar', 'Clonar', 'Remover', and 'Cancelar'. The footer text reads 'Zabbix 2.4.6 é uma marca registrada 2001-2015 pela Zabbix SIA'.

Figura 58 Criação das ações a serem notificadas via e-mail

Fonte: Autor

No conteúdo da notificação será apresentado:

- O Assunto da mensagem, contém o Status da Trigger, se é um problema ou se ela foi resolvida e o Trigger Name, que apresentará o nome da mesma;
- Na mensagem padrão apresentará o Nome da Trigger, seu status, sua severidade, que pode ser de Desastre, Alta, Média, Atenção, Informação e Url que poderá apresentar um link apontando para a mesma.

Abaixo tem a mensagem de recuperação, que será enviada quando o problema tiver resolvido e abaixo os mesmos dados apresentando as informações contidas na notificação. Clique em Atualizar para aplicar as configurações. Na próxima

aba “Condições”, é encontrado as operações necessárias para o Zabbix executar suas devidas ações.

Na Figura 59 temos a tela de Condições das Ações, ela define quando o Zabbix deverá executar essa ação a ser criada. Apresentando as seguintes condições:

The screenshot shows the Zabbix web interface for configuring actions. The main navigation bar includes 'Monitoramento', 'Inventário', 'Relatórios', 'Configuração', and 'Administração'. The sub-navigation bar includes 'Grupos de hosts', 'Templates', 'Hosts', 'Manutenção', 'Ações', 'Telas', 'Slideshows', 'Mapas', 'Autobusca', and 'Serviços de TI'. The breadcrumb trail is 'Histórico: Configuração dos grupos de hosts » Configuração de ações » Configuração dos templates » Configuração das triggers » Configuração de ações'. The main heading is 'CONFIGURAÇÃO DE AÇÕES'. Below it, there are three tabs: 'Ação', 'Condições', and 'Ações'. The 'Condições' tab is selected. The 'Tipo do cálculo' is set to 'E/OU'. The 'Condições' table lists five conditions (A-E) based on trigger severity levels, each with a 'Remover' link. Below the table is a 'Nova condição' form with a dropdown for 'Nome da trigger', a 'como' dropdown, and an input field. At the bottom, there are buttons for 'Atualizar', 'Clonar', 'Remover', and 'Cancelar'. The footer states 'Zabbix 2.4.6 é uma marca registrada 2001-2015 pela Zabbix SIA'.

Texto	Nome	Ação
A	Severidade da trigger = <i>Desastre</i>	<a href="#">Remover</a>
B	Severidade da trigger = <i>Alta</i>	<a href="#">Remover</a>
C	Severidade da trigger = <i>Média</i>	<a href="#">Remover</a>
D	Severidade da trigger = <i>Atenção</i>	<a href="#">Remover</a>
E	Severidade da trigger = <i>Informação</i>	<a href="#">Remover</a>

Figura 59 Criação das Condições das ações

Fonte: Autor

- Tipo de cálculo: O Zabbix irá executar uma operação booleana, podendo ser personalizada, E/OU, E e OU utilizando as condições definidas abaixo;
- Condições: O Zabbix apresenta diversas informações quanto aos tipos de condições, mas para o trabalho foi preferencial a utilização da condição Nome da Trigger igual a sua determinada severidade. Não sendo relevante neste momento a utilização de alguma outra condição.

Desta forma o Zabbix irá realizar a operação lógica A OU B OU C OU D OU E comparando todas as condições explicitadas abaixo, de forma que quando ocorrer qualquer disparo de uma trigger, será enviado uma notificação.

Clique em atualizar e acesse a aba “Ações”, conforme a Figura 60.

The screenshot shows the Zabbix configuration interface for creating an action. The interface is divided into several sections:

- Top Bar:** Tabs for 'Ação', 'Condições', and 'Ações'.
- Duration:** 'Duração padrão do passo da operação' set to 3600 (mínimo de 60 segundos).
- Table of Actions:**

Passos	Detalhes	Iniciar em	Duração (segundos)	Ação
1	Enviar mensagem para o grupo de usuários: Report de Problemas via EMAIL via Reporte de Problemas via Email	Imediatamente	Padrão	<a href="#">Editar</a> <a href="#">Remover</a>
- Details Form:**
  - Passo:** 1
  - De:** 1
  - Para:** 1 (0 - indefinidamente)
  - Duração do passo:** 0 (mínimo de 60 segundos, 0 - usar a ação padrão)
  - Tipo da operação:** Enviar mensagem
  - Enviar para grupos de usuários:**

Grupo de usuários	Ação
Reporte de Problemas via EMAIL	<a href="#">Remover</a>
  - Enviar para usuários:**

Usuário	Ação
<a href="#">Adicionar</a>	
  - Enviar apenas para:** Reporte de Problemas via Email
  - Mensagem padrão:**
  - Condições:**

Texto	Nome	Ação
<a href="#">Nova</a>		
- Bottom Bar:** Buttons for 'Atualizar', 'Clonar', 'Remover', and 'Cancelar'.

Figura 60 Criação das Ações

Nesta etapa é definida qual ação será tomada pelo Zabbix quando ocorrer qualquer uma das condições configuradas anteriormente. Clique no botão “Novo” para criar uma nova Ação.

O Zabbix trabalha com dois tipos de Operação, podendo enviar uma mensagem ou executar um comando remoto, como é necessário o envio de um e-mail foi definido que a operação será do tipo “enviar mensagem”. Logo após, é necessário definir se a notificação será enviada a um grupo de usuários ou a usuário apenas, como foi criado um grupo específico para e-mail, foi necessário escolher este grupo em Grupos de Usuários.

Abaixo será escolhido apenas para quem será enviado, sendo necessário marcar a mídia criada anteriormente. Reporte de problemas via e-mail e clicar em atualizar. Assim quando o Zabbix encontrar um disparo de uma trigger e o mesmo estabelecer as condições definidas anteriormente será enviado um e-mail.

Ao ter alguma trigger disparada, o Zabbix irá executar a ação configurada enviando um e-mail. O envio ocorre em duas etapas: uma de preparação e uma de conclusão da ação. Na Figura abaixo é possível notar que o Zabbix apresenta qual servidor está monitorando, o assunto da trigger, a última alteração do status da trigger e quando surgiu o problema, se tem algum reconhecimento do sistema e as ações, que serão executadas. Na Figura 61 abaixo apresenta um alerta de uma trigger de Desastre, sinalizada com a cor vermelha, e o quantitativo de ações a serem tomadas

na execução dessa trigger, a ação irá estar na cor laranja até que a mesma finalize a validação e passe para o outro status de enviado ou problema na execução da ação.

Últimos 20 incidentes						
Host	Assunto	Última alteração	Idade	Informação	Reconhecido	Ações
ZabbixProxy	Atividade do Site S2BIFGoiano.net	02-10-2015 09:57:34	4s		Não	1

Figura 61 Preparação do envio da notificação via e-mail

Quando a ação for executada, o Zabbix apresentará em verde o quantitativo de ações realizadas com sucesso e colocando o cursor sobre a ação apresentará a qual usuário ela foi enviada, os detalhes da ação e seu status, se foi enviado ou em vermelho se houver algum problema, conforme a Figura 62.

Últimos 20 incidentes						
Host	Assunto	Última alteração	Idade	Informação	Reconhecido	Ações
ZabbixProxy	Atividade do Site S2BIFGoiano.net	02-10-2015 09:57:34	16s		Não	1
Lab02PC28	Zabbix agent on Lab02PC28 is unreachable for 5 minutes	01-10-2015 22:52:00	11h 5m 50s		Não	3
Lab02PC18	Zabbix agent on Lab02PC18 is unreachable for 5 minutes	01-10-2015 16:41:30	17h 16m 20s		Não	3

Usuário	Detalhes	Status
Admin (Zabbix Administrator)	Reporte de Problemas via Email	Enviado

Figura 62 Envio de notificação via e-mail com sucesso.

Quando o Zabbix apresentar que a ação foi executada com sucesso, poderá observar na caixa de entrada do e-mail, que foi cadastrado para receber as notificações que terá um e-mail da conta criada, zabbixifgoiano@gmail.com, com o assunto, podendo ser Problem, no caso de um problema ou OK quando o problema for solucionado, e na mensagem constará todo o conteúdo definido na ação, como o nome da Trigger, seu status, gravidade e os valores do item, apresentando o item que identificou o problema, a Figura 63 mostra uma notificação de problema.

Filtrar por: Zabbix	Limpar filtros	PROBLEMA: Atividade do Site S2BIFGoiano.net
<input type="checkbox"/> zabbixifgoiano@gmail.com	03/10/2015	<p>zabbixifgoiano@gmail.com (zabbixifgoiano@gmail.com) Adicionar aos contatos 02/10/2015 Ações</p> <p>Para: joaovictor_b20@hotmail.com</p> <p>Trigger: Atividade do Site S2BIFGoiano.net            Trigger status: PROBLEMA            Trigger severity: Disaster            Trigger URL:</p> <p>Item values:</p> <ol style="list-style-type: none"> <li>Download speed for scenario "Servico de monitoramento do S2BIFgoiano.net.br". (ZabbixProxy:web.test.in[Servico de monitoramento do S2BIFgoiano.net.br,bps]): 0 Bps</li> <li>*UNKNOWN* (*UNKNOWN*:*UNKNOWN*): *UNKNOWN*</li> <li>*UNKNOWN* (*UNKNOWN*:*UNKNOWN*): *UNKNOWN*</li> </ol> <p>Original event ID: 1424028</p>
<input type="checkbox"/> zabbixifgoiano@gmail.com	03/10/2015	
<input type="checkbox"/> zabbixifgoiano@gmail.com	02/10/2015	
<input checked="" type="checkbox"/> zabbixifgoiano@gmail.com	02/10/2015	

Figura 63 e-mail de Notificação Trigger: Problema

E como a ação foi configurada para alertar também quando o problema for solucionado, será enviado um e-mail com status OK, conforme a Figura 64, apresentando as mesmas informações anteriormente. Porém não será apresentado no Dashboard, apenas o alerta será removido.

The screenshot displays a Zabbix notification interface. On the left, a list of notifications is shown, filtered by 'zabbixifgoiano@gmail.com'. The selected notification is 'OK: Atividade do Site S2BIFGoiano.net' from 02/10/2015. The right pane shows the details of this notification, including the trigger status (OK), severity (Disaster), and a list of item values for a download speed scenario.

Figura 64 e-mail de Notificação Trigger: OK

## 19.4. CONFIGURAÇÃO DO SISTEMA DE ALERTA VIA WHATSAPP

O processo de instalação e configuração do WhatsApp será feito no servidor principal junto com o sistema de envio via e-mail. O processo de instalação do sistema de notificação foi adaptado do artigo publicado por Medeiros. (2015) juntamente com apoio da equipe de integrantes da comunidade Zabbix-Brasil no Facebook.

Como feito anteriormente todo o processo de instalação dos recursos necessários serão executados dentro da pasta /etc/zabbix.

Para que o Yowsup funcione, alguns pacotes precisam ser instalados. Acessando o terminal com permissão de root foi utilizado os seguintes parâmetros:

```
yum install python python-libs python-argparse python-dateutil python-py python-devel
```

#Baixando e instalando o yowsup. Vamos criar uma pasta para baixar o yowsup:

```
mkdir yowsup
cd yowsup
wget https://github.com/tgalal/yowsup/archive/master.zip
```

#Descompactamos o arquivo. Instale o unzip :

```
Yum install unzip
unzip master.zip
cd yowsup-master
```

#Instalando o Yowsup:

#Dentro da pasta descompactada, basta rodar o script de instalação com o argumento "install":

```
./setup.py install
```

#Ele vai compilar, baixar alguns pacotes e o ambiente vai estar pronto, inclusive com os executáveis nas respectivas pastas bin!

Ativando o Yowsup.

O Whatsapp precisa de um número de telefone válido para o envio de mensagens. É recomendado reservar um número específico para o zabbix utilizar para enviar as mensagens. Não é necessário deixar nada conectado no servidor, pois o Yowsup utiliza uma API que fará o envio das mensagens, necessitando apenas que seja ativado o número a ser utilizado.

Primeiramente é criado um arquivo de configuração com os dados do número a serem cadastrado no Yowsup.

```
vi /opt/zap.config
cc=55 #Código do país
phone=551199990000 #Número de telefone com código de país e ddd
id=ZabbixMhos #Invente uma ID
password=
```

O campo senha deverá ser deixado em branco por enquanto, pois futuramente será recebida quando ativar o Yowsup. E necessário rodar o comando para solicitar o código de ativação. A mensagem que será retornada, está logo abaixo:

```
yowsup-cli registration -r sms -c /opt/zap.config
INFO:yowsup.common.http.warequest:{"status":"sent","length":6,"method":
"sms","retry_after":1805}
status: sent
retry_after: 1805
length: 6
method: sms
```

Nesse momento, deverá ter recebido um SMS no número, que foi informado no arquivo de configuração. Agora deverá utilizar o código recebido para ativar o número (o 001-001 é apenas um exemplo):

```
yowsup-cli registration -R 001-001 -c /opt/zap.config
INFO:yowsup.common.http.warequest:{"status":"ok","login":"55489130816
7","pw":"29gnQdVaWtg8MJGnN95zj4Md7Ko=","type":"new","expiration":1466600857
,"kind":"free","price":"US$0.99","cost":"0.99","currency":"USD","price_expiration":1438
164915}
status: ok
kind: free
pw: 29gnQdVaWtg8MJGnN95z34Md7Ko=
price: US$0.99
price_expiration: 1438164915
currency: USD
cost: 0.99
expiration: 1466600857
login: 551199990000
type: new
```

Nesse processo deverá ter recebido informações do Yowsup, com uma senha. Copie a senha e inserira-a no arquivo /etc/zabbix/zap.config que foi criado anteriormente:

```
vi /opt/zap.config
```

```
cc=55 #Código do país
phone=551199990000 #Número de telefone com código de país e ddd
id=Zabbix Medeiros #Invente uma ID
password=29gnQdVaWtg8MJGnN95z34Md7Ko=
```

Basta salvar o arquivo, e realizar um teste para verificar se a configuração do Yowsup está correta e se está enviando mensagens através do Whatsapp. Para testar basta utilizar o comando abaixo, que enviará uma mensagem para o número inserido abaixo e com a mensagem do lado.

```
yowsup-cli demos -s 554890001111 "Teste do Yowsup" -c /opt/zap.config
```

Após executar o comando deverá ter recebido uma mensagem no Whatsapp do número inserido acima, como mostra a Figura 65.



Figura 65 Mensagem de Teste do Yowsup

Com o primeiro teste concluído conforme mostra a Figura 68, é necessário criar um script para que o Zabbix execute na hora de enviar a mensagem. Por padrão, o Zabbix procura os scripts personalizados na pasta alertscripts. Essa pasta pode variar de caminho, dependendo dos (pacotes ou fontes) e da distribuição que foi

utilizada. Para ter certeza, é recomendado fazer uma busca pela pasta utilizando os comandos:

```
find / -name alertscripts
/usr/lib/zabbix/alertscripts
```

Foi necessário criar o script na pasta encontrada, utilizando o comando:

```
vi /usr/lib/zabbix/alertscripts/whatsapp_zabbix.sh
```

Ao criar o arquivo de script foi necessário inserir os seguintes parâmetros:

```
#LOGFILE="/var/log/zabbix/whatsapp.log"
DEST="$1"
MSG="$2"
YOWSUP="/opt/yowsup-cli"
YCONF="/opt/zap.config"
$YOWSUP demos -c $YCONF -s "${DEST}" "${MSG}"
HORA=$(date +%d-%m-%Y-%H:%M:%S)
echo "$HORA - To: "${DEST}" Text: "${MSG}"
```

Os parâmetros acima são responsáveis por criar um arquivo de log para o script do whatsapp, criar duas variáveis responsáveis por identificar o número de destino, que receberá a notificação do Zabbix, os locais onde estão armazenados o arquivo de configuração do yowsup e do zap.config que foram criados anteriormente.

E abaixo foi um comando que irá enviar a notificação e apresentar alguns dados no relatório de log, como o destino, hora, data, e a mensagem enviada para futuras consultas.

Para o funcionamento correto do script foi necessário dar permissão total ao mesmo, utilizando o comando `chmod 777 whatsapp_zabbix.sh`. Também necessário acessar o arquivo do Sudoers, e adicionar o seguinte comando para que o Zabbix não necessite senha para executar seus comandos:

```
zabbix ALL =NOPASSWD:ALL
Defaults:zabbix !requiretty
```

Também foi necessário criar a pasta zabbix localizada em em `/var/lib` e dar permissão total. Esta pasta que deveria ser criada automaticamente, porém por algum problema no sistema não foi criada, assim sendo necessário cria-la para que o sistema de notificação funcionasse corretamente.

Foi utilizado os seguintes parâmetros:

```
mkdir /var/lib/zabbix
```

```
chmod 777 /var/lib/zabbix
```

Com o script criado foi possível realizar um teste para verificar se o mesmo estava funcionando corretamente, e foi necessário acessar a pasta /usr/lib/zabbix/alertscripts e executar o script do whatsapp com o comando: whatsapp\_zabbix.sh (Número do telefone com código do país + DDD) "Mensagem". E em questão de segundos a mensagem enviada foi recebida no número inserido.

Após finalizar o processo de configuração do Yowsup, do script do whatsapp e verificar que estava tudo funcionando, foi necessário criar a mídia específica para o whatsapp, da mesma forma que foi criada a mídia para o e-mail, porém o tipo de mídia dessa vez será script, pois o Zabbix irá acessar o script que foi criado anteriormente e concedido permissão total.

Com a mídia devidamente criada conforme a Figura 66, foi necessário criar a mídia para o usuário que receberá a notificação. Foi definido que além do administrador mais um usuário iria receber as notificações do Zabbix, portando foi necessário criar um novo usuário e um grupo específico para as notificações do Zabbix, pois esse grupo determinaria quais permissões o novo usuário teria e por questões de segurança ele terá acesso restrito as partes de configurações da ferramenta, podendo apenas visualizar a página de Monitoramento.

The image shows a web form for configuring media types in Zabbix. The form has a blue header with the text 'CONFIGURAÇÃO DE TIPOS DE MÍDIA'. Below the header, there is a section titled 'Tipo de mídia'. The form contains the following fields and controls:

- 'Nome': A text input field containing 'WhatsApp'.
- 'Tipo': A dropdown menu with 'Script' selected.
- 'Nome script': A text input field containing 'whatsapp\_zabbix.sh'.
- 'Ativo': A checkbox that is checked.

At the bottom of the form, there are three buttons: 'Atualizar' (highlighted with a yellow border), 'Remover', and 'Cancelar'. Below the buttons, there is a footer that reads 'Zabbix 2.4.6 é uma marca registrada 2001-2015 pela Zabbix SIA'.

Figura 66 Criação Mídia Script Whatsapp

Para criar foi necessário acessar o menu Administração -> Usuários -> Criar grupo de usuários, como mostra a Figura 67.

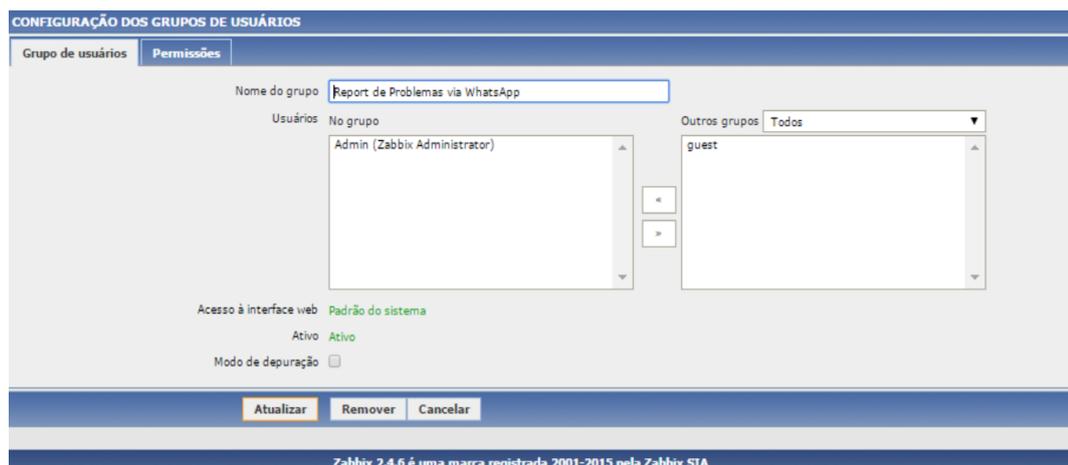


Figura 67 Criação do grupo de notificação do Whatsapp

Foi definido que este grupo terá como usuário o administrador do Zabbix e o novo usuário criado, foi utilizado um nome fantasma para tal: João. João receberá igualmente ao administrador do Zabbix as notificações ocorridas pelo disparo de uma trigger que foram configuradas nas ações. Porém não receberá via e-mail as notificações. O grupo foi criado com os seguintes parâmetros:

- Nome do grupo: Report de Problemas via Whatsapp.;
- Usuários no grupo: Admin e futuramente quando criado será adicionado o usuário João.

Na aba permissões, Figura 68, foi definido quais os acessos os usuários pertencentes a esse grupo teriam. O usuário Admin do Zabbix faz parte de um grupo de super Administradores com permissão total ao sistema, porém não é interessante, tão pouco seguro deixar qualquer usuário com permissão de administrador, por isso foi delegado que o grupo Reporte de Problemas via Whatsapp teria apenas permissão de “Somente Leitura”, de modo que qualquer outro usuário criado no zabbix como usuário “comum” herdaria essas permissões quando vinculado a esse grupo, recebendo as notificações como o administrador, e tendo acesso ao frontend com restrições de acesso.

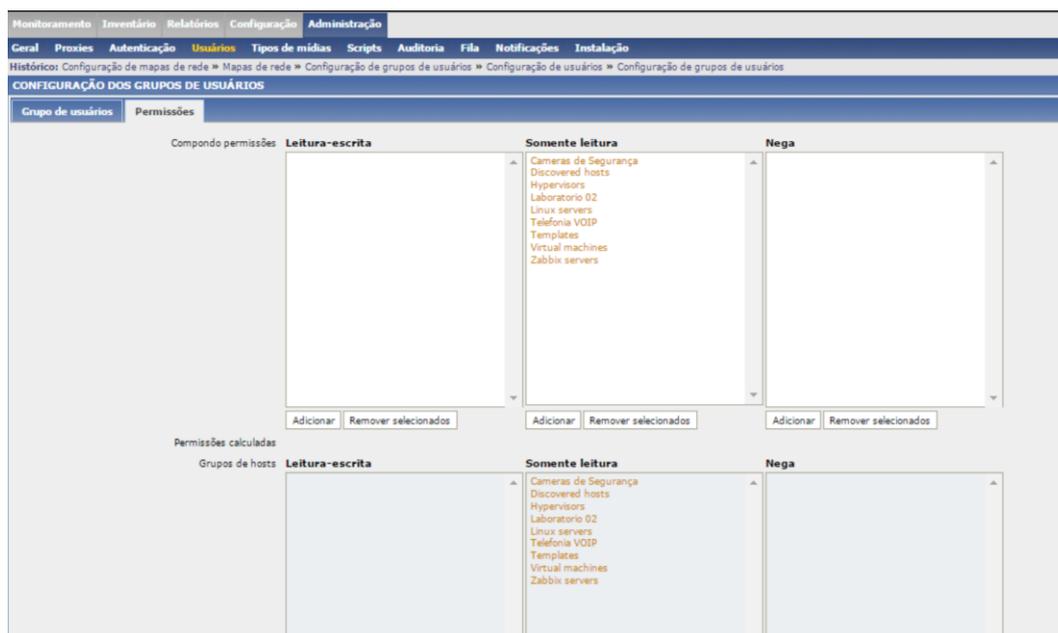


Figura 68 Permissão do grupo notificação WhatsApp

## 19.5. CRIAÇÃO DE UM USUÁRIO PARA NOTIFICAÇÃO DO WHATSAPP

Para criar o usuário foi necessário acessar o menu Administração > Usuários, acessar o menu Usuários no canto direito superior > criar usuário.

O Zabbix permite definir alguns parâmetros ao cadastrar um novo usuário, podendo definir o Grupo a qual este usuário pertence, o idioma que estará na interface quando o usuário logar, tema padrão, se o usuário terá uma sessão com um tempo de duração predeterminado, podendo definir também o tempo de atualização da tela e o quantitativo de registros por páginas e se for do interesse do administrador definir um URL que será acessado após o login do novo usuário. Foi necessário inserir apenas o Apelido, Nome e qual grupo o novo usuário pertenceria os outros parâmetros se mantiveram no padrão do sistema como mostra a Figura 69.

Monitoramento Inventário Relatórios Configuração Administração

Geral Proxies Autenticação **Usuários** Tipos de mídias Scripts Auditoria Fila Notificações Instalação

Histórico: Mapas de rede » Configuração de grupos de usuários » Configuração de usuários » Configuração de grupos de usuários » Configuração de usuários

**CONFIGURAÇÃO DOS USUÁRIOS**

Usuário Mídia Permissões

Apelido: João

Nome: João

Sobrenome:

Grupos: Report de Problemas via WhatsApp [Adicionar]

Remover selecionados

Senha: Alterar senha

Língua: Inglês (en\_GB)

Tema: Padrão do sistema

Login automático:

Auto-logout (mín. 90 segundos):  900

Atualização da tela (em seg.):  30

Registros por página:  50

URL (após se conectar):

Atualizar Remover Cancelar

Figura 69 Criação de usuário

Na próxima aba “Mídia” foi criado uma mídia para o usuário João, de forma semelhante quando criado a mídia de e-mail para o usuário Admin. Adicionando uma nova mídia através do botão “Adicionar” é aberto uma nova janela, sendo necessário informar os seguintes parâmetros de acordo com a Figura 70.

- Tipo: O tipo da nova mídia, foi escolhido a mídia criada: Whatsapp;
- Enviar para: O número de telefone do destinatário contendo Código do país com DDD;
- Quando ativo: O Zabbix possibilita gerenciar os horários que essas mídias poderão ser enviadas, por padrão é definido sete dias por semana, vinte e quatro horas por dia;
- Usar se severidade: Pode ser definido em qual tipo de gravidade essa mídia será utilizada, podendo filtrar também na criação das ações;
- Status: Se ela está ativa ou não.

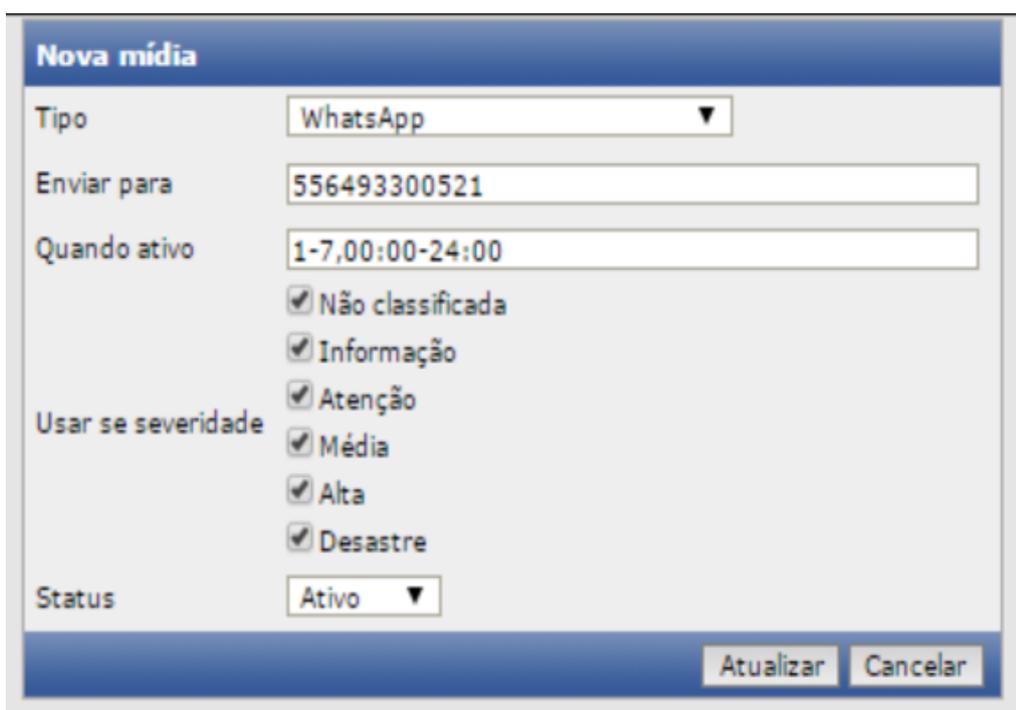


Figura 70 Mídia WhatsApp usuário Joao

Na aba “Permissões”, Figura 71, é definido qual tipo de usuário será criado, podendo variar entre Usuário Zabbix, Administrador Zabbix, Super Administrador Zabbix, onde os dois primeiros tipos receberam as permissões definidas no grupo vinculado, e o Super Administrador Zabbix concedendo permissão total ao sistema, e sobrepondo as permissões definidas no grupo.

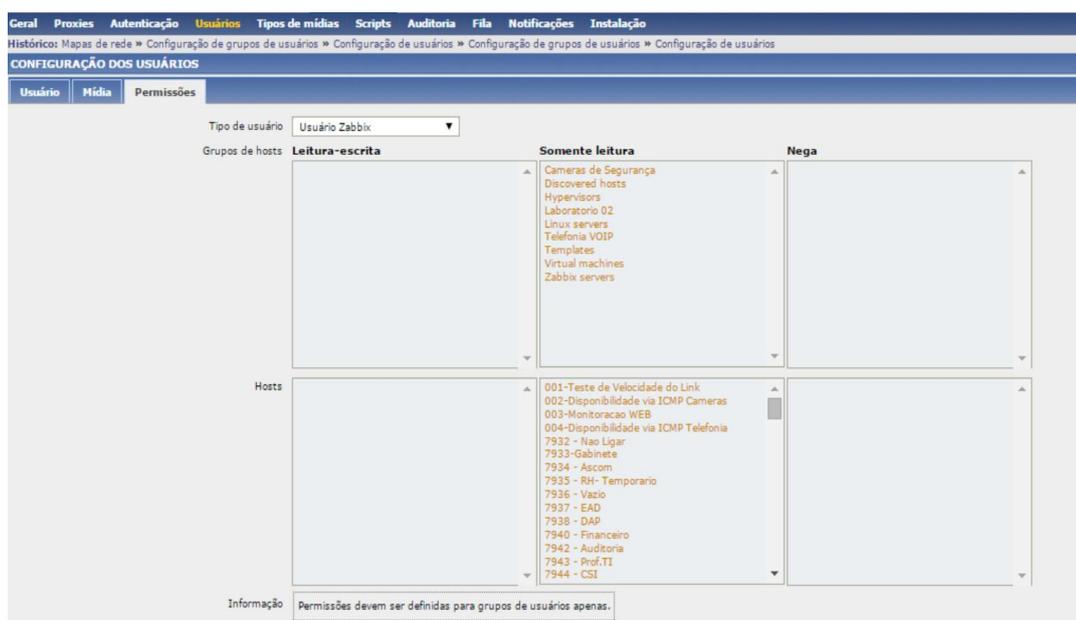


Figura 71 Permissão de usuário do grupo WhatsApp

Com o usuário devidamente criado foi criada uma ação específica, Figura 72, para realizar a notificação para os dois usuários. Sendo configurada de forma semelhante a criada anteriormente para e-mail, alterando apenas o conteúdo da mensagem, pois como se trata de um smartphone que irá visualizar a informação a mensagem deverá ser o mais limpa possível facilitando sua visualização e acelerando a tomada de providência do administrador.

Foi deixado como conteúdo da mensagem apenas a TRIGGER.NAME e TRIGGER.STATUS, responsável por apresentar o nome do problema e sua gravidade, conforme a imagem abaixo.

The image shows the 'CONFIGURAÇÃO DE AÇÕES' (Action Configuration) window in Zabbix. It has three tabs: 'Ação', 'Condições', and 'Ações', with 'Ações' selected. The configuration includes:

- Nome:** Report de Problema via WhatsApp
- Assunto padrão:** {TRIGGER.STATUS}: {TRIGGER.NAME}
- Mensagem padrão:** Trigger: {TRIGGER.NAME}  
Trigger status: {TRIGGER.STATUS}
- Mensagem da recuperação:**  (checked)
- Assunto da recuperação:** {TRIGGER.STATUS}: {TRIGGER.NAME}
- Mensagem da recuperação:** Trigger: {TRIGGER.NAME}  
Trigger status: {TRIGGER.STATUS}
- Ativo:**  (unchecked)

At the bottom, there are buttons for 'Atualizar', 'Clonar', 'Remover', and 'Cancelar'. The footer of the window reads: 'Zabbix 2.4.6 é uma marca registrada 2001-2015 pela Zabbix SIA'.

Figura 72 Ação notificação WhatsApp

Com os usuários devidamente criados, as mídias criadas, foi realizado um teste para verificar se o sistema de notificação estava funcionando devidamente. Foi realizado a simulação da queda de um dos sites que estão sendo monitorados pelo serviço web do Zabbix, afim de obter um resultado igual no ambiente de produção.

Com o serviço parado, a trigger de Desastre será ativada conforme configurado, alertando que o site s2bifgoiano.net.br está fora do ar, e apresentará o quantitativo de ações que serão tomadas devido a esta ocorrência. Como foi configurado para enviar um e-mail ao administrador e uma notificação a ele e ao usuário João, será apresentado três ações e estará em laranja pois a mesma está em andamento conforme a Figura 73.

Host	Assunto	Última alteração	Idade	Informação	Reconhecido	Ações
ZabbixProxy	Atividade do Site S2BIFGoiano.net	14-10-2015 22:50:47	1m 24s		Não	3

Figura 73 Notificação WhatsApp em Andamento

Quando as ações forem executadas com sucesso o Zabbix apresentará em verde quantas notificações tiveram sucesso, como apresenta a Figura 74.

Host	Assunto	Última alteração	Idade	Informação	Reconhecido	Ações
ZabbixProxy	Atividade do Site S2BIFGoiano.net	14-10-2015 22:50:47	1m 24s		Não	3
7955 - Transporte	Equipamento 7955 - Transporte não responde ao (PING).	14-10-2015 16:56:58	5h 51			Fechar
Lab02PC18	Zabbix agent on Lab02PC18 is unreachable for 5 minutes	14-10-2015 16:36:30	6h 11	Usuário	Detalhes	Status
Lab02PC05	Zabbix agent on Lab02PC05 is unreachable for 5 minutes	14-10-2015 16:35:00	6h 11	Admin (Zabbix Administrator)	Reporte de Problemas via Email	Enviado
7933 - Gabinete	Equipamento 7933 - Gabinete não responde ao (PING).	14-10-2015 16:26:09	6h 21	Joao (Joao)	WhatsApp	Enviado
Lab02PC18	Free disk space is less than 20% on volume G:	14-10-2015 15:52:45	6h 51	Admin (Zabbix Administrator)	WhatsApp	Enviado

Figura 74 Notificação WhatsApp enviada

Com a intenção de verificar a confidencialidade da informação passada ao Zabbix, a caixa de entrada do e-mail criado para o Zabbix foi verificada, notando que havia uma mensagem apresentando um problema com o site junto com todas suas informações a respeito da trigger, como configurado em sua ação. E logo foi iniciado o serviço do site para que fosse verificado a notificação de que o serviço voltasse, como pode ser observado na Figura 75.

Exibição: Tudo ▾ Organizar por ▾

Assunto	Tempo
zabbixifgoiano@gmail.com	04:56
OK: Atividade do Site S2BIFGoiano.net	(9) ▶
zabbixifgoiano@gmail.com	04:52
PROBLEM: Atividade do Site S2BIFGoiano.net	▶
zabbixifgoiano@gmail.com	04:50
OK: Equipamento 7973 - Hidrolandia não responde ao (... (100)▶	
zabbixifgoiano@gmail.com	04:49
PROBLEM: Equipamento 7973 - Hidrolandia não respon...	▶
zabbixifgoiano@gmail.com	04:47
PROBLEM: Atividade do Site S2BIFGoiano.net	▶
zabbixifgoiano@gmail.com	04:45
PROBLEM: Atividade do Site S2BIFGoiano.net	▶
zabbixifgoiano@gmail.com	04:44

**PROBLEM: Atividade do Site S2BIFGoiano.net**

zabbixifgoiano@gmail.com Adicionar aos contatos 04:52 ▶

Para: joaoavictor\_b20@hotmail.com ▾

Ações

Trigger: Atividade do Site S2BIFGoiano.net

Trigger status: PROBLEM

Trigger severity: Disaster

Trigger URL:

Item values:

- Download speed for scenario "Servico de monitoramento do S2BIFgoiano.net.br". (ZabbixProxy:web.test.in[Servico de monitoramento do S2BIFgoiano.net.br,,bps]): 0 Bps
- \*UNKNOWN\* (\*UNKNOWN\*:\*UNKNOWN\*): \*UNKNOWN\*
- \*UNKNOWN\* (\*UNKNOWN\*:\*UNKNOWN\*): \*UNKNOWN\*

Figura 75 Notificação de problema e OK via e-mail

Da mesma forma foi verificado nos smartphones do administrador e do usuário Joao se havia relatado o problema e a normalização do mesmo, tendo como resultado uma mensagem limpa e de fácil visualização como na Figura 76.



Figura 76 Notificação de Problem e OK no WhatsApp

## 20. APÊNDICE E - INSTALAÇÃO DO ZABBIX AGENT EM HOST WINDOWS

O Zabbix como outras ferramentas de monitoramento possui um agente específico, responsável por realizar consultas em um determinado host, como por exemplo memória, hd, processador. Foi instalado o agente em todos os computadores localizados no laboratório dois, do Campus Morrinhos e também em seus servidores Windows, onde estão hospedados alguns sites.

Afim de coletar informações e verificar a disponibilidade de recursos de hardware desses hosts o agente do Zabbix foi instalado e configurado de acordo com estruturado anteriormente. Para os laboratórios de informática foi destinado um segundo servidor proxy, responsável por realizar a coleta desses hosts e repassar ao Zabbix Server, para os servidores Windows quem realiza a coleta é o primeiro servidor proxy.

O agente possui uma compatibilidade bastante vasta, atendendo plataformas proprietárias e open source como: Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, OS X, Tru64/OSF1, Windows NT, Windows Server, Windows XP e Windows Vista.

A instalação do agente pode ser realizada de duas formas, baixando os arquivos necessários do site oficial, ou copiando os arquivos do agente contidos nos arquivos do Zabbix Server, instalado anteriormente.

Optou-se por baixar os arquivos diretos do site oficial, não sendo necessário realizar uma busca e cópia dos arquivos para os hosts Windows. Após o download é necessário criar uma pasta na unidade C:\ com o nome zabbix e colar a pasta extraída. Nela conterà os arquivos necessários para configurar o agente e inserir o serviço do agente no sistema. Contém na pasta principal duas pastas. A bin contém os arquivos correspondentes a duas plataformas do sistema x86 ou x64, foi necessário utilizar a x64, pois todos os sistemas utilizados são baseados nessa plataforma. E a pasta conf, que contém o arquivo de configuração do agente. Foi necessário copiar o arquivo zabbix\_agentd contido na pasta x64 e o arquivo zabbix\_agentd.conf contido na pasta conf e mover ambos para a pasta criada em C:\zabbix para melhor gerenciamento.

Com um editor de texto foi editado o arquivo zabbix\_agentd.conf com os seguintes parâmetros:

- Log file: c:\zabbix\zabbix\_agentd.log: Define onde será salvo o arquivo de log do zabbix\_agentd;
- LogFileSize = 1: Define o tamanho do arquivo de log;
- DebugLevel = 3: Define o que conterà no arquivo de log, neste caso toda informação básica do serviço, informações críticas, erros e alertas;
- Server: 192.168.0.3: Defini o IP do servidor que receberá as informações coletadas. No caso implantado utilizou-se o IP 192.168.0.3, do servidor Proxy I para a coleta dos hosts Windows Server e 192.168.0.4, do servidor Proxy II para os hosts Windows 7 do laboratório em análise;
- ListenPort:10050: Porta em que o agente irá responder, a mesma teve que ser cadastrada no firewall do Windows para o pleno funcionamento do agente e cadastrada junto com o ip e nome definido do host no Zabbix Server;

- StartAgents = 3: Define o número de instâncias do processo da checagem passiva do zabbix agente. Por padrão o valor inserido é 3;
- ServerActive=192.168.0.3: Define a atividade de checagem a um servidor. Configurado de acordo com o servidor que irá atender o host, como em Server;
- Hostname: S2BSRV01= Nome único que referenciará o host. É case sensitive, e deverá ser informado no ZabbixServer da mesma forma que foi definido no arquivo de configuração;
- Timeoute = 3: Define o tempo máximo gasto para cada processamento. Por padrão o valor é 3.

Após as configurações foi necessário salvar o arquivo e executar o aplicativo zabbix\_agentd, com permissão de Administrador para que instalasse o serviço do agente. O serviço deverá constar na lista de serviços do Windows e deverá estar parado, sendo necessário uma reinicialização do sistema ou iniciar manualmente para que o serviço comece a realizar as coletas, como apresenta a Figura 77.

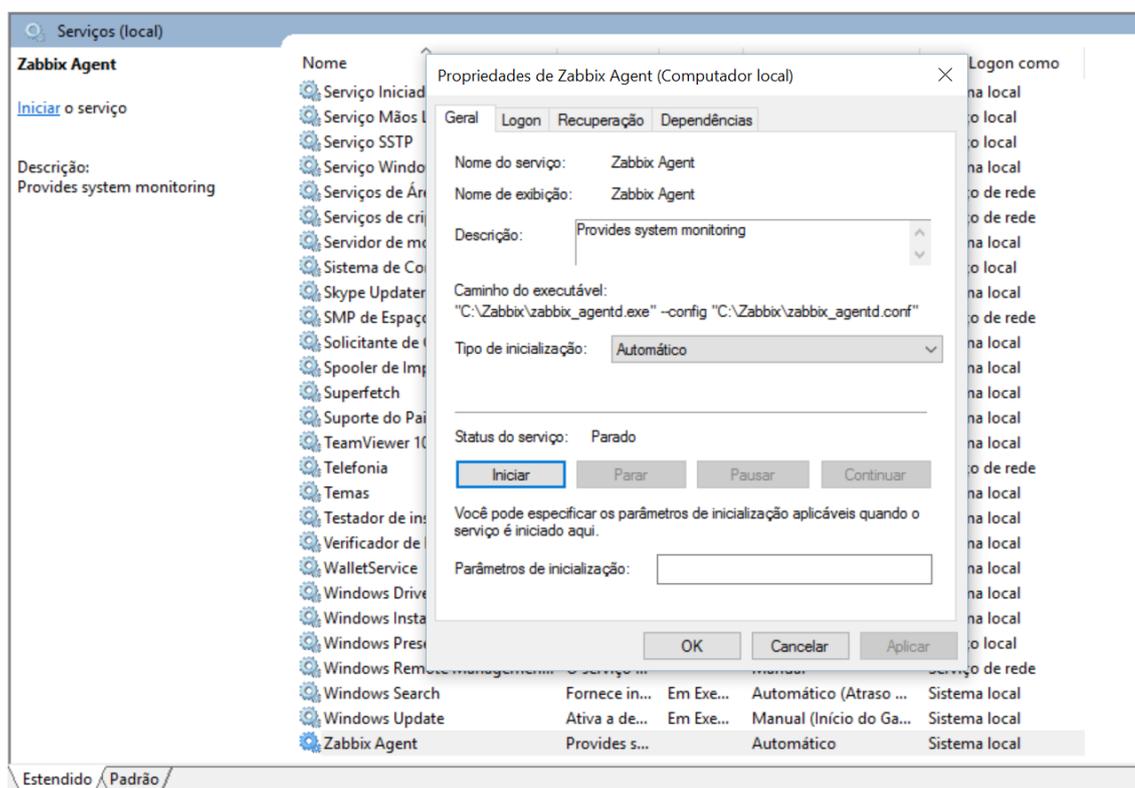


Figura 77 Serviço Zabbix Agente Windows

Foi necessário criar permissões de entrada no firewall do Windows para que o serviço funcionasse, dessa forma não tendo a necessidade de deixar o firewall desabilitado, permitindo brechas de segurança.

Em Firewall do Windows com Segurança Avançada foi criado duas regras de entrada para a porta 10050 para os protocolos UDP E TCP, permitindo acesso a todos os tipos de rede. Dessa forma independente da configuração do firewall não haverá o bloqueio do agente.

As regras criadas podem ser vistas na Figura 78.

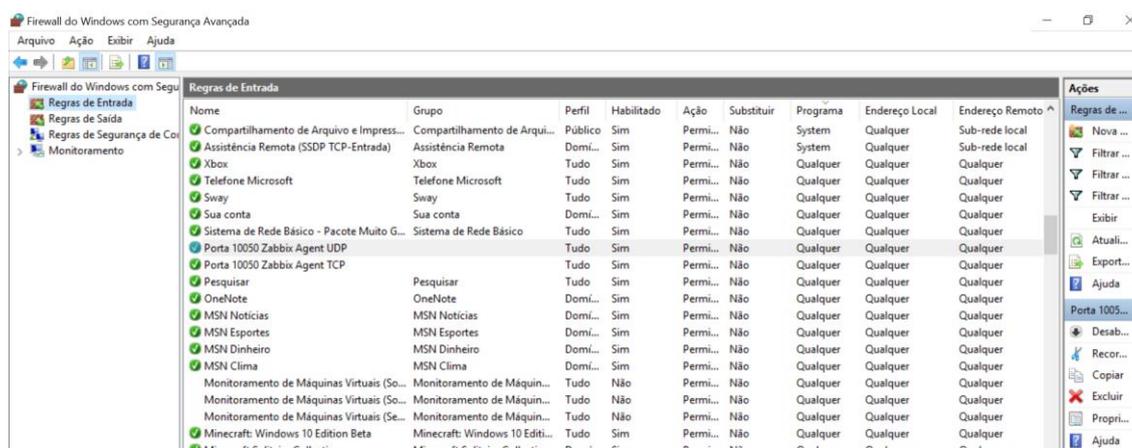


Figura 78 Regras de entrada Firewall Windows

## 20.1. CRIAÇÃO DOS GRUPOS DE HOSTS

Para um melhor gerenciamento e agrupamento de todos os hosts a serem criados, foram criados grupos, para que seu gerenciamento e organização se tornasse mais fácil, possibilitando uma administração mais centralizada.

Foi criado o grupo Servidores Windows e Laboratorio02 que agrupam os servidores Windows da escola e os computadores de seu laboratório. Os grupos foram criados da seguinte maneira, acessando o menu configurações > Grupos de Hosts > Criar Grupo de hosts.

A tela de criação é bem simples, como pode ser observado na Figura 79. Pode vincular no ato da criação um host que esteja em um outro grupo ou que não faça parte de nenhum. Também pode vincular o host no grupo no ato da criação do host, como será visto futuramente. Tendo como resultado a seguinte tela. Adaptando o nome para cada grupo a ser criado.

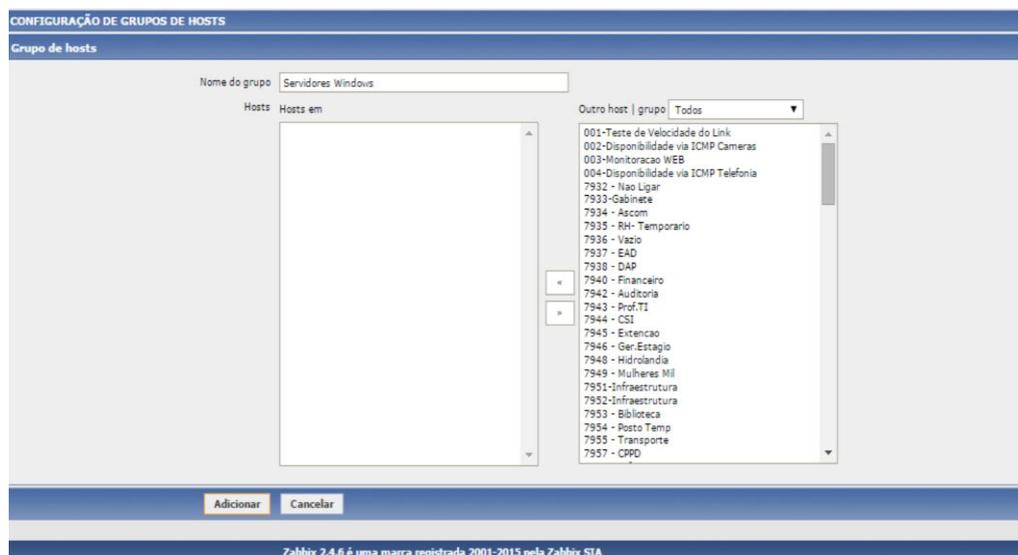


Figura 79 Criação de Grupo de Hosts

## 20.2. CRIAÇÃO DOS HOSTS WINDOWS NO FRONTEND

A criação de todos os hosts Windows procedeu de forma semelhante quando foi criado os Hosts dos servidores. Porém esses hosts serão monitorados através de proxy, necessitando identificar em sua criação em qual proxy ele enviará suas informações que futuramente serão repassadas ao Zabbix Server.

Após inserir os parâmetros necessários para a criação do Host como Nome, Grupo (correspondente que foi criado anteriormente), IP, Porta será necessário selecionar qual proxy irá monitorar o Host. Foi selecionado o Proxy conforme definido anteriormente: ZabbixProxy para os servidores Windows e ZabbixProxyII para hosts Windows. Na seleção foi possível escolher entre ser monitorado por nenhum proxy, pelo ZabbixProxy ou ZabbixProxyII, conforme a Figura 80.

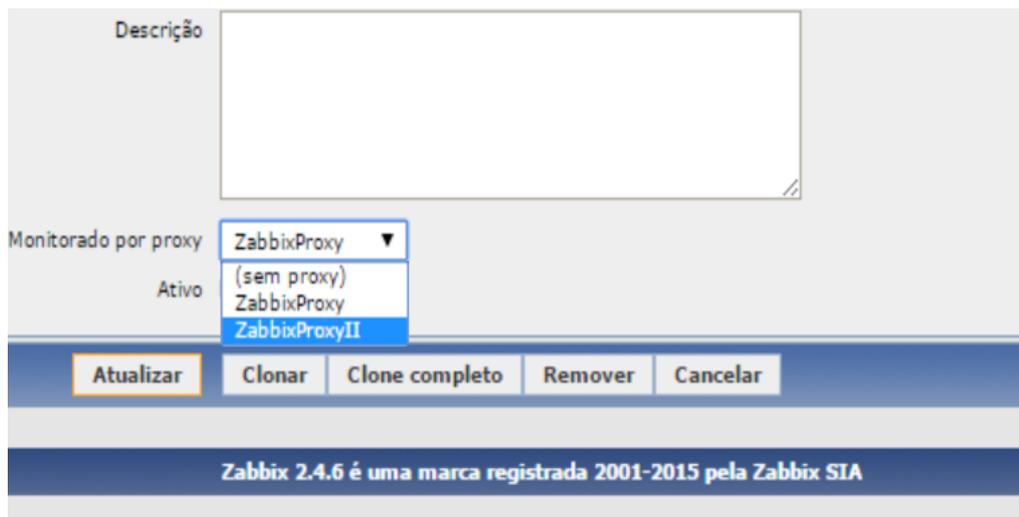


Figura 80 Escolha do ZabbixProxy Fonte: Autor

Para todos os Hosts Windows adicionados foi vinculado o Template OS WINDOWS, responsável por coletar os dados de uso de memória ram, processador, disco e rede. Com a criação dos hosts corretamente, em questão de alguns minutos o agente já estará coletando as informações repassando ao proxy e ele ao servidor. Quando a coleta estiver sendo realizada, no menu host, e selecionando o grupo correspondente é possível notar em verde que há um agente Zabbix realizando a coleta, e em vermelho quando não estiver, devido a algum problema de configuração ou desligamento do host como é apresentado nas Figuras 81 e 82.

CONFIGURAÇÃO DE HOSTS											Criar host Importar	
Hosts											Grupo: Servidores Windows	
Mostrando 1 para 2 de 2 encontrados												
Esibir filtro												
Nome	Aplicações	Itens	Triggers	Gráficos	Autobusca	Web	Interface	Templates	Status	Disponibilidade		
ZabbixProxy: FRIENDZONE1	Aplicações (9)	Itens (80)	Triggers (10)	Gráficos (32)	Autobusca (2)	Web (0)	192.168.180.16: 10050	Template OS Windows (Template App Zabbix Agent)	Ativo	✓	□	□
ZabbixProxy: ZABSRV01	Aplicações (9)	Itens (72)	Triggers (10)	Gráficos (28)	Autobusca (2)	Web (0)	192.168.180.55: 10050	Template OS Windows (Template App Zabbix Agent)	Ativo	✓	□	□

Figura 81 Hosts Servidores Windows OK

CONFIGURAÇÃO DE HOSTS											Criar host Importar	
Hosts											Grupo: Laboratorio 02	
Mostrando 1 para 27 de 27 encontrados												
Esibir filtro												
Nome	Aplicações	Itens	Triggers	Gráficos	Autobusca	Web	Interface	Templates	Status	Disponibilidade		
ZabbixProxyII: Lab02PC01	Aplicações (9)	Itens (18)	Triggers (9)	Gráficos (2)	Autobusca (2)	Web (0)	10.1.2.32: 10050	Template OS Windows (Template App Zabbix Agent)	Ativo	✗	□	□
ZabbixProxyII: Lab02PC02	Aplicações (9)	Itens (108)	Triggers (12)	Gráficos (44)	Autobusca (2)	Web (0)	10.1.2.34: 10050	Template OS Windows (Template App Zabbix Agent)	Ativo	✗	□	□
ZabbixProxyII: Lab02PC04	Aplicações (9)	Itens (18)	Triggers (9)	Gráficos (2)	Autobusca (2)	Web (0)	10.1.2.10: 10050	Template OS Windows (Template App Zabbix Agent)	Ativo	✗	□	□

Figura 82 Hosts Windows 7 Problema