

**UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ**  
**DEPARTAMENTO ACADÊMICO DE INFORMÁTICA**  
**TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS**

**ALEXANDRO BAHLS**

**MONITORAMENTO PROATIVO DO AMBIENTE DE REDE**  
**UTILIZANDO O SOFTWARE ZABBIX**

**TRABALHO DE CONCLUSÃO DE CURSO**

**PONTA GROSSA**

**2016**

**ALEXANDRO BAHLS**

**MONITORAMENTO PROATIVO DO AMBIENTE DE REDE  
UTILIZANDO O SOFTWARE ZABBIX**

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas, do Departamento Acadêmico de Informática, da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Augusto Foronda

**PONTA GROSSA**

**2016**



Ministério da Educação  
**Universidade Tecnológica Federal do Paraná**  
Campus Ponta Grossa  
Diretoria de Pesquisa e Pós-Graduação  
Departamento Acadêmico de Informática  
Tecnologia em Análise e Desenvolvimento de Sistemas

---

## TERMO DE APROVAÇÃO

### MONITORAMENTO PROATIVO DO AMBIENTE DE REDE UTILIZANDO O SOFTWARE ZABBIX

por

ALEXANDRO BAHLS

Este Trabalho de Conclusão de Curso (TCC) foi apresentado em 18 de maio de 2016 como requisito parcial para a obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

---

Prof. Dr. Augusto Foronda  
Orientador

---

Prof. Msc. Geraldo Ranthum  
Membro titular

---

Prof. Msc. Luiz Rafael Schmitke  
Membro titular

---

Prof<sup>a</sup>. Dra. Helyane Bronoski Borges  
Responsável pelo Trabalho de Conclusão  
de Curso

---

Prof<sup>a</sup>. Dra. Mauren Louise Sguario  
Coordenadora do curso

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

Dedico este trabalho à minha família, em especial à minha esposa Rosângela, minhas filhas Amanda e Alexia, pelo apoio e compreensão.

## **AGRADECIMENTOS**

Certamente estes parágrafos não irão atender a todas as pessoas que fizeram parte dessa importante fase de minha vida, mas elas podem estar certas de que fazem parte de meu pensamento e de que tem toda minha gratidão.

Agradeço inicialmente ao meu orientador Prof. Dr. Augusto Foronda, pela sabedoria com que me guiou nesta trajetória.

Aos meus colegas de sala, em especial aos “Irmãos de Farda”.

À Coordenação do Curso, pela cooperação e dedicação à docência.

Enfim, a todos os que, de alguma forma, contribuíram para a realização desta pesquisa.

## RESUMO

BAHLS, Alexandro. **Monitoramento Proativo do Ambiente de Rede Utilizando o Software Zabbix**. 2016. 64 f. Trabalho de Conclusão de Curso, Universidade Tecnológica Federal do Paraná. Ponta Grossa, 2016.

Este trabalho pretende demonstrar a solução para monitoramento proativo do ambiente de rede utilizando a ferramenta Zabbix. A estrutura de rede consiste de um servidor de gerenciamento principal, onde será instalado o Servidor Zabbix e a estrutura a ser monitorada, que consiste de um servidor *web* Apache, um servidor DNS Bind, um servidor DHCP, um servidor de arquivos Samba. A versão Agente Zabbix será instalada em todos os servidores. O Servidor Zabbix fará o monitoramento da estrutura e executará as medidas necessárias ao reestabelecimento do serviço monitorado que apresentar falha. Será documentada a instalação, configuração e monitoramento da estrutura. O objetivo é mostrar que é possível monitorar o ambiente de rede de maneira proativa, diminuindo a necessidade de intervenção direta do administrador da rede.

**Palavras-chave:** Zabbix. Monitoramento. Gerenciamento.

## ABSTRACT

BAHLS, Alexandro. **Proactive Monitoring Network Environment Using the Software Zabbix**. 2016. 64 f. Completion of Course Work, Federal Technological University of Paraná. Ponta Grossa, 2016.

This work aims to demonstrate the solution for proactive monitoring of the network environment using the Zabbix tool. The network structure consists of one Main Management Server , where will be installed Zabbix Server and the structure to be monitored, which consist of an Apache web server , a DNS server BIND , a DHCP server, a Samba File Server . The Zabbix Agent version will be installed on all servers. Zabbix Server will monitor the structure and implement the necessary measures to reestablish service fails. Will be documented installation configuration and monitoring of the structure. The goal is to show that you can proactively monitor network environment, reducing the need for direct intervention by the network administrator.

**Keywords:** Zabbix. Monitoring. Management.

## LISTA DE FIGURAS

Figura 1- Exemplo de arquitetura de gerenciamento de rede.....	20
Figura 2- Relacionamento entre o Gerente e o Agente.....	22
Figura 3- Modelo de utilização do Proxy Zabbix.....	25
Figura 4- Interface <i>Web</i> do Servidor Zabbix.....	26
Figura 5- Instalação repositório yum.....	28
Figura 6- Atualização dos repositórios.....	29
Figura 7- Instalação do Servidor Zabbix e Interface <i>Web</i> .....	29
Figura 8- Relação de dependências instaladas.....	30
Figura 9- Instalação do agente Zabbix.....	32
Figura 10- Tela inicial do instalador da interface <i>web</i> .....	35
Figura 11- Tela de checagem de pré-requisitos.....	36
Figura 12- Configuração da conexão com o banco de dados.....	37
Figura 13- Detalhes da configuração do servidor.....	37
Figura 14- Sumário para checagem de parâmetros.....	38
Figura 15- Página de confirmação do processo de instalação.....	38
Figura 16- Tela de login do Zabbix.....	39
Figura 17- <i>Host</i> pré-configurado.....	40
Figura 18- Formulário de configuração de <i>host</i> .....	41
Figura 19- Formulário de configuração de <i>host</i> preenchido.....	42
Figura 20- Formulário para adição de <i>templates</i> ao <i>host</i> .....	43
Figura 21- Personalização do template.....	44
Figura 22- Formulário de configuração da ação.....	46
Figura 23- Condições para execução da ação.....	47
Figura 24- Formulário de configuração das operações.....	48
Figura 25- Topologia utilizada no ambiente testado.....	51
Figura 26- Log do serviço 'httpd' no Servidor Zabbix.....	52
Figura 27- Log do Agente Zabbix no Servidor Zabbix.....	53
Figura 28- Log do serviço 'mysql' no Servidor Apache.....	53
Figura 29- Log do Agente Zabbix no Servidor Apache.....	54
Figura 30- Log do serviço 'named' no Servidor DNS.....	54
Figura 31- Log do Agente Zabbix no Servidor DNS.....	55
Figura 32- Status do serviço 'dhcpd' no Servidor DHCP.....	55
Figura 33- Log do Agente Zabbix no Servidor DHCP.....	56
Figura 34- Status do serviço 'dhcpd' (reestabelecido).....	56
Figura 35- Log do serviço 'smb' no Servidor SAMBA.....	57
Figura 36- Log do Agente Zabbix no Servidor SAMBA.....	57
Figura 37- Status do serviço 'smb' (reestabelecido).....	57
Figura 38- <i>Dashboard</i> de monitoração.....	58



Figura 39- <i>Hosts</i> configurados para o monitoramento.....	59
Figura 40- Lista de ações configuradas.....	60

## LISTA DE TABELAS

Tabela 1- Versões existentes do protocolo SNMP.....	23
Tabela 2- <i>Hardware</i> indicado para o Servidor Zabbix.....	28

## LISTA DE QUADROS

Quadro 1- Resumo dos itens monitorados.....	50
Quadro 2- Resumo dos SO e dos serviços monitorados.....	51

## SUMÁRIO

<b>1. INTRODUÇÃO.....</b>	<b>13</b>
1.1 . OBJETIVOS.....	16
1.1.1 Objetivo Geral.....	17
1.1.2 Objetivos Específicos.....	17
1.2 JUSTIFICATIVA.....	17
<b>2. EMBASAMENTO TEÓRICO.....</b>	<b>19</b>
2.1 GERENCIAMENTO DE REDES.....	19
2.2 MODELO SNMP.....	20
2.2.1 Gerentes SNMP.....	21
2.2.2 Agentes SNMP.....	22
2.2.3 Operações SNMP.....	22
2.2.4 Versões.....	22
2.3 A SOLUÇÃO ZABBIX.....	23
2.3.1 Servidor Zabbix.....	23
2.3.2 Agente Zabbix.....	23
2.3.2.1 Tipos de verificação.....	24
2.3.3 Proxy Zabbix.....	24
2.3.4 Interface <i>Web</i> .....	25
<b>3. DESENVOLVIMENTO.....</b>	<b>27</b>
3.1 INSTALAÇÃO DO ZABBIX.....	27
3.1.1 Aquisição do Zabbix.....	27
3.1.2 Pré-Requisitos.....	27
3.1.3 Instalação a Partir de Pacotes.....	28
3.1.3.1 Instalação dos pacotes do Servidor Zabbix e da Interface <i>Web</i> .....	29
3.1.3.2 Criação do Banco de Dados.....	31
3.1.3.3 Instalação do Agente Zabbix.....	32
3.1.3.4 Ajuste de configuração do servidor.....	33
3.1.3.5 Complementação da instalação da Interface <i>Web</i> .....	34
3.2 CONFIGURAÇÃO DO ZABBIX.....	39
3.2.1 Adicionando um novo <i>host</i> .....	40
3.2.2 Adicionando templates ao <i>host</i> .....	43
3.2.3 Personalizando itens do <i>template</i> .....	44
3.2.4 Habilitando comandos remotos.....	45
3.2.4.1 Habilitando o comando 'sudo' para o usuário 'zabbix'.....	45
3.2.5 Criando nova ação.....	46
<b>4. RESULTADOS.....</b>	<b>49</b>
4.1 RESULTADOS OBTIDOS NO PROCESSO DE INSTALAÇÃO.....	49
4.1.1 Instalação do Servidor Zabbix.....	49

4.1.2 Instalação do Agente Zabbix.....	49
4.2 RESULTADOS OBTIDOS NA REALIZAÇÃO DOS TESTES.....	50
4.2.1 Realização de testes.....	52
4.2.1.1 Teste no Servidor Zabbix.....	52
4.2.1.2 Teste no Servidor Apache.....	53
4.2.1.3 Teste no Servidor DNS.....	54
4.2.1.4 Teste no Servidor DHCP.....	55
4.2.1.5 Teste no Servidor Samba.....	56
4.2.2 Alertas gerados pela Interface <i>Web</i> do Servidor Zabbix.....	58
4.2.3 Tela de configuração de <i>hosts</i> e ações.....	59
<b>5.CONCLUSÃO.....</b>	<b>61</b>
5.1 DIFICULDADES ENCONTRADAS.....	61
5.2 TRABALHOS FUTUROS.....	62
<b>REFERÊNCIAS.....</b>	<b>63</b>

## 1. INTRODUÇÃO

No início da concepção das redes de computadores, quando elas ainda eram objetos de pesquisa e diferentemente dos dias atuais, não eram utilizadas por milhões de pessoas diariamente, o termo 'gerenciamento de rede' era algo de que ainda não se tinha ouvido falar. Quando um problema de rede era identificado, testes simples como o '*ping*' eram utilizados para localizar a fonte do problema possibilitando sua manutenção (KUROSE, 2010, p. 554).

Ao se deparar com o crescimento da Internet pública, bem como das Intranets privadas, passando “de pequenas redes a grandes infraestruturas globais”, o gerenciamento da enorme quantidade de componentes de *hardware* e de *software* cresceu de importância (KUROSE, 2010, p. 554).

Existem, basicamente, três razões que podem tornar o gerenciamento da rede uma tarefa difícil (COMER, 2008, p. 536):

- Em primeiro lugar, na maioria das organizações, a Intranet é heterogênea, ou seja, contém *hardware* e *software* com componentes fabricados por várias empresas;
- Em segundo lugar está o avanço da tecnologia, que faz com que novos dispositivos e novos serviços apareçam constantemente;
- Em terceiro lugar, está o tamanho das redes, que pode significar que algumas partes da Intranet fiquem distantes geograficamente umas das outras, tornando a detecção da causa de um problema de comunicação em um dispositivo remoto uma tarefa difícil.

O gerente da rede, por vezes chamado de administrador da rede, é a pessoa responsável por planejar, instalar, operar, monitorar e controlar o *hardware* e todos os sistemas que compõem a rede de computadores ou Intranet da qual é responsável (COMER, 2008, p. 535).

Ao planejar uma rede, o gerente preocupa-se em atender os requisitos relacionados ao desempenho. Dentre as atribuições do gerente destacam-se o monitoramento de operações, a detecção e correção de problemas que podem tornar a comunicação ineficiente ou até mesmo inexistente, a continuada

preocupação para evitar condições que possam resultar em novos problemas (COMER, 2008, p. 535).

Outra situação que deve ser levada em conta ao planejar uma rede e seu monitoramento, é o fato de que muitos dispositivos de rede são concebidos para resolver problemas automaticamente. Os protocolos de rede, como o TCP, ignoram falhas de pacotes, restringindo-se a retransmitir aqueles que apresentem falha, o que pode fazer com que a perda intermitente de pacotes passe despercebida pelo gerente da rede, além de comprometer a largura de banda da rede (COMER, 2008, p. 536).

O monitoramento do ambiente de rede não deve restringir-se unicamente ao aspecto de um serviço estar ou não respondendo, ou um dispositivo estar ou não ligado. Deve ser levado em conta que falhas de *hardware* ou falhas de *software* podem causar problemas no ambiente de rede, um gerente de rede deve ter a preocupação de monitorar ambos (COMER, 2008, p. 535).

Após a criação pela *International Organization for Standardization* (ISO) do modelo de Interconexão de Sistemas Abertos (*Open Systems Interconnection* – OSI), que tinha como principal objetivo garantir a comunicação entre os dispositivos em uma rede, particularmente àquele estabelecido pelo Modelo Funcional, foram desenvolvidos diversos modelos de gerenciamento de redes (KUROSE, 2010, p. 39).

A partir da publicação pela União Internacional de Telecomunicações (UIT) da recomendação M.3400<sup>1</sup>, foi criado o modelo de gerenciamento FCAPS, cuja sigla deriva das iniciais em inglês de cada aspecto de gerenciamento que o modelo propõe (COMER, 2008, p. 536).

O modelo de gerenciamento FCAPS serviu de base para todos os demais modelos de gerenciamento, por ter definido as áreas funcionais da gerências de redes, que são (COMER, 2008, p. 537):

- Detecção de falhas e correção: detecção de falhas e correção para grande parte do aspecto operacional do gerenciamento de rede;
- Configuração e operação: garantir o controle e monitorar as condições do ambiente de rede;

---

<sup>1</sup>M.3400 faz parte de uma série de normas que especificam como o gerenciamento de redes de telecomunicações deve ser configurado e operado (ITU, 2000).

- Contabilização e faturamento: gerencia a contabilidade e o faturamento;
- Ajustes de performance e otimização: garantir a qualidade dos serviços acordados;
- Garantia de segurança e proteção: gerencia os aspectos relativos à garantia da segurança.

Para que seja possível monitorar um dispositivo de rede, basicamente o gerente da rede configura um dispositivo alvo da monitoração para que envie um alerta quando determinados limites pré-estabelecidos forem atingidos, como por exemplo, a utilização de um *link* de rede atinge 80% da carga máxima, conseqüentemente, uma ferramenta de monitoração passa a exibir um alerta na estação de trabalho do gerente (COMER, 2008, p. 539).

A maioria das ferramentas de gerenciamento de rede operam através de uma rede, estando no mesmo local do gerente da rede e utilizando-se da mesma tecnologia para comunicar-se com um determinado elemento da rede (COMER, 2008, p. 540).

Sempre que um gerente precisa de informações sobre um dispositivo da rede que está sendo monitorado, este executa um *software* no servidor, que atua como cliente, e um programa que está no dispositivo monitorado, é executado e atua como servidor (COMER, 2008, p. 540).

A arquitetura cliente-servidor permite o uso de protocolos convencionais, como o TCP e o UDP para interagirem, dispensando a construção de uma rede separada e possibilitando a utilização da própria rede de produção no monitoramento (COMER, 2008, p. 540).

As informações de gerenciamento que residem em uma entidade gerenciada de rede, necessitam ser padronizadas para assegurar que a sintaxe e a semântica dos dados de gerenciamento sejam bem definidos e não apresentem ambigüidade. Partindo deste princípio, foi criada uma linguagem de definição, chamada de Estrutura de Informações de Gerenciamento (*Structure of Management Information - SMI*) (KUROSE, 2010, p. 561).

Após o estabelecimento do SMI, foi possível desenvolver uma solução de monitoramento centralizada, que pudesse monitorar todo o ambiente de rede, tanto



*hardware* quanto *software* bem como seus componentes. Sob este conceito, Alexei Vladishev criou o Zabbix, “uma solução de código aberto de nível empresarial que possibilita o monitoramento de praticamente qualquer componente do ambiente de rede”, e que também suporta o monitoramento distribuído (VLADISHEV, 2016, Cap. 1).

Com o Zabbix é possível monitorar vários parâmetros da rede e dos servidores, bem como a saúde dos serviços. O mecanismo de notificação permite configurar alertas para praticamente qualquer evento, proporcionando a rápida reação aos problemas apresentados (VLADISHEV, 2016, Cap. 1).

“O Zabbix suporta tanto “*pooling*” quanto “*trapping*””. A comunicação por *pooling*, é aquela centralizada a partir do servidor Zabbix e executada em intervalos regulares, já o *trapping* são os processos executados localmente nos *hosts* monitorados e enviados ao servidor Zabbix para processamento. A interface *web* possibilita o acompanhamento de relatórios e estatísticas, bem como a verificação dos parâmetros de configuração (VLADISHEV, 2016, Cap. 1).

Através da interface *web* é possível “avaliar o estado da rede e a saúde dos servidores a partir de qualquer local”. A solução Zabbix pode ser empregada no monitoramento tanto de pequenas organizações com alguns servidores quanto para grandes empresas, com milhares de servidores (VLADISHEV, 2016, Cap 1).

Um dos problemas enfrentados por empresas de pequeno, médio e grande porte, é a necessidade de monitorar seus sistemas informatizados e sua infraestrutura de TI, de forma a evitar a ocorrência de indisponibilidade decorrente de falhas que poderiam ter sido evitadas.

Sendo assim, a proposta consiste em monitorar um ambiente de rede, particularmente quanto ao reestabelecimento de serviços que tenham apresentado falha, utilizando o Zabbix, que é “uma solução de monitoração integrada, que provê diversos recursos de monitoração em um único pacote” (VLADISHEV, 2016, Cap. 1).

## 1.1 . OBJETIVOS

Os objetivos geral e específicos serão descritos abaixo.

### 1.1.1 Objetivo Geral

Monitorar o servidor e o agente Zabbix em um ambiente de rede.

### 1.1.2 Objetivos Específicos

- Instalar e configurar o Servidor Zabbix versão 3.0 LTS em um servidor previamente configurado com o (SO) Sistema Operacional CentOS 7 x86\_64;
- Instalar e configurar o Agente Zabbix nas estações que serão monitoradas: Servidor Zabbix, Servidor DNS, Servidor DHCP, Servidor de Arquivos Samba, Servidor Web Apache;
- Testar o funcionamento do sistema de monitoramento no Servidor DNS, Servidor DHCP, Servidor de Arquivos Samba, Servidor *Web* Apache e no Servidor Zabbix;
- Analisar a atuação do Servidor Zabbix e do Agente Zabbix relativa às informações apresentadas bem como a correção dos incidentes criados e reestabelecimento dos serviços que apresentem falha.

O Zabbix deverá monitorar o ambiente emitindo alertas sobre os incidentes verificados, atuando automaticamente no *host* monitorado, por intermédio do Agente Zabbix, atuando desta forma no reestabelecimento dos serviços que apresentem falha.

Espera-se demonstrar que o Zabbix pode ser utilizado como uma ferramenta de monitoramento proativo, eliminando a dependência da ação direta do administrador da rede para corrigir as falhas apresentadas pelo sistema monitorado, particularmente quanto ao reestabelecimento de serviços.

## 1.2 JUSTIFICATIVA

O monitoramento proativo visa contribuir para a diminuição das ocorrências de indisponibilidade no ambiente de rede, uma vez que alerta o administrador do

sistema sobre os locais onde poderão ocorrer falhas e em alguns casos, atua automaticamente para o reestabelecimento do serviço.

Por vezes, o administrador da rede pode ter uma quantidade de dispositivos muito grande conectados em sua rede, uma vez que os cenários envolvendo TI (Tecnologia da Informação) são cada vez mais complexos.

Buscando maximizar a eficiência e a produtividade dos sistemas informatizados em sua área de responsabilidade, o administrador necessita de uma ferramenta que além de mostrar o componente da rede que apresenta falha, seja capaz de, segundo critérios estabelecidos, atuar sobre os serviços ou ativos de rede, de forma a, por exemplo, reiniciar um serviço que tenha parado de responder, ou avisar sobre um disco rígido que está com pouco espaço de armazenamento ou com indícios de que falhará em breve.

## 2. EMBASAMENTO TEÓRICO

Neste capítulo, serão vistos os principais conceitos e tecnologias relacionados ao monitoramento de redes, que serve como base para o entendimento da solução de monitoramento proposta.

### 2.1 GERENCIAMENTO DE REDES

O gerenciamento de redes envolve ações visando garantir o controle sobre a situação dos componentes que compõem um ambiente de rede.

O objetivo da Gerência de Redes é monitorar e controlar os elementos da rede (sejam eles físicos ou lógicos), assegurando um certo nível de qualidade de serviço. Para realizar esta tarefa, os gerentes de redes são geralmente auxiliados por um sistema de gerência de redes. Um sistema de gerência de rede pode ser definido como uma coleção de ferramentas integradas para a monitoração e controle da rede. Este sistema oferece uma interface única, com informações sobre a rede e pode oferecer também um conjunto poderoso e amigável de comandos que são usados para executar quase todas as tarefas da gerência da rede (STALLINGS, 1998 apud LOPES; SAUVE; NICOLLETTI, 2003, p. 17).

A arquitetura geral que compõem os sistemas de gerência de redes pode ser definida por quatro componentes básicos: “elementos gerenciados, estações de gerência, protocolos de gerência e informações de gerência” (LOPES; SAUVE; NICOLLETTI, 2003, p. 17).

- **Elementos gerenciados:** São os que “possuem um software especial chamado agente”, que por sua vez “permite que o equipamento seja monitorado e controlado através de uma ou mais estações de gerência” (LOPES; SAUVE; NICOLLETTI, 2003, p. 17);

- **Estações de gerência:** Nos “sistemas de gerência distribuídos existem duas ou mais estações de gerência”, já nos sistemas centralizados, que são mais comuns, existe apenas uma. São chamados de “gerentes os *softwares* da estação de gerência que conversam diretamente com os agentes” que estão instalados nos elementos gerenciados, esse acesso pode ter como objetivo monitorá-los, bem

como controlá-los. Uma interface é oferecida pela estação de gerência através da qual usuários previamente autorizados podem gerenciar a rede (LOPES; SAUVE; NICOLLETTI, 2003, p. 17);

- **Protocolo de gerência:** Uma linguagem comum entre gerente e agente que permite o monitoramento (leitura) e controle (escrita) (LOPES; SAUVE; NICOLLETTI, 2003, p. 17);

- **Informação de gerência:** Tratam-se dos “dados que podem ser referenciados em operações do protocolo de gerência, isto é, dados sobre os quais gerente e agente conversam” (LOPES; SAUVE; NICOLLETTI, 2003, p. 17).

A figura 1 mostra os principais componentes de uma arquitetura de gerenciamento de rede.

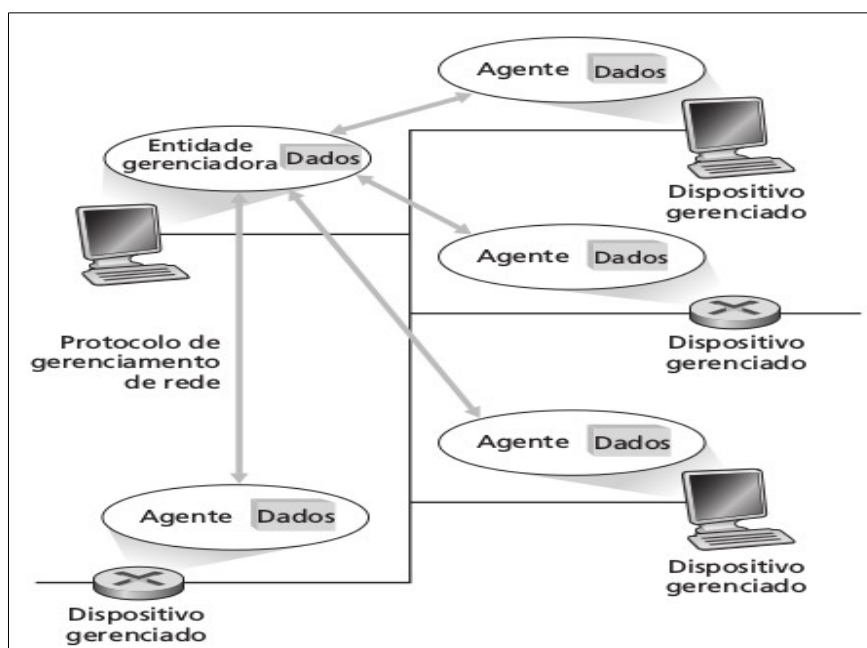


Figura 1- Exemplo de arquitetura de gerenciamento de rede  
Fonte: Kurose, 2010, p. 558

## 2.2 MODELO SNMP

Com o crescimento das redes de computadores, as dificuldades de gerenciamento aumentaram consideravelmente. “A demora no aparecimento de soluções abertas baseadas no modelo OSI fez com que um grupo de engenheiros

decidissemos elaborar uma solução temporária baseada num novo protocolo, o SNMP” (LOPES; SAUVE; NICOLLETTI, 2003, apêndice 1, p. 16).

A padronização de solução de gerência mais usada no mundo chama-se *Internet-Standard Network Management Framework*. Esta solução é mais conhecida como Gerência SNMP. O SNMP é o protocolo de gerência deste padrão. Este padrão descreve não apenas o protocolo de gerência, mas também um conjunto de regras que são usadas para definir as informações de gerência e um conjunto inicial de informações de gerência que já podem ser utilizadas (ROSE, 1995 apud LOPES; SAUVE; NICOLLETTI, 2003, p. 18).

Nos dias atuais, praticamente todos os dispositivos que compõem o ambiente de rede dão suporte ao SNMP (LOPES; SAUVE; NICOLLETTI, 2003, apêndice 1, p. 16).

Segundo Lopes (2003, apêndice 1, p. 18), o mundo SNMP está baseado em três documentos:

- “**Structure of Management Information**. Definido pela RFC 1155, a SMI define essencialmente, a forma pela qual a informação gerenciada é definida.”

- “**Management Information Base (MIB)** principal. Definida na RFC 1156, a MIB principal do mundo SNMP (chamada MIB-2) define as variáveis de gerência que todo elemento gerenciado deve ter, independentemente de sua função particular [...]”

- “**Simple Network Management Protocol (SNMP)**. Definido pela RFC 1157, é o protocolo usado entre gerente e agente para a gerência, principalmente trocando valores de variáveis de gerência.”

### 2.2.1 Gerentes SNMP

Executa sondagens periódicas (*pollings*) nos agentes de “todos os elementos gerenciados”, descobrindo desta forma “a existência de eventos anormais nos elementos” (LOPES; SAUVE; NICOLLETTI, 2003, apêndice 1, p. 18).

### 2.2.2 Agentes SNMP

O agente fornece informações de gerenciamento às estações de gerenciamento NMS, mantendo o controle de vários aspectos operacionais do dispositivo monitorado (Mauro & Shimidt, 2001, p. 11).

Na figura 2 vemos o fluxo de informações entre a Estação de Gerenciamento NMS e o Agente.

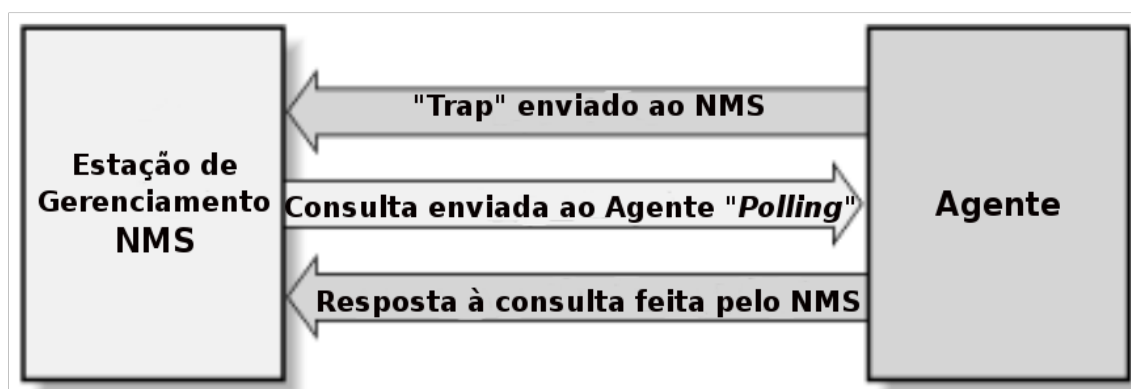


Figura 2- Relacionamento entre o Gerente e o Agente

Fonte: Mauro & Shimidt, 2001, p. 11

### 2.2.3 Operações SNMP

O funcionamento do protocolo SNMP segue o modelo chamado “modelo de leitura escrita” ou “modelo *fetch-store*”. A comunicação entre agente e gerente acontece através de três operações, quais sejam o GET, utilizado para “ler o valor de uma variável de gerência”, o SET, utilizado “para alterar seu valor” e o TRAP, quando a estação que implementa o agente, envia dados não solicitados à estação gerente (geralmente servindo como Alerta) (LOPES; SAUVE; NICOLLETTI, 2003, apêndice 1, p. 18 e 19).

### 2.2.4 Versões

Segundo Frye *et al*, (2003, p. 4 e 5) atualmente coexistem 3 versões do SNMP.

Tabela 1- Versões existentes do protocolo SNMP

Versão	Data	RFCs	Operações Suportadas
V1	1990	1157, 1155, 1212 e 1215	<i>get, get-next, set, get-response</i> e <i>trap</i>
V2	1996	2578-2580, 3416-3418 e 1901*	<i>get-bulk, inform, notification</i> e <i>report</i>
V3	1999	3411, 3412, 3413, 3414 e 3415	

Fonte: Frye et al, 2003, p. 4 e 5

\* trata-se uma definição experimental para usar SNMPv2, referida como SNMPv2c.

## 2.3 A SOLUÇÃO ZABBIX

O Zabbix é uma solução de monitoramento de rede de nível empresarial, “de código aberto e com suporte a monitoração distribuída” (VLADISHEV, 2016, Cap. 1).

### 2.3.1 Servidor Zabbix

“Servidor Zabbix é o componente central da solução e, em ambientes centralizados, os agentes enviam os dados coletados (sobre integridade, disponibilidade e estatísticos) para ele” (VLADISHEV, 2016, Cap 1).

O servidor é responsável pelo gerenciamento e pela coleta e recebimento de dados, pelo cálculo do estado das *triggers*, e pelo envio de notificações aos usuários (VLADISHEV, 2016, Cap. 2).

“O servidor também pode executar por si só verificações remotas nos dispositivos monitorados, estas verificações ocorrem quando se utiliza itens do tipo “verificação simples”” (VLADISHEV, 2016, Cap 2).

### 2.3.2 Agente Zabbix

O Agente Zabbix é o componente da solução de monitoramento que “é instalado no dispositivo alvo da monitoração. Possui capacidade de monitorar ativamente os recursos e aplicações locais (discos e partições, memória, estatísticas do processador, etc)” (VLADISHEV, 2016, Cap 2).



“O agente concentra as informações locais sobre o dispositivo monitorado para posterior envio ao servidor ou *Proxy Zabbix* (dependendo da configuração)” (VLADISHEV, 2016, Cap 2).

Em caso de falhas ou mau funcionamento em algum componente do dispositivo monitorado, “o servidor Zabbix pode alertar ativamente os administradores do ambiente sobre o ocorrido” (VLADISHEV, 2016, Cap. 2).

### 2.3.2.1 Tipos de verificação

Existem duas formas utilizadas pelos agentes para realizar as verificações (VLADISHEV, 2016, Cap. 2):

- Verificação Ativa: “O agente precisa primeiro receber a lista de itens a monitorar e o intervalo entre coletas pretendido. Esta informação vem do servidor Zabbix através de requisições periódicas do agente.”
- Verificação Passiva: “O servidor ou o *proxy* Zabbix requisitam o dado toda vez que é necessário (uso de CPU, memória, disco, etc), o agente responde com o resultado do teste solicitado”.

### 2.3.3 Proxy Zabbix

O *Proxy Zabbix* é um Servidor Zabbix configurado para funcionar como “um processo que pode receber dados de um ou mais dispositivos monitorados e enviar ao servidor Zabbix”, assim sendo, para os agentes monitorados “o *proxy* passa a ser o servidor Zabbix”. Os dados de monitoramento coletados dos agentes são armazenados no *proxy* e posteriormente enviados ao servidor Zabbix ao qual ele pertence, sendo excluídos na sequência (VLADISHEV, 2016, Cap. 2).

“A utilização deste componente é opcional, mas normalmente é muito benéfica pois distribui a carga de monitoração normalmente atribuída ao Zabbix *Server*” (VLADISHEV, 2016, Cap. 2).

“O *Proxy Zabbix* é a solução ideal para a monitoração centralizada de localidades geograficamente dispersas e para redes gerenciadas remotamente” (VLADISHEV, 2016, Cap. 2).

O uso do Proxy Zabbix requer um banco de dados local, que pode ser SQLite, MySQL ou PostgreSQL, que são suportados nativamente. Ainda assim, é possível utilizar outros banco de dados, como o Oracle ou IBM DB2, porém, nestes casos os riscos e limitações devem ser analisados criteriosamente (VLADISHEV, 2016, Cap. 2).

Na figura 3 vemos um exemplo de utilização de um Proxy Zabbix utilizado para monitorar um conjunto remoto de servidores.

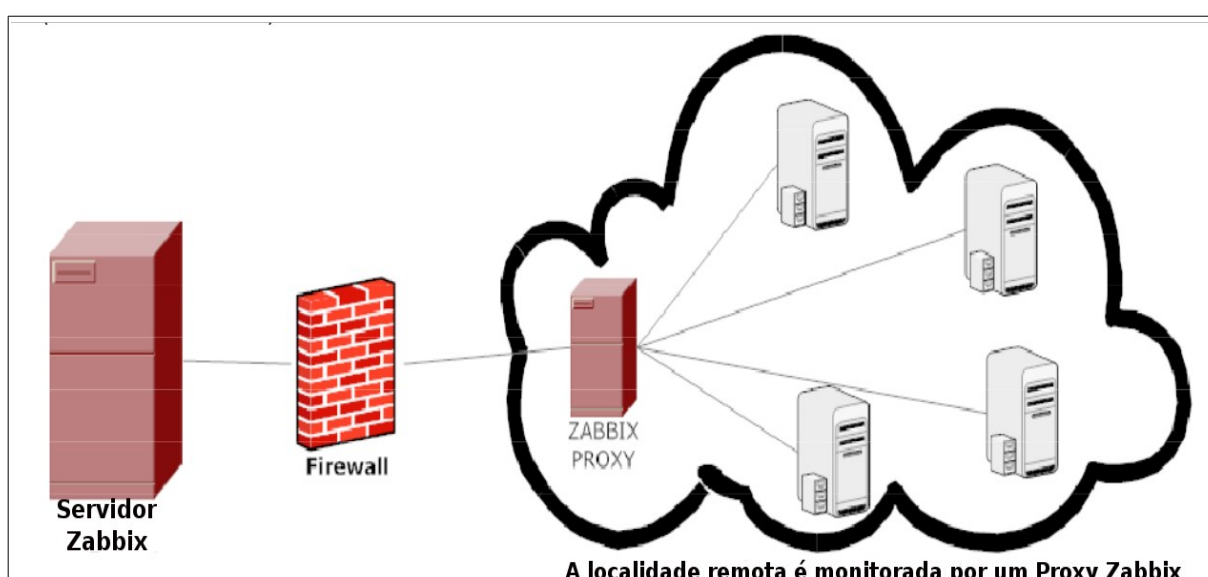


Figura 3- Modelo de utilização do Proxy Zabbix

Fonte: Zabbix Brasil, 2016

#### 2.3.4 Interface Web

Levando em conta que os dispositivos e serviços a serem monitorados estão em um ambiente de rede, a aplicação Zabbix conta com uma interface web, acessível através de qualquer navegador, que foi idealizada e desenvolvida “para possibilitar um fácil acesso a partir de qualquer plataforma” e possibilitar o gerenciamento do Zabbix através desta interface” (VLADISHEV, 2016, Cap 17).

Na figura 4 pode-se ver a tela principal do Servidor Zabbix, onde visualiza-se o 'Dashboard' da aba 'Monitoramento', página que mostra de forma prática e agrupada, um resumo das ocorrências de todo o ambiente monitorado.

The screenshot displays the Zabbix web interface dashboard. The top navigation bar includes 'Monitoring', 'Inventory', 'Reports', 'Configuration', and 'Administration'. The main dashboard is divided into several sections:

- Favourite maps:** Local network
- Favourite graphs:** New host: CPU load
- Favourite screens:** Zabbix server
- Last 20 issues:**

HOST	ISSUE	LAST CHANGE	AGE	INFO	ACK	ACTIONS
Zabbix server 1	Version of zabbix-agent(d) was changed on Zabbix server 1	2016-01-11 22:36:06	1m 39s		No	1
Zabbix server 1	Lack of free swap space on Zabbix server 1	2015-08-11 23:29:28	5m 3d		Yes 4	
- System status:**

HOST GROUP	DISASTER	HIGH	AVERAGE	WARNING	INFORMATION	NOT CLASSIFIED
Discovered hosts	0	0	0	1	1	0
Network devices	0	0	0	0	0	0
SNMP hosts	0	0	0	0	0	0
Zabbix servers	0	0	0	1	1	0
- Host status:**

HOST GROUP	WITHOUT PROBLEMS	WITH PROBLEMS	TOTAL
Discovered hosts	7	1	8
Network devices	1	0	1
SNMP hosts	2	0	2
Zabbix servers	0	1	1
- Discovery status:**

DISCOVERY RULE	UP	DOWN
Local network2	6	1
- Status of Zabbix:**

PARAMETER	VALUE	DETAILS
Zabbix server is running	Yes	localhost10051
Number of hosts (enabled/disabled/templates)	54	10 / 1 / 43
Number of items (enabled/disabled/not supported)	356	350 / 0 / 6
Number of triggers (enabled/disabled/problemok)	95	94 / 1 / 2 / 92
Number of users (online)	3	2
Required server performance, new values per second	4.79	
- Web monitoring:**

HOST GROUP	OK	FAILED	UNKNOWN
Discovered hosts	1	0	0
Zabbix servers	1	0	0

**Figura 4- Interface Web do Servidor Zabbix**  
**Fonte: Zabbix, 2016**

### 3. DESENVOLVIMENTO

#### 3.1 INSTALAÇÃO DO ZABBIX

A instalação do Servidor Zabbix e do Agente Zabbix, será feita sobre o SO CentOS 7 64 *bits*, com base nos pacotes existentes no repositório oficial.

##### 3.1.1 Aquisição do Zabbix

Os pacotes oficiais de instalação no formato RPM estão disponíveis para *download* em <<http://repo.zabbix.com>>. Os repositórios no formato **yum** que serão utilizados para a instalação dos pacotes Zabbix, também estão disponíveis neste servidor. Após a instalação do repositório oficial na distribuição que irá receber a instalação do Servidor Zabbix, este estará disponível para ser instalado a partir do gerenciador de pacotes (VLADISHEV, 2016, Cap. 3).

##### 3.1.2 Pré-Requisitos

Para instalar o Servidor Zabbix existem requisitos mínimos de memória (128MB) e de armazenamento em disco rígido (256MB). Ressalta-se, porém, que a quantidade de memória e de espaço em disco necessários, dependerá da quantidade de *hosts* e de parâmetros monitorados pelo Zabbix (VLADISHEV, 2016, Cap. 3).

“Cada processo *daemon* do Servidor Zabbix irá requerer diversas conexões com o servidor de banco de dados. A quantidade de memória alocada para cada conexão dependerá das configurações da *engine* do SGBD”, desta forma, ao dimensionar o Servidor Zabbix, o gerente da rede deve levar em consideração a extensão do ambiente que será monitorado (VLADISHEV, 2016, Cap. 3).

A tabela 2 mostra exemplos de configuração para o Servidor Zabbix em função da quantidade de *hosts* monitorados.

**Tabela 2: Hardware indicado para o Servidor Zabbix**

Tamanho	Plataforma	CPU/Memória	SGDB	Nr Hosts
Pequeno	CentOS	Sistema Virtualizado	MySQL InnoDB	100
Médio	CentOS	2 núcleos CPU/2GB	MySQL InnoDB	500
Grande	RedHat Enterprise Linux	4 núcleos CPU/8GB	RAID10 MySQL InnoDB ou PostgreSQL	>1000
Muito Grande	RedHat Enterprise Linux	8 núcleos CPU/16GB	RAID10 rápido MySQL InnoDB ou PostgreSQL	>10000

Fonte: Vladishev, 2016, Cap. 3

### 3.1.3 Instalação a Partir de Pacotes

Para instalar os pacotes Zabbix, é necessário instalar previamente o pacote de configuração do repositório, que contém os arquivos de configuração do *yum*.

A instalação é feita a partir do terminal do SO, com um usuário que tenha privilégios de *root*, digitando a linha de comando “`rpm -ivh http://repo.zabbix.com/zabbix/3.0/rhel/7/x86_64/zabbix-release-3.0-1.el7.noarch.rpm`” conforme mostra a figura 5 (VLADISHEV, 2016, Cap. 3):

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
[root@localhost admin]# rpm -ivh http://repo.zabbix.com/zabbix/3.0/rhel/7/x86_64/zabbix-release-3.0-1.el7.noarch.rpm
Obtendo http://repo.zabbix.com/zabbix/3.0/rhel/7/x86_64/zabbix-release-3.0-1.el7.noarch.rpm
aviso: /var/tmp/rpm-tmp.DMxBVC: Cabeçalho V4 DSA/SHA1 Signature, ID da chave 79ea5ed4: NOKEY
Preparando... ##### [100%]
Updating / installing...
 1:zabbix-release-3.0-1.el7 ##### [100%]
[root@localhost admin]#
```

**Figura 5- Instalação repositório yum**  
Fonte: Zabbix, 2016

### 3.1.3.1 Instalação dos pacotes do Servidor Zabbix e da Interface Web

A partir da instalação do repositório, os pacotes Zabbix já estarão disponíveis para instalação.

Antes da instalação propriamente dita, é necessário atualizar a lista de *softwares* dos repositórios com o comando “*yum update*”, como mostra a figura 6.

```

Arquivo Editar Ver Pesquisar Terminal Ajuda
[root@localhost admin]# yum update
Plugins carregados: fastestmirror, langpacks
zabbix | 951 B 00:00:00
zabbix-non-supported | 951 B 00:00:00
(1/2): zabbix/x86_64/primary | 4.7 kB 00:00:00
(2/2): zabbix-non-supported/x86_64/primary | 1.6 kB 00:00:01
Loading mirror speeds from cached hostfile
* base: centos.xpg.com.br
* extras: centos.xpg.com.br
* updates: centos.xpg.com.br
zabbix 27
/27
zabbix-non-supported
4/4
No packages marked for update
[root@localhost admin]#

```

**Figura 6- Atualização dos repositórios**  
**Fonte: Zabbix, 2016**

Após atualizados os repositórios, os pacotes Servidor Zabbix e a Interface Web já podem ser instalados com o comando “*yum install zabbix-server-mysql zabbix-web-mysql*”, como mostra a figura 7.

```

Arquivo Editar Ver Pesquisar Terminal Ajuda
[root@localhost admin]# yum install zabbix-server-mysql zabbix-web-mysql
Plugins carregados: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
* base: centos.xpg.com.br
* extras: centos.xpg.com.br
* updates: centos.xpg.com.br
Resolvendo dependências

```

**Figura 7- Instalação do Servidor Zabbix e Interface Web**  
**Fonte: Zabbix, 2016**

Verifica-se ao final da figura 7, a sentença “Resolvendo dependências”, esta etapa varia dependendo dos pacotes já instalados no sistema base, porém, todas as dependências devem ser resolvidas para que o Zabbix funcione corretamente. Na figura 8 pode-se verificar as dependências instaladas no SO em questão.

```

Dependências resolvidas
=====
Package                Arq.      Versão      Repo          Tam.
=====
Instalando:
zabbix-server-mysql    x86_64    3.0.1-1.el7    zabbix        1.7 M
zabbix-web-mysql       noarch    3.0.1-1.el7    zabbix        3.5 k
Instalando para as dependências:
OpenIPMI-libs          x86_64    2.0.19-11.el7    base          501 k
OpenIPMI-modalias      x86_64    2.0.19-11.el7    base          15 k
apr                     x86_64    1.4.8-3.el7      base          103 k
apr-util                x86_64    1.5.2-6.el7      base          92 k
fping                   x86_64    3.10-1.el7       zabbix-non-supported  40 k
httpd                   x86_64    2.4.6-40.el7.centos    base          2.7 M
httpd-tools            x86_64    2.4.6-40.el7.centos    base          82 k
iksemel                 x86_64    1.4-2.el7.centos    zabbix-non-supported  49 k
libzip                  x86_64    0.10.1-8.el7     base          48 k
mailcap                 noarch    2.1.41-2.el7     base          31 k
php                     x86_64    5.4.16-36.el7_1   base          1.4 M
php-bcmath              x86_64    5.4.16-36.el7_1   base          56 k
php-cli                 x86_64    5.4.16-36.el7_1   base          2.7 M
php-common              x86_64    5.4.16-36.el7_1   base          563 k
php-gd                  x86_64    5.4.16-36.el7_1   base          126 k
php-ldap                x86_64    5.4.16-36.el7_1   base          51 k
php-mbstring            x86_64    5.4.16-36.el7_1   base          503 k
php-mysql               x86_64    5.4.16-36.el7_1   base          99 k
php-pdo                 x86_64    5.4.16-36.el7_1   base          97 k
php-xml                 x86_64    5.4.16-36.el7_1   base          124 k
t1lib                   x86_64    5.1.2-14.el7     base          166 k
unixODBC                x86_64    2.3.1-11.el7     base          413 k
zabbix-web              noarch    3.0.1-1.el7     zabbix        3.3 M

Resumo da transação
=====
Instalar 2 Packages (+23 Dependent packages)

Tamanho total do download: 15 M
Tamanho depois de instalado: 65 M
Is this ok [y/d/N]: █

```

**Figura 8- Relação de dependências instaladas**  
**Fonte: Zabbix, 2016**

Neste ponto, basta pressionar a tecla “y” e aguardar o término da instalação.

### 3.1.3.2 Criação do Banco de Dados

Será utilizado o banco de dados MariaDB, previamente instalado no SO. Durante a instalação do Servidor Zabbix, é necessário que seja criado um banco de dados que será utilizado pela aplicação (VLADISHEV, 2016, Cap. 3).

Para criar o banco de dados é necessário executar a seguinte sequência de comandos no *shell* do SO (VLADISHEV, 2016, Cap. 3):

```
$> mysql -uroot -psenha*  
mysql> create database zabbix character set utf8 collate utf8_bin;  
mysql> grant all privileges on zabbix.* to zabbix@localhost identified by  
'senha'2;  
mysql> quit;
```

Feito isso, o banco de dados está criado, porém vazio, sendo necessário preenchê-lo com as informações necessárias ao funcionamento da aplicação. Para tanto o banco de dados deve ser populado com base no arquivo de informações que acompanha o pacote Zabbix instalado (VLADISHEV, 2016, Cap. 3).

Para popular a base de dados é necessário executar o seguinte comando no terminal do SO, com um usuário que tenha privilégios de *root*:

```
#> zcat /usr/share/doc/zabbix-server-mysql-3.0.1/create.sql.gz | mysql -u  
root -p zabbix
```

Após executar o comando acima, será solicitada a senha do usuário *root* do banco de dados. Este comando aplica o esquema '**sql**' existente no arquivo compactado de nome '**create.sql.gz**' à base de dados de nome '**zabbix**', que estava vazia até então.

---

<sup>2</sup> A palavra 'senha' deve ser substituída pela senha do usuário *root* do SO



### 3.1.3.3 Instalação do Agente Zabbix

Análogo à instalação do Servidor Zabbix, a partir da instalação do pacote de configuração do repositório oficial, o pacote do agente Zabbix fica disponível para instalação através do comando 'yum install zabbix-agent', executado a partir de um terminal, por um usuário com privilégios de *root* (VLADISHEV, 2016, Cap. 3).

O pacote de instalação do agente também pode ser baixado diretamente do repositório oficial do Zabbix e instalado manualmente através de um terminal, bastando para isso que seja observada a versão correspondente ao *kernel* do SO instalado.

A figura 9 mostra o processo de instalação do Agente Zabbix através do pacote disponível no repositório oficial.

```

Arquivo Editar Ver Pesquisar Terminal Ajuda
[root@localhost admin]# yum install zabbix-agent
Plugins carregados: fastestmirror, langpacks
base | 3.6 kB 00:00:00
extras | 3.4 kB 00:00:00
updates | 3.4 kB 00:00:00
Loading mirror speeds from cached hostfile
* base: centos.xpg.com.br
* extras: centos.xpg.com.br
* updates: centos.xpg.com.br
Resolvendo dependências
--> Executando verificação da transação
---> 0 pacote zabbix-agent.x86_64 0:3.0.1-1.el7 será instalado
--> Resolução de dependências finalizada

Dependências resolvidas

=====
Package           Arq.           Versão           Repo             Tam.
=====
Instalando:
zabbix-agent      x86_64         3.0.1-1.el7     zabbix           320 k
Resumo da transação
=====
Instalar 1 Package

Tamanho total do download: 320 k
Tamanho depois de instalado: 1.0 M
Is this ok [y/d/N]: █

```

**Figura 9- Instalação do agente Zabbix**  
**Fonte: Zabbix, 2016**

Neste ponto basta pressionar a tecla “y” e aguardar o término da instalação.

### 3.1.3.4 Ajuste de configuração do servidor

Faz-se necessário o ajuste em algumas configurações para que a aplicação funcione corretamente.

É necessário iniciar o servidor Zabbix, o agente Zabbix e o servidor Web, bem como configurá-los para iniciar automaticamente após o reinício do sistema. Para realizar essa alteração, é necessário digitar os seguintes comandos em um terminal, com um usuário com privilégios de *root*:

```
# systemctl start mariadb
# systemctl start httpd
# systemctl start zabbix-server
# systemctl start zabbix-agent
# systemctl enable mariadb
# systemctl enable httpd
# systemctl enable zabbix-server
# systemctl enable zabbix-agent
```

É necessário ajustar o arquivo de configuração do servidor Zabbix, localizado em `/etc/zabbix/zabbix_server.conf`, realizando as seguintes alterações (VLADISHEV, 2016, apêndice 3):

Antes:

```
# DBHost=localhost
DBName=zabbix
DBUser=zabbix
# DBPassword=
```

Depois:

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=senha
```

É necessário ajustar o arquivo de configuração do agente Zabbix, localizado em `/etc/zabbix/zabbix_agentd.conf`, realizando as seguintes alterações (VLADISHEV, 2016, apêndice 3):

<p>Antes:</p> <pre># Server= # ServerActive= # Hostname=</pre>
<p>Depois:</p> <pre>Server=127.0.0.1 ServerActive=127.0.0.1 Hostname=localhost</pre>

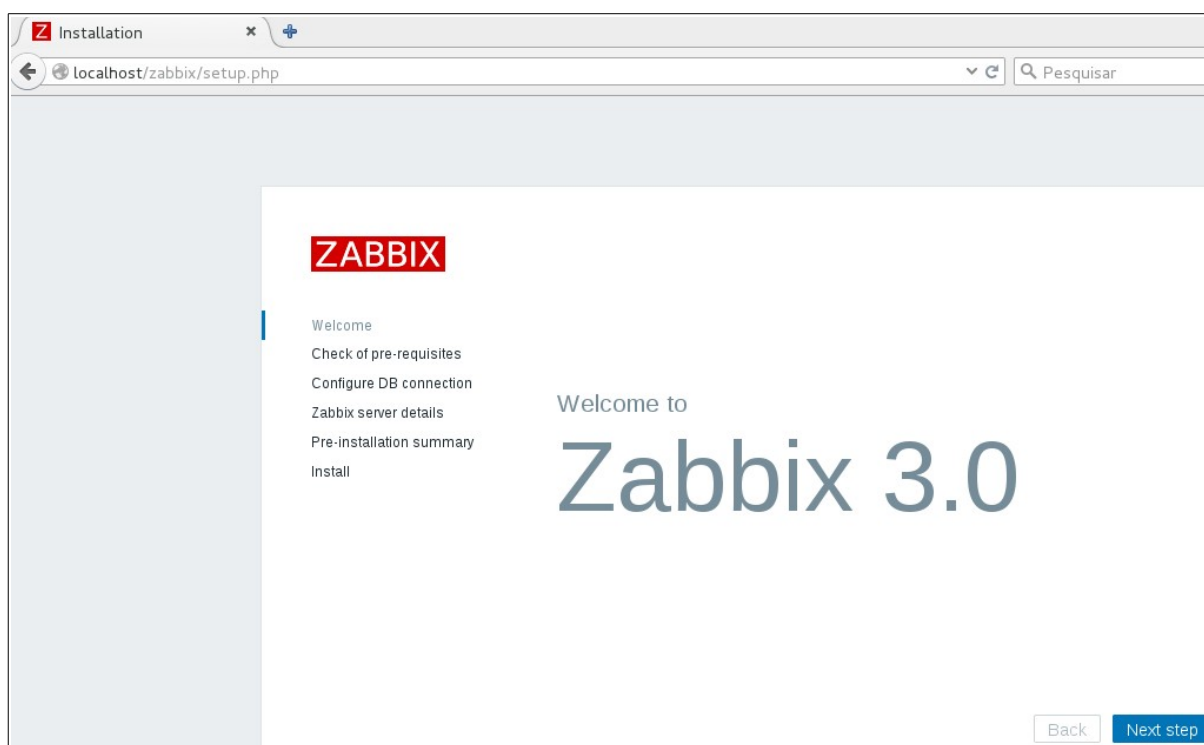
As modificações no arquivo `zabbix_agentd.conf` devem ser feitas em todas as estações onde o agente Zabbix for instalado (VLADISHEV, 2016, Cap. 3).

### 3.1.3.5 Complementação da instalação da Interface *Web*

O pacote da Interface *Web* já foi instalado, porém ela precisa ser configurada diretamente no navegador, onde serão inseridos os parâmetros de configuração da aplicação (VLADISHEV, 2016, Cap 3).

Para configurar a Interface *Web*, basta acessar o endereço *web* do servidor a partir do navegador, que neste caso específico encontra-se no próprio servidor Zabbix.

A figura 10 mostra a tela de boas vindas do instalador da Interface *Web*.



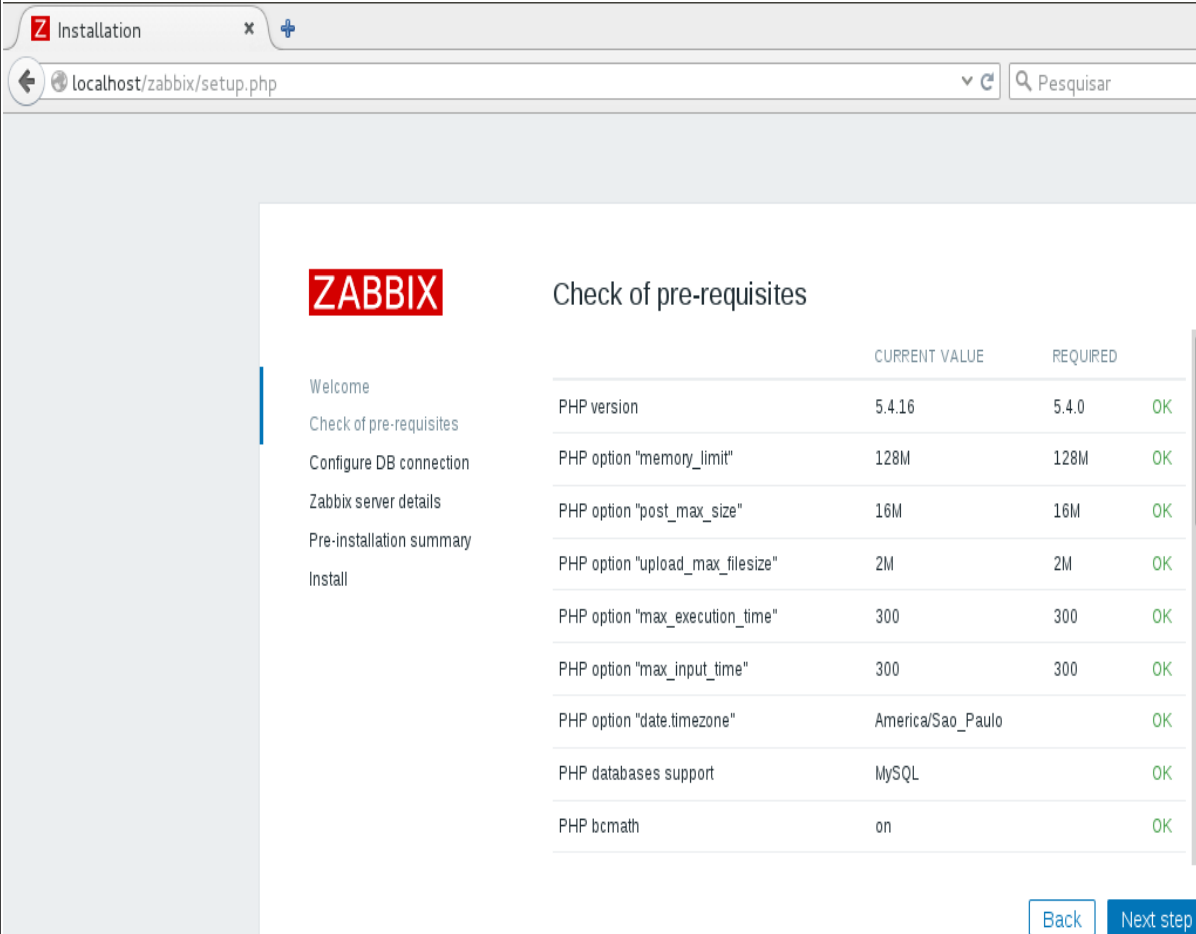
**Figura 10- Tela inicial do instalador da interface web**  
**Fonte: Zabbix, 2016**

Clicando em '*Next step*', o instalador passa para a checagem dos pré-requisitos necessários para a instalação.

Neste ponto, qualquer problema relatado pelo assistente deve ser solucionado antes do prosseguimento do processo de instalação. Os parâmetros de configuração do PHP devem ser alterados para os valores mínimos requeridos para a instalação da interface *web*.

A cada alteração efetuada nos parâmetros do PHP, o serviço 'apache' deve ser reiniciado e após este procedimento, retoma-se o processo de instalação da interface *web*, até que todos os requisitos mínimos tenham sido atingidos.

Na figura 11 pode-se ver a tela de checagem de pré-requisitos, bem como o status de cada item checado.



The screenshot shows the Zabbix installation pre-requisite check page. The page title is "Check of pre-requisites". The Zabbix logo is visible on the left. A navigation menu on the left includes: Welcome, Check of pre-requisites (selected), Configure DB connection, Zabbix server details, Pre-installation summary, and Install. The main content area displays a table with the following data:

	CURRENT VALUE	REQUIRED	
PHP version	5.4.16	5.4.0	OK
PHP option "memory_limit"	128M	128M	OK
PHP option "post_max_size"	16M	16M	OK
PHP option "upload_max_filesize"	2M	2M	OK
PHP option "max_execution_time"	300	300	OK
PHP option "max_input_time"	300	300	OK
PHP option "date.timezone"	America/Sao_Paulo		OK
PHP databases support	MySQL		OK
PHP bcmath	on		OK

At the bottom right of the page, there are two buttons: "Back" and "Next step".

**Figura 11- Tela de checagem de pré-requisitos**  
**Fonte: Zabbix, 2016**

Clicando em 'Next step' passamos para a página de configuração da conexão com o banco de dados. Nesta página inserimos o nome da base de dados, o nome do usuário do banco de dados e a senha de acesso ao banco de dados.

Para que este procedimento seja feito com sucesso, a base de dados já deve ter sido criada, como descrito anteriormente, e o servidor MySQL deve estar ativo.

Na figura 12 verifica-se a tela de configuração da conexão com o banco de dados.



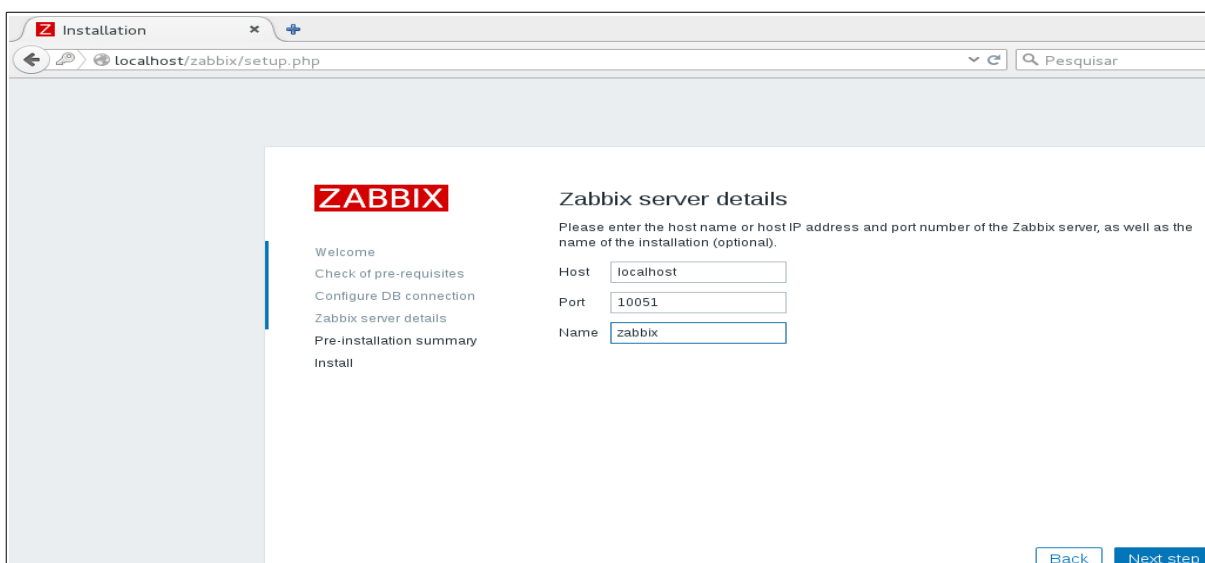
The screenshot shows a web browser window with the URL `localhost/zabbix/setup.php`. The page title is "ZABBIX" and the main heading is "Configure DB connection". Below the heading, there is a message: "Please create database manually, and set the configuration parameters for connection to this database. Press 'Next step' button when done." The form contains the following fields:

- Database type:
- Database host:
- Database port:  (with a note: "0 - use default port")
- Database name:
- User:
- Password:

At the bottom right, there are two buttons: "Back" and "Next step". On the left side, there is a navigation menu with the following items: Welcome, Check of pre-requisites, Configure DB connection (highlighted), Zabbix server details, Pre-installation summary, and Install.

**Figura 12- Configuração da conexão com o banco de dados**  
Fonte: Zabbix, 2016

Clicando em 'Next step' passamos para a página de configuração de detalhes do servidor, como o nome do *host*, porta de funcionamento (padrão 10051) e um nome para a instalação, como podemos ver na figura 13.



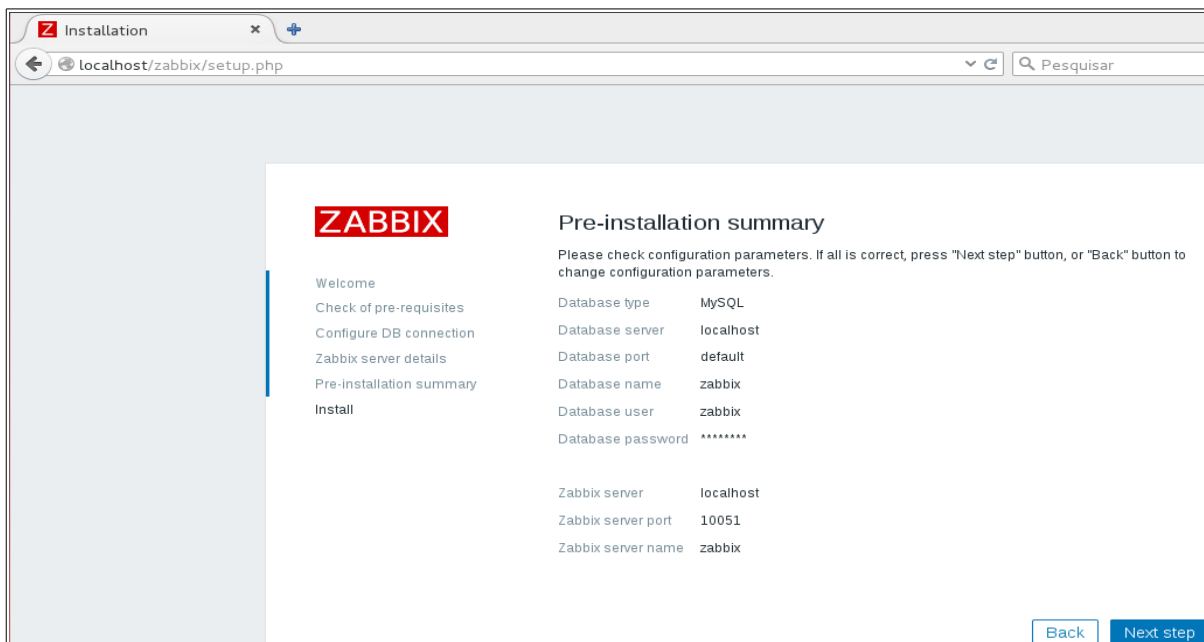
The screenshot shows the same web browser window, but the main heading is now "Zabbix server details". Below the heading, there is a message: "Please enter the host name or host IP address and port number of the Zabbix server, as well as the name of the installation (optional)." The form contains the following fields:

- Host:
- Port:
- Name:

At the bottom right, there are two buttons: "Back" and "Next step". On the left side, the navigation menu is the same as in Figure 12, but "Zabbix server details" is now highlighted.

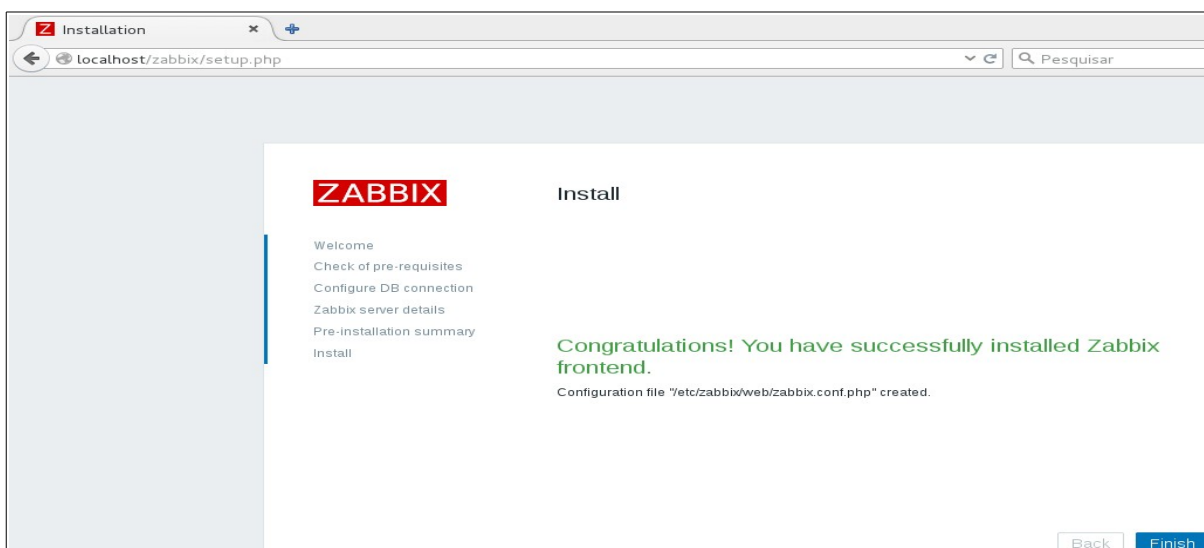
**Figura 13- Detalhes da configuração do servidor**  
Fonte: Zabbix, 2016

Clicando em 'Next step' é apresentado o sumário das configurações de pré-instalação, onde é possível checar os parâmetros, como podemos ver na figura 14.



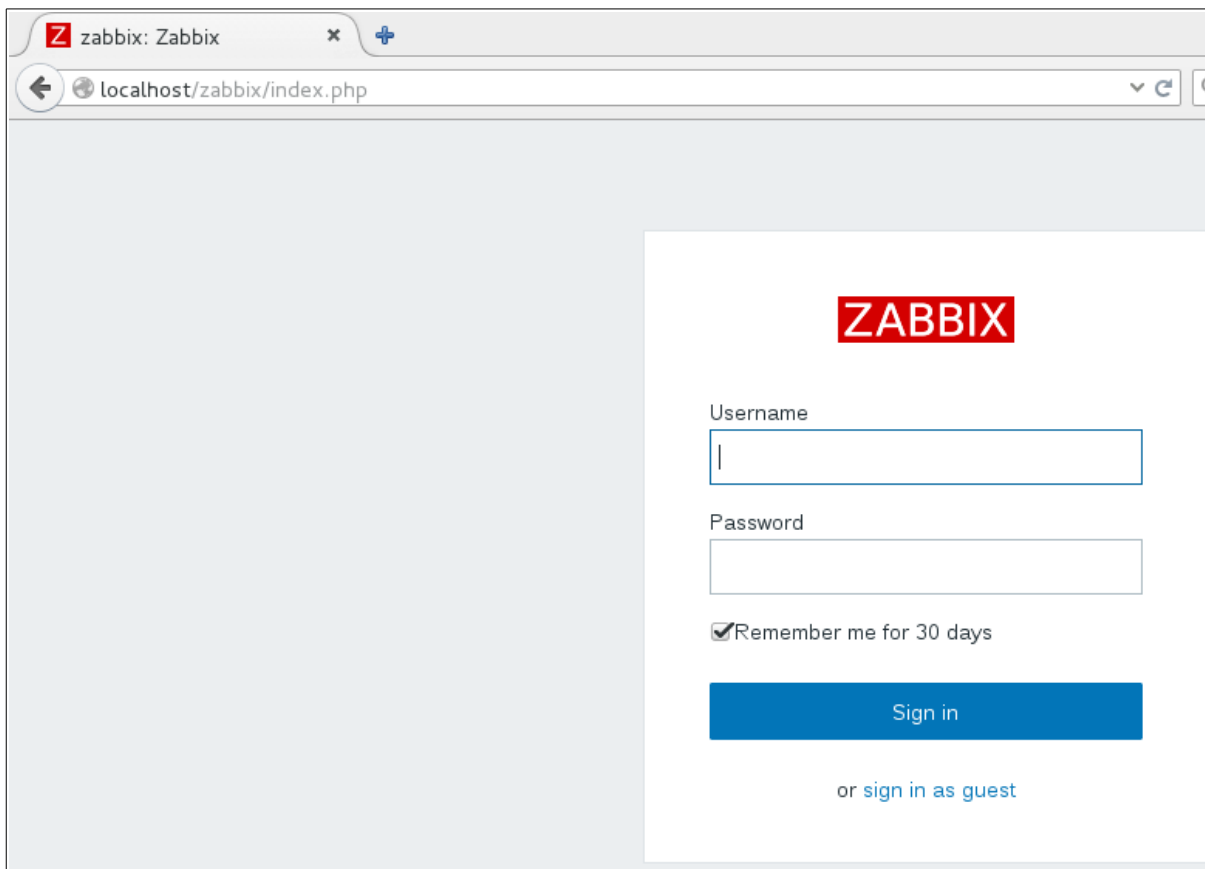
**Figura 14- Sumário para checagem de parâmetros**  
Fonte: Zabbix, 2016

Clicando em 'Next step' é apresentada a página de confirmação do processo de instalação, como podemos ver na figura 15.



**Figura 15- Página de confirmação do processo de instalação**  
Fonte: Zabbix, 2016

Clicando em '*Finish*' é apresentada a tela de login do Zabbix, como verificamos na figura 16.



**Figura 16- Tela de login do Zabbix**  
Fonte: Zabbix, 2016

O usuário inicial para acessar o sistema é **Admin** e a senha inicial é **zabbix** (VLADISHEV, 2016, Cap. 4).

### 3.2 CONFIGURAÇÃO DO ZABBIX

Após o término do processo de instalação do Servidor Zabbix e do Agente Zabbix, o sistema está pronto para iniciar o monitoramento.

Ao fazer login no sistema pela primeira vez, verifica-se que o Servidor Zabbix já inicia pré-configurado para fazer seu próprio monitoramento, de acordo



com informações prestadas no processo de instalação. Já existe um *host* definido com *templates*<sup>3</sup> associados, como podemos verificar na figura 17.



**Figura 17- Host pré-configurado**  
Fonte: Zabbix, 2016

O Zabbix monitora *hosts* com base em *templates* associados a estes *hosts*, sendo assim, para iniciar o processo de monitoramento, inicia-se configurando os *hosts* e posteriormente associando *templates* a estes *hosts*, desta forma o Zabbix poderá ser configurado para monitorar qualquer um dos itens existentes no *template*, de acordo com situações preestabelecidas.

### 3.2.1 Adicionando um novo *host*

Um *host* é qualquer elemento da rede que possua um IP, *Internet Protocol* e que tenha capacidade de comunicação com o Servidor Zabbix, como por exemplo: (servidores, estações de trabalho, *switches*, roteadores, etc) (VLADISHEV, 2016, Cap. 4).

Para adicionar um novo *host* ao Zabbix, estando na interface *web* do Zabbix, realiza-se os seguintes passos (VLADISHEV, 2016, Cap. 4):

- Acesse as abas: Configuração → *Hosts*
- Clique em: 'Criar *host*' no canto superior direito da tela.
- Informar os parâmetros de configuração no formulário

<sup>3</sup> “Um *template* é um conjunto de entidades que pode ser associadas de forma fácil e conveniente a vários *hosts*” (VLADISHEV, 2016, Cap. 6).

Na figura 18 verificamos o formulário de configuração do novo *host*. A aba '*Host*' deste formulário contém os atributos gerais de um *host* (VLADISHEV, 2016, Cap. 4).

The screenshot shows the Zabbix web interface for configuring a new host. The main navigation bar includes 'Grupos de hosts', 'Templates', 'Hosts', 'Manutenção', 'Ações', 'Descoberta', and 'Serviços de TI'. The 'Hosts' section has sub-tabs: 'Host', 'Templates', 'IPMI', 'Macros', 'Inventário do host', and 'Criptografia'. The 'Host' tab is selected.

Fields for configuration include:

- Nome do host:** An empty text input field.
- Nome visível:** An empty text input field.
- Grupos:** A list box currently empty, labeled 'Nos grupos'.
- Outros grupos:** A list box containing 'Discovered hosts', 'Hypervisors', 'Linux servers', 'Templates', 'Virtual machines', and 'Zabbix servers', with left and right arrow navigation buttons.
- Novo grupo:** An empty text input field.
- Interfaces do agente:** A table with columns: ENDEREÇO IP, NOME DNS, CONNECTADO A PORTA, and PADRÃO. The first row contains '127.0.0.1', an empty field, 'IP', 'DNS', and '10050'. A 'Remove' button is next to the last cell. Below the table is an 'Adicionar' button.
- Interfaces SNMP:** An 'Adicionar' button.
- Interfaces JMX:** An 'Adicionar' button.
- Interfaces IPMI:** An 'Adicionar' button.
- Descrição:** A large empty text area.
- Monitorado por proxy:** A dropdown menu set to '(sem proxy)'.
- Ativo:** A checked checkbox.
- Buttons:** 'Adicionar' and 'Cancelar' buttons at the bottom.

**Figura 18- Formulário de configuração de *host***  
**Fonte: Zabbix, 2016**

Ao configurar um novo *host*, basicamente configuramos o nome do *host*, nome visível, selecionamos um grupo ou criamos um novo, selecionamos por quais interfaces o *host* será monitorado, informamos se o *host* é ou não monitorado por *proxy* e finalizamos clicando em adicionar.

Todo *host* que for utilizar a 'interface do agente' para o monitoramento, deve ter o Agente Zabbix instalado e configurado, conforme descrito no item 3.1.3.3 Instalação do Agente Zabbix.

A figura 19 mostra o formulário de configuração de *host* preenchido com os dados necessários ao monitoramento de um servidor de nome 'apache', que será monitorado pela 'interface agente' e tem como IP o endereço 10.35.91.7.

The screenshot displays the Zabbix web interface for configuring a host. The top navigation bar includes 'ZABBIX' and menu items: 'Monitoramento', 'Inventário', 'Relatórios', 'Configuração', and 'Administração'. Below this is a secondary navigation bar with 'Grupos de hosts', 'Templates', 'Hosts', 'Manutenção', 'Ações', 'Descoberta', and 'Serviços de TI'. The main header shows 'Hosts' and a breadcrumb 'Todos os hosts / Apache'. A status bar indicates 'Ativo', 'ZBX', 'SNMP', 'JMX', 'IPMI', and various statistics like 'Aplicações 11', 'Itens 47', 'Triggers 20', 'Gráficos 9', 'Regras de descoberta 2', and 'Cenários web'. The configuration form includes fields for 'Nome do host' (apache), 'Nome visível' (Apache), and 'Grupos' (Linux servers). A table for 'Interfaces do agente' shows the IP '10.35.91.7', 'CONECTADO A PORTA' 'IP DNS', and 'PADRÃO' '10050'. Other sections include 'Interfaces SNMP', 'Interfaces JMX', 'Interfaces IPMI', 'Descrição' (Monitoramento do serviço apache2), 'Monitorado por proxy' (sem proxy), and an 'Ativo' checkbox. Action buttons at the bottom are 'Atualizar', 'Clonar', 'Clone completo', 'Excluir', and 'Cancelar'.

Figura 19- Formulário de configuração de *host* preenchido  
Fonte: Zabbix, 2016

O *host* em questão é um Servidor *Web Apache* e neste caso, monitoraremos o serviço 'apache2', que é o responsável pelo provimento de páginas *web* na rede local.

### 3.2.2 Adicionando *templates* ao *host*

Prosseguindo com a configuração do novo *host*, agora que já definimos o que queremos monitorar neste servidor, passamos à etapa seguinte que é a seleção dos *templates* a serem utilizados.

Neste caso, como trata-se de um servidor linux que possui o serviço *apache* instalado, selecionaremos dois *templates*, o “*Template App HTTP Service*” e o “*Template OS Linux*”.

Para selecionar os *templates*, basta clicar em 'Selecionar', escolher os *templates* na lista apresentada e em seguida clicar em 'Adicionar', como mostra a figura 20 (VLADISHEV, 2016, Cap. 4).

The screenshot shows the Zabbix web interface. At the top, there is a navigation bar with the ZABBIX logo and menu items: Monitoramento, Inventário, Relatórios, Configuração, and Administração. Below this is a sub-menu with: Grupos de hosts, Templates, Hosts (selected), Manutenção, Ações, Descoberta, and Serviços de TI. The main content area is titled 'Hosts' and shows the configuration for a host named 'Apache'. It includes a table of associated templates and a section for adding new templates.

Associado aos templates	NOME	AÇÃO
	Template App HTTP Service	<a href="#">Desassociar</a> <a href="#">Desassociar e limpar</a>
	Template OS Linux	<a href="#">Desassociar</a> <a href="#">Desassociar e limpar</a>

Vincular a novos templates

informe aqui o argumento para pesquisa

[Adicionar](#)

Figura 20- Formulário para adição de *templates* ao *host*

Fonte: Zabbix, 2016

Após adicionar os *templates*, basta clicar em 'Atualizar' para que o Zabbix passe monitorar o *host*, verificando todos os itens constantes dos *templates* que sejam suportados.

Existem várias outras opções de configuração disponíveis para personalização do *host* que não serão abordadas por não serem essenciais para a obtenção dos resultados propostos neste trabalho.

### 3.2.3 Personalizando itens do *template*

Os *templates* podem ser modificados de acordo com a necessidade do administrador (VLADISHEV, 2016, Cap. 4). Para o *host* configurado como descrito no item 3.2.1, por tratar-se de um servidor *web*, necessita-se de um menor tempo entre a falha e a comunicação ao administrador.

O '*Template App HTTP*' que foi atribuído ao *host*, tem configurado um intervalo entre verificações de 60 segundos. Com o objetivo de diminuir o tempo de indisponibilidade do servidor *web*, alterou-se esse valor para 15 segundos, conforme verifica-se na figura 21.

The screenshot shows the Zabbix web interface for configuring an item. The breadcrumb path is: Todos os templates / Template App HTTP Service / Aplicações 1 / Itens 1. The configuration fields are as follows:

- Nome: HTTP service is running
- Tipo: Agente Zabbix
- Chave: net.tcp.service[http] (with a 'Selecionar' button)
- Tipo de informação: Numérico (inteiro sem sinal)
- Tipo de dados: Decimal
- Unidades: (empty)
- Usar multiplicador customizado:  1
- Intervalo atualização (em seg): 15
- Intervalo customizado table:

TIPO	INTERVALO	PERÍODO	AÇÃO
Flexível	Agendamento	50	1-7,00:00-24:00

At the bottom of the table, there is a 'Remover' link and an 'Adicionar' button.

**Figura 21- Personalização do template**  
**Fonte: Zabbix, 2016**

### 3.2.4 Habilitando comandos remotos

Após a criação de um novo *host* e sua respectiva configuração com a adição de *templates*, o Zabbix passa a monitorá-lo e fornecer informações acerca da situação dos serviços monitorados, porém nenhum serviço será reestabelecido, ainda, sem a ação do administrador.

Para que seja possível a atuação direta do Zabbix na solução de falhas reportadas pelo monitoramento, é necessário habilitar o Agente Zabbix para que execute comandos remotos no *host* monitorado, assim que determinada condição “preestabelecida” for atingida (VLADISHEV, 2016, Cap. 6).

Para que comandos remotos possam ser executados pelo Agente Zabbix o mesmo deverá ter seu arquivo de configuração devidamente configurado para permitir isso (VLADISHEV, 2016, apêndice 3).

Deve-se certificar de que o parâmetro **EnableRemoteCommands** está definido como **1** e sua linha não está comentada. O Agente deve ser reiniciado após a modificação (VLADISHEV, 2016, apêndice 3).

Para possibilitar o acompanhamento da execução dos comandos remotos, deve-se habilitar o parâmetro **LogRemoteComands**, verificando se a linha não está comentada e se está definida como **1** (VLADISHEV, 2016, apêndice 3).

#### 3.2.4.1 Habilitando o comando 'sudo' para o usuário 'zabbix'

Para que os comandos remotos possam ser executados pelo Servidor Zabbix nos clientes que possuem o Agente Zabbix instalado, é necessário que o usuário 'zabbix' do sistema onde o comando será executado, possua permissão para executar tais comandos localmente (VLADISHEV, 2016, Cap. 6).

Tomando por base o *host* já configurado, que monitora o Servidor *Web Apache*, deve-se adicionar a seguinte linha de configuração ao arquivo '/etc/sudoers', conforme seja o caso (VLADISHEV, 2016, Cap. 6):

- Para autorizar o usuário 'zabbix' a reiniciar o serviço 'apache2' sem senha

```
zabbix ALL=(ALL) NOPASSWD: /etc/init.d/apache2 restart
```

- Para autorizar o usuário 'zabbix' a executar qualquer comando sem senha

```
zabbix ALL=(ALL) NOPASSWD: ALL
```

### 3.2.5 Criando nova ação

A configuração da ação no Zabbix, é a etapa onde configura-se os comandos remotos a serem executados nos *hosts* monitorados ao serem obedecidas as condições estabelecidas (VLADISHEV, 2016, Cap. 6).

Para criar uma nova ação, clica-se em Configuração-->Ações-->Criar Ação, a partir desse ponto tem-se acesso ao formulário de configuração da nova ação, conforme mostra a figura 22.

The screenshot displays the Zabbix web interface for configuring a new action. The top navigation bar includes 'ZABBIX' and 'Configuração'. The main menu shows 'Ações' selected. The 'Ações' page has three tabs: 'Ação', 'Condições', and 'Operações'. The 'Ação' tab is active, showing the following configuration fields:

- Nome:**
- Assunto padrão:**
- Mensagem padrão:**
- Mensagem da recuperação:**
- Ativo:**

At the bottom of the form, there are four buttons: 'Atualizar', 'Clonar', 'Excluir', and 'Cancelar'.

Figura 22- Formulário de configuração da ação

Fonte: Zabbix, 2016

Ao preencher os campos, pode-se fazer uso das macros internas do Zabbix, que retornam valores das variáveis do sistema, que no exemplo da figura 22 são os códigos escritos entre '{ }'.

Após configurar os valores conforme a figura de exemplo, clica-se em 'Condições', para obter acesso ao próximo formulário que é mostrado na figura 23.



**ZABBIX** Monitoramento Inventário Relatórios Configuração Administração

Grupos de hosts Templates Hosts Manutenção **Ações** Descoberta Serviços de TI

**Ações**

Ação Condições Operações

Tipo do cálculo: E/OU A and B and C and D

TEXTO	NOME	AÇÃO
A	Status de manutenção não em <i>manutenção</i>	<a href="#">Remover</a>
B	Valor da trigger = <i>INCIDENTE</i>	<a href="#">Remover</a>
C	Severidade da trigger = <i>Alta</i>	<a href="#">Remover</a>
D	Trigger = <i>Apache: HTTP service is down on Apache</i>	<a href="#">Remover</a>

Nova condição: Trigger = informe aqui o argumento para pesquisa

[Adicionar](#)

**Atualizar** **Clonar** **Excluir** **Cancelar**

**Figura 23- Condições para execução da ação**  
**Fonte: Zabbix, 2016**

No formulário 'Condições' são estabelecidas as condições que serão testadas para permitir a execução da ação.

As opções constantes na figura 23 são suficientes para que a ação seja executada em caso de falha no serviço 'apache2' (VLADISHEV, 2016, Cap. 6).

Após configurar os valores conforme a figura de exemplo, clica-se em 'Operações', para obter acesso ao próximo formulário.

Na figura 24 observa-se o formulário de especificação dos parâmetros do comando remoto que será executado no cliente.

Pontos a serem observados:

- Tipo da operação = Comando remoto
- Lista de destinos = *Host:Apache (host remoto)*
- Tipo = *Script personalizado*



- Executar em = Agente Zabbix
- Comandos = sudo /etc/init.d/apache2 restart

The screenshot shows the 'Operações' (Operations) tab in the Zabbix configuration interface. At the top, there are three tabs: 'Ação', 'Condições', and 'Operações'. Below the tabs, the 'Duração padrão do passo da operação' (Default step duration) is set to 60 seconds. The 'Operações da ação' (Action operations) section shows a table with one operation: '1 Executar comandos remotos nos hosts: Apache Imediatamente 60'. The 'Detalhes da operação' (Operation details) section includes fields for 'Passos' (Steps) set to 1, 'Duração do passo' (Step duration) set to 60, and 'Tipo da operação' (Operation type) set to 'Comando remoto'. Below this, there is a table for 'Lista de destinos' (Destination list) with one entry: 'Host: Apache' and an 'AÇÃO' (Action) column with a 'Remover' link. The 'Tipo' (Type) is set to 'Script personalizado' (Custom script). The 'Executar em' (Execute on) field is set to 'Agente Zabbix'. The 'Comandos' (Commands) field contains the command 'sudo /etc/init.d/apache2 restart'. At the bottom, there are buttons for 'Atualizar', 'Clonar', 'Excluir', and 'Cancelar'.

**Figura 24- Formulário de configuração das operações**  
**Fonte: Zabbix, 2016**

Após serem inseridos os parâmetros, conforme exemplo, clica-se em 'Atualizar', finalizando dessa forma a configuração da ação.

## 4. RESULTADOS

Neste capítulo serão detalhados os resultados obtidos durante o monitoramento do ambiente de testes proposto.

Os testes realizados têm por finalidade comprovar a capacidade do Zabbix de, a partir de um problema detectado em um *host* monitorado, executar um procedimento, remotamente, com a finalidade de reestabelecer o serviço interrompido .

### 4.1 RESULTADOS OBTIDOS NO PROCESSO DE INSTALAÇÃO

#### 4.1.1 Instalação do Servidor Zabbix

A instalação do Servidor Zabbix, versão 3.0, se deu seguindo os passos detalhados no item 3.1 deste documento.

Usou-se como SO base para a instalação a distribuição Linux CentOS-7-x86\_64, sendo constatado que não houve quaisquer problemas de compatibilidade entre a versão Zabbix instalada e o SO no qual foi instalado.

A instalação se deu através dos pacotes de *software* oficiais disponíveis no repositório do desenvolvedor, de tal forma que todas as dependências para o seu funcionamento foram sanadas de forma automática durante o processo de instalação.

Desta forma, chegou-se a conclusão de que a instalação e a configuração inicial do Servidor Zabbix, de acordo com os procedimentos aqui documentados, ocorreu sem que fosse necessário recorrer a ajustes não previstos pelo desenvolvedor.

#### 4.1.2 Instalação do Agente Zabbix

A instalação do Agente Zabbix se deu seguindo os passos detalhados no item 3.1.3.3 deste documento.

A instalação se deu através dos pacotes disponíveis nos repositórios oficiais de cada distribuição testada. Análogo à instalação do Servidor Zabbix, as dependências foram sanadas de forma automática durante o procedimento de instalação.

Foi observado que, dependendo da funcionalidade a ser monitorada, bem como do *template* utilizado na configuração do *host*, podem ser necessários configurações adicionais no arquivo de configuração do Agente Zabbix.

No ambiente testado, para o monitoramento da base de dados Mysql, foi necessário realizar ajustes nos parâmetros de usuário do arquivo de configuração do Agente Zabbix (VLADISHEV, 2016, apêndice 9).

Com exceção do Agente Zabbix instalado no Servidor Mysql, todos os demais agentes não necessitaram de configurações extras, além daquelas descritas no procedimento de instalação inicial.

#### 4.2 RESULTADOS OBTIDOS NA REALIZAÇÃO DOS TESTES

O quadro 1 apresenta o resumo do ambiente proposto para monitoramento e dos itens específicos a serem monitorados em cada servidor.

Nome do Servidor	Agente Instalado	Item Monitorado	Comando Remoto
ZABBIX	Sim	Serviço 'apache2'	Sim
DNS	Sim	Serviço 'named'	Sim
DHCP	Sim	Serviço 'dhcp3'	Sim
SAMBA	Sim	Serviço 'smb'	Sim
APACHE	Sim	Serviço 'mysql'	Sim

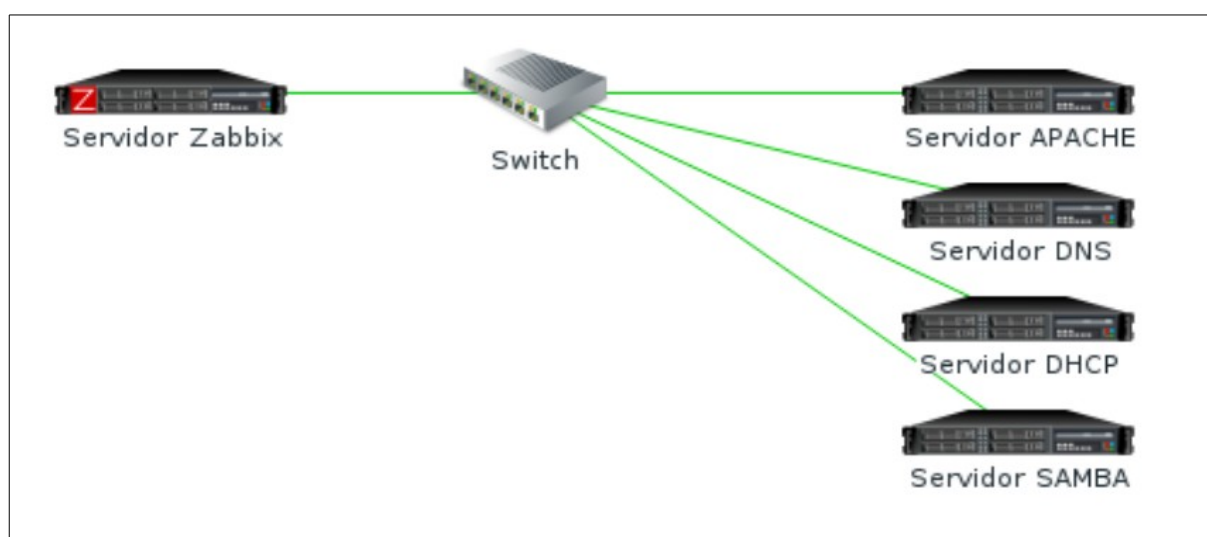
**Quadro 1: Resumo dos itens monitorados**  
**Fonte: Autoria própria**

O quadro 2 mostra detalhes dos SO e dos serviços que foram monitorados, bem como o endereço de rede de cada servidor.

Nome do Servidor	Versão SO	Versão Serviço	Endereço IP
ZABBIX	CentOS 7 64bit	APACHE 2.4.7	10.35.91.249
APACHE	Ubuntu 14.04.4 LTS 64bit	MYSQL 14.14	10.35.91.7
DNS	CentOS 7 64bit	BIND 9.9.4	10.35.91.2
DHCP	CentOS 7 64bit	DHCP Server 4.2.5	10.35.91.3
SAMBA	CentOS 6 64bit	SMBD 3.6.23-20.el6	10.35.88.11

**Quadro 2: Resumo dos SO e dos serviços monitorados**  
**Fonte: Autoria própria**

A figura 25 mostra a topologia utilizada no ambiente testado.



**Figura 25- Topologia utilizada no ambiente testado**  
**Fonte: Zabbix, 2016**

Todos os servidores alvos de monitoramento tiveram os Agentes Zabbix instalados a partir de pacotes, como já foi abordado neste documento.

Todos os Agentes Zabbix foram configurados para permitir a execução de comandos remotos, bem como foram executadas as alterações necessárias nos SO para permitir a execução de comandos pelo usuário 'zabbix' sem o uso de senha.

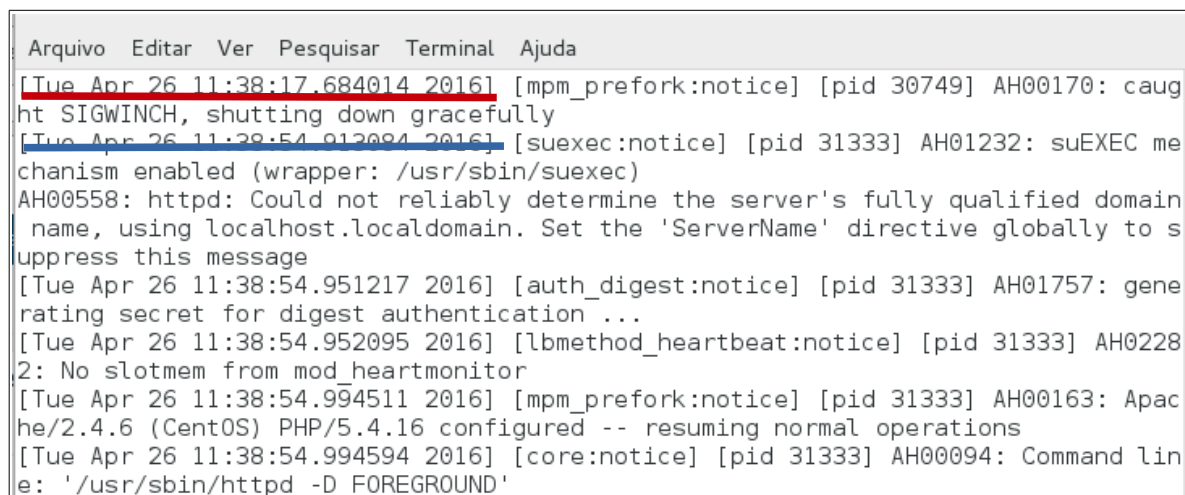
Todos os *hosts* foram criados e configurados no Servidor Zabbix para a execução de **ação remota** conforme visto neste trabalho.

O teste foi executado induzindo uma falha ao serviço monitorado, realizando o acompanhamento dos *logs* das aplicações envolvidas para comprovar a atuação do Servidor Zabbix no reestabelecimento do serviço que apresentou falha.

#### 4.2.1 Realização de testes

##### 4.2.1.1 Teste no Servidor Zabbix

O Servidor Zabbix foi testado quando ao reestabelecimento do Servidor Apache. A partir do terminal o serviço 'httpd' foi parado, induzindo a falha. A hora exata da queda do serviço e posterior reestabelecimento, podem ser verificadas na figura 26.



```
Arquivo Editar Ver Pesquisar Terminal Ajuda
[Tue Apr 26 11:38:17.684014 2016] [mpm_prefork:notice] [pid 30749] AH00170: caught SIGWINCH, shutting down gracefully
[Tue Apr 26 11:38:54.912094 2016] [suexec:notice] [pid 31333] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using localhost.localdomain. Set the 'ServerName' directive globally to suppress this message
[Tue Apr 26 11:38:54.951217 2016] [auth_digest:notice] [pid 31333] AH01757: generating secret for digest authentication ...
[Tue Apr 26 11:38:54.952095 2016] [lbmethod_heartbeat:notice] [pid 31333] AH02282: No slotmem from mod_heartbeat
[Tue Apr 26 11:38:54.994511 2016] [mpm_prefork:notice] [pid 31333] AH00163: Apache/2.4.6 (CentOS) PHP/5.4.16 configured -- resuming normal operations
[Tue Apr 26 11:38:54.994594 2016] [core:notice] [pid 31333] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
```

**Figura 26- Log do serviço 'httpd' no Servidor Zabbix**  
**Fonte: Zabbix, 2016**

Acompanhou-se também o *log* de atividades do Agente Zabbix, onde pode-se confirmar a hora da execução do comando remoto para o reestabelecimento do serviço interrompido. O comando foi enviado pelo Servidor Zabbix após a constatação de que o serviço monitorado havia parado.

Na figura 27 é possível verificar a atividade do Agente Zabbix no Servidor Apache.

```
Arquivo Editar Ver Pesquisar Terminal Ajuda
30930:20160426:113811.607 agent #3 started [listener #2]
30931:20160426:113811.620 agent #4 started [listener #3]
30932:20160426:113811.622 agent #5 started [active checks #1]
30928:20160426:113811.625 agent #1 started [collector]
30931:20160426:113854.785 Executing command 'sudo service httpd restart'
```

**Figura 27- Log do Agente Zabbix no Servidor Zabbix**  
Fonte: Zabbix, 2016

#### 4.2.1.2 Teste no Servidor Apache

O Servidor Apache foi testado quando ao reestabelecimento do Servidor Mysql. Esta abordagem foi realizada uma vez que o teste anterior já comprovou o monitoramento proativo do serviço 'apache2' e por não ser possível desativar o banco de dados no Servidor Zabbix sem que o monitoramento deixasse de funcionar.

A partir do terminal o serviço 'mysql' foi parado, induzindo a falha. A hora exata da queda do serviço e posterior reestabelecimento, podem ser verificadas na figura 28.

```
160427 0:18:34 [Note] Event Scheduler: Purging the queue. 0 events
160427 0:18:34 InnoDB: Starting shutdown...
160427 0:18:36 InnoDB: Shutdown completed; log sequence number 1955719
160427 0:18:36 [Note] /usr/sbin/mysqld: Shutdown complete

160427 0:18:38 [Warning] Using unique option prefix myisam-recover instead of myisam-recover-options is deprecated and will be removed in a future release. Please use the full name instead.
160427 0:18:38 [Note] Plugin 'FEDERATED' is disabled.
160427 0:18:38 InnoDB: The InnoDB memory heap is disabled
160427 0:18:38 InnoDB: Mutexes and rw_locks use GCC atomic builtins
160427 0:18:38 InnoDB: Compressed tables use zlib 1.2.8
160427 0:18:38 InnoDB: Using Linux native AIO
160427 0:18:38 InnoDB: Initializing buffer pool, size = 128.0M
160427 0:18:39 InnoDB: Completed initialization of buffer pool
160427 0:18:39 InnoDB: highest supported file format is Barracuda.
160427 0:18:39 InnoDB: Waiting for the background threads to start
160427 0:18:40 InnoDB: 5.5.49 started; log sequence number 1955719
160427 0:18:40 [Note] Server hostname (bind-address): '127.0.0.1'; port: 3306
160427 0:18:40 [Note] - '127.0.0.1' resolves to '127.0.0.1';
160427 0:18:40 [Note] Server socket created on IP: '127.0.0.1'.
160427 0:18:40 [Note] Event Scheduler: Loaded 0 events
160427 0:18:40 [Note] /usr/sbin/mysqld: ready for connections.
Version: 5.5.49-0ubuntu0.14.04.1 socket: /var/run/mysqld/mysqld.sock port: 3306 (Ubuntu)
```

**Figura 28- Log do serviço 'mysql' no Servidor Apache**  
Fonte: Zabbix, 2016

Acompanhou-se também o *log* de atividades do Agente Zabbix, como é possível verificar na figura 29, onde pode-se confirmar a hora da execução do comando remoto para o reestabelecimento do serviço interrompido.

```
mysqladmin: connect to server at 'localhost' failed
error: 'Can't connect to local MySQL server through socket '/var/run/mysqld/mysqld.sock' (2)'
Check that mysqld is running and that the socket: '/var/run/mysqld/mysqld.sock' exists!
2155:20160427:001838.950 Executing command 'sudo service mysql start'
```

**Figura 29- Log do Agente Zabbix no Servidor Apache**  
Fonte: Zabbix, 2016

#### 4.2.1.3 Teste no Servidor DNS

O Servidor DNS foi testado quando ao reestabelecimento do Servidor Bind9. A partir do terminal o serviço 'named' foi parado, induzindo a falha. A hora exata da queda do serviço e posterior reestabelecimento, podem ser verificadas na figura 30.

```
Apr 27 15:43:55 dns1 named[11306]: received control channel command 'stop'
Apr 27 15:43:55 dns1 named[11306]: shutting down: flushing changes
Apr 27 15:43:55 dns1 named[11306]: stopping statistics channel on 127.0.0.1#8053
Apr 27 15:43:55 dns1 named[11306]: stopping command channel on 127.0.0.1#953
Apr 27 15:43:55 dns1 named[11306]: no longer listening on 127.0.0.1#53
Apr 27 15:43:55 dns1 named[11306]: no longer listening on 10.35.88.2#53
Apr 27 15:43:55 dns1 named[11306]: exiting

Apr 27 15:44:02 dns1 named[12156]: zone localhost/IN: loaded serial 0
Apr 27 15:44:02 dns1 named[12156]: all zones loaded
Apr 27 15:44:02 dns1 named[12156]: running
```

**Figura 30- Log do serviço 'named' no Servidor DNS**  
Fonte: Zabbix, 2016

Acompanhou-se também o *log* de atividades do Agente Zabbix, onde pode-se confirmar a hora da execução do comando remoto para o reestabelecimento do serviço interrompido. O comando foi enviado pelo Servidor Zabbix após a constatação de que o serviço monitorado havia parado.

Na figura 31 é possível verificar a atividade do Agente Zabbix no Servidor DNS.

```
11886:20160427:154342.182 agent #0 started [main process]
11889:20160427:154342.206 agent #2 started [listener #1]
11890:20160427:154342.206 agent #3 started [listener #2]
11891:20160427:154342.206 agent #4 started [listener #3]
11892:20160427:154342.206 agent #5 started [active checks #1]
11888:20160427:154342.206 agent #1 started [collector]
11889:20160427:154402.767 Executing command 'sudo systemctl restart named.service'
```

**Figura 31- Log do Agente Zabbix no Servidor DNS**  
Fonte: Zabbix, 2016

#### 4.2.1.4 Teste no Servidor DHCP

O Servidor DHCP foi testado quando ao reestabelecimento do serviço 'dhcpd'. A hora exata da queda do serviço pode ser verificada na figura 32.

```
[root@dhcp sgtalexandro]# systemctl status dhcpd.service
● dhcpd.service - DHCPv4 Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/dhcpd.service; enabled; vendor preset: disabled)
   Active: inactive (dead) since Sex 2016-04-29 09:44:42 BRT; 1s ago
     Docs: man:dhcpd(8)
           man:dhcpd.conf(5)
   Process: 6148 ExecStart=/usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -group dhcpd --no-pid (code=killed, signal=TERM)
   Main PID: 6148 (code=killed, signal=TERM)
   Status: "Dispatching packets..."

Abr 29 09:44:23 dhcp dhcpd[6148]: DHCPREQUEST for 10.35.91.66 from 00:24:2b...he
Abr 29 09:44:23 dhcp dhcpd[6148]: DHCPACK on 10.35.91.66 to 00:24:2b:9c:d0:...he
Abr 29 09:44:24 dhcp dhcpd[6148]: DHCPREQUEST for 10.35.90.112 from 00:e0:4...he
Abr 29 09:44:24 dhcp dhcpd[6148]: DHCPACK on 10.35.90.112 to 00:e0:4c:68:07...he
Abr 29 09:44:24 dhcp dhcpd[6148]: DHCPREQUEST for 10.35.90.86 from 5c:c9:d3...he
Abr 29 09:44:24 dhcp dhcpd[6148]: DHCPACK on 10.35.90.86 to 5c:c9:d3:04:d7:...he
Abr 29 09:44:41 dhcp dhcpd[6148]: DHCPREQUEST for 10.35.91.66 from 00:24:2b...he
Abr 29 09:44:41 dhcp dhcpd[6148]: DHCPACK on 10.35.91.66 to 00:24:2b:9c:d0:...he
Abr 29 09:44:42 dhcp systemd[1]: Stopping DHCPv4 Server Daemon...
Abr 29 09:44:42 dhcp systemd[1]: Stopped DHCPv4 Server Daemon.
```

**Figura 32- Status do serviço 'dhcpd' no Servidor DHCP**  
Fonte: Zabbix, 2016

Acompanhou-se também o *log* de atividades do Agente Zabbix, onde pode-se confirmar a hora da execução do comando remoto para o reestabelecimento do serviço interrompido.



Na figura 33 é possível verificar a atividade do Agente Zabbix no Servidor DHCP.

```
6366:20160429:094254.217 agent #0 started [main process]
6369:20160429:094254.220 agent #3 started [listener #2]
6370:20160429:094254.220 agent #4 started [listener #3]
6367:20160429:094254.220 agent #1 started [collector]
6371:20160429:094254.221 agent #5 started [active checks #1]
6368:20160429:094254.221 agent #2 started [listener #1]
6370:20160429:094512.623 Executing command 'sudo systemctl restart dhcpd.servic
e'
```

Figura 33- Log do Agente Zabbix no Servidor DHCP

Fonte: Zabbix, 2016

A hora exata do reestabelecimento do serviço pode ser verificada abaixo, na figura 34.

```
● dhcpd.service - DHCPv4 Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/dhcpd.service; enabled; vendor preset
: disabled)
   Active: active (running) since Sex 2016-04-29 09:45:13 BRT; 2s ago
     Docs: man:dhcpd(8)
           man:dhcpd.conf(5)
  Main PID: 6533 (dhcpd)
    Status: "Dispatching packets..."
   CGroup: /system.slice/dhcpd.service
           └─6533 /usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -gr...

Abr 29 09:45:13 dhcp dhcpd[6533]: to which interface eth1 is attached. **
Abr 29 09:45:13 dhcp dhcpd[6533]:
Abr 29 09:45:13 dhcp dhcpd[6533]: Listening on LPF/eth0/06:eb:59:ee:57:3c/1...22
Abr 29 09:45:13 dhcp dhcpd[6533]: Sending on LPF/eth0/06:eb:59:ee:57:3c/1...22
Abr 29 09:45:13 dhcp dhcpd[6533]: Sending on Socket/fallback/fallback-net
Abr 29 09:45:13 dhcp systemd[1]: Started DHCPv4 Server Daemon.
```

Figura 34- Status do serviço 'dhcpd' (reestabelecido)

Fonte: Zabbix, 2016

#### 4.2.1.5 Teste no Servidor Samba

O Servidor SAMBA foi testado quando ao reestabelecimento do serviço 'smb'. A partir do terminal o serviço 'smb' foi parado, induzindo a falha. O comando foi enviado pelo Servidor Zabbix após a constatação de que o serviço monitorado havia parado.

Na figura 35 é possível verificar a atividade do Agente Zabbix no Servidor SAMBA.

```
[2016/04/29 11:55:13.299759, 3] smbd/server_exit.c:181(exit_server_common)
  Server exit (termination signal)
[2016/04/29 11:55:13.529463, 3] smbd/server_exit.c:181(exit_server_common)
[2016/04/29 11:55:13.529461, 3] smbd/server_exit.c:181(exit_server_common)
  Server exit (termination signal)
  Server exit (termination signal)
[2016/04/29 11:55:13.529605, 3] smbd/server_exit.c:181(exit_server_common)
  Server exit (termination signal)
[2016/04/29 11:55:13.529889, 3] smbd/server_exit.c:181(exit_server_common)
  Server exit (termination signal)
```

**Figura 35- Log do serviço 'smb' no Servidor SAMBA**  
Fonte: Zabbix, 2016

Acompanhou-se também o *log* de atividades do Agente Zabbix, como é possível verificar na figura 36, onde pode-se confirmar a hora da execução do comando remoto para o reestabelecimento do serviço interrompido.

```
38471:20160429:115505.393 agent #0 started [main process]
38473:20160429:115505.393 agent #1 started [collector]
38474:20160429:115505.393 agent #2 started [listener #1]
38475:20160429:115505.393 agent #3 started [listener #2]
38476:20160429:115505.393 agent #4 started [listener #3]
38477:20160429:115505.393 agent #5 started [active checks #1]
38475:20160429:115538.962 Executing command 'sudo /etc/init.d/smb restart'
```

**Figura 36- Log do Agente Zabbix no Servidor SAMBA**  
Fonte: Zabbix, 2016

A hora em que o sistema voltou a responder pelas requisições aos compartilhamentos pode ser verificada na figura 37.

```
Linux kernel oplocks enabled
[2016/04/29 11:55:40.566698, 3] smbd/process.c:1609(process_smb)
  Transaction 0 of length 72 (0 toread)
[2016/04/29 11:55:40.566718, 2] smbd/reply.c:553(reply_special)
  netbios connect: name1=*SMBSERVER 0x20 name2=XENSERVER-2 0x0
[2016/04/29 11:55:40.566739, 2] smbd/reply.c:573(reply_special)
  netbios connect: local=10.35.88.17 remote=xenserver-2, name type = 0
```

**Figura 37- Status do serviço 'smb' (reestabelecido)**  
Fonte: Zabbix, 2016

A Interface *Web* do Servidor Zabbix proporciona o acompanhamento visual dos incidentes ocorridos no ambiente monitorado, como mostra a figura 38.

#### 4.2.2 Alertas gerados pela Interface *Web* do Servidor Zabbix

A situação apresentada na figura 38 descreve o momento em que dois serviços apresentam falhas, respectivamente o serviço 'smbd' do Servidor Samba e o serviço 'mysql' do Servidor Apache.

Ressalta-se que as ações de reestabelecimento dos serviços foram temporariamente desativadas, para possibilitar a visualização desta tela.

Verificou-se que os alertas são customizáveis e podem ou não disparar uma ação de retorno ao *host* com problemas.

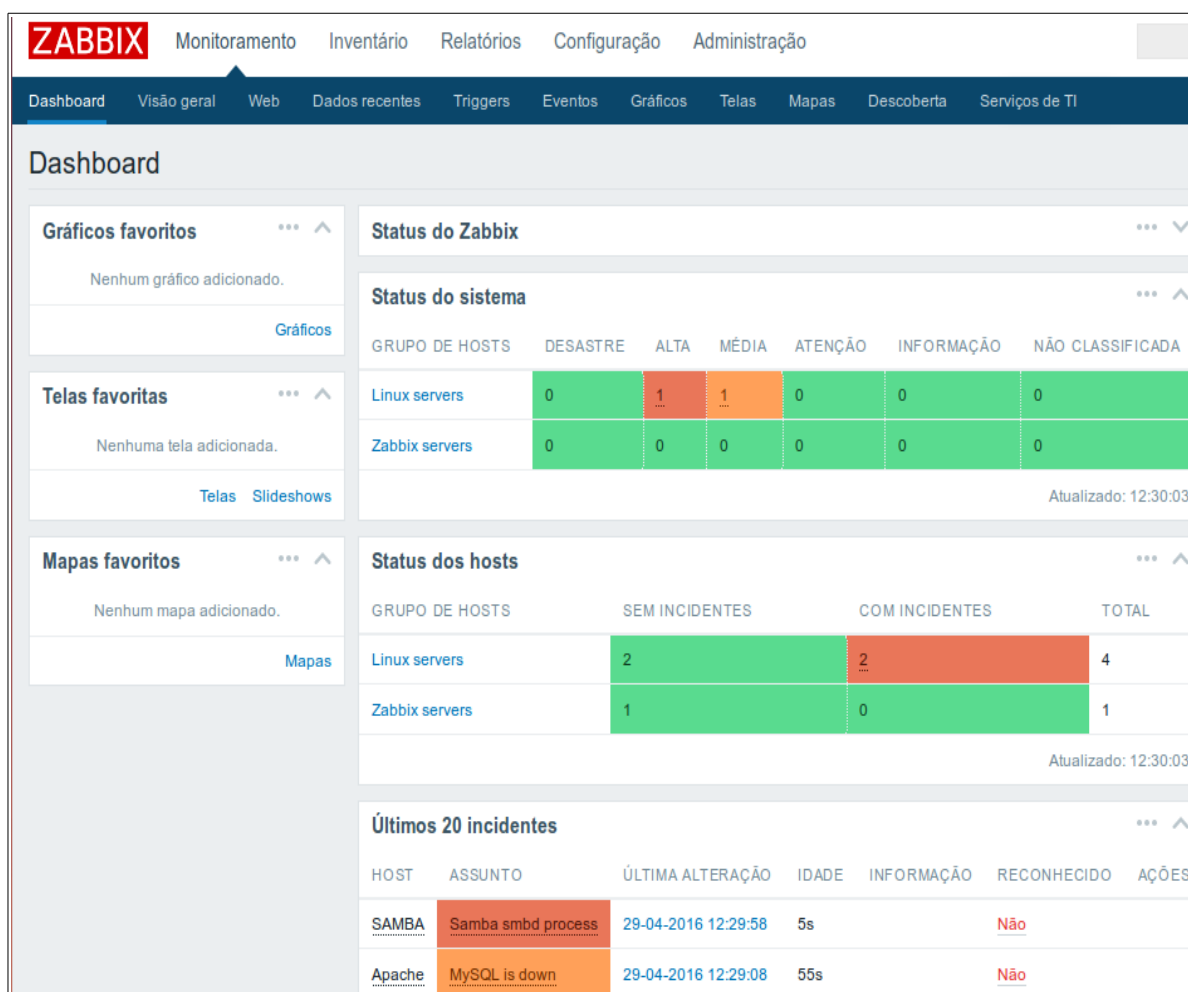


Figura 38- *Dashboard* de monitoração  
Fonte: Zabbix, 2016

### 4.2.3 Tela de configuração de *hosts* e ações

Na figura 39 pode-se observar a tela de configuração de *hosts*, com o resumo dos *hosts* configurados e testados, com seus respectivos *templates* utilizados para o monitoramento.

The screenshot shows the Zabbix web interface. At the top, there is a navigation bar with the ZABBIX logo and menu items: Monitoramento, Inventário, Relatórios, Configuração, and Administração. Below this is a sub-menu for 'Hosts' with options: Grupos de hosts, Templates, Hosts, Manutenção, Ações, Descoberta, and Serviços de TI. The main heading is 'Hosts' with a dropdown menu for 'Grupo' set to 'todos'. There are search filters for 'Nome como', 'DNS como', 'IP similar', and 'Porta como', along with 'Filtrar' and 'Limpar' buttons. Below the filters is a table of hosts.

<input type="checkbox"/>	NOME ▲	APLICAÇÕES	ITENS	TRIGGERS	GRÁFICOS	DESCOBERTA	WEB	INTERFACE	TEMPLATES	STATUS	DISPONIBILIDADE	CRIPTOGRAFIA
<input type="checkbox"/>	Apache	Aplicações 1	Itens 14	Triggers 2	Gráficos 2	Descoberta	Web	10.35.91.7: 10050	Template App MySQL	Ativo	ZBX SNMP JMX IPMI	NENHUM
<input type="checkbox"/>	Dhcp	Aplicações 1	Itens 1	Triggers 1	Gráficos	Descoberta	Web	10.35.88.3: 10050	MyTemplate_DHCP	Ativo	ZBX SNMP JMX IPMI	NENHUM
<input type="checkbox"/>	Dns1	Aplicações 2	Itens 163	Triggers 8	Gráficos 11	Descoberta 1	Web	10.35.88.2: 10050	Template App DNS-bind Service, Template_App_named	Ativo	ZBX SNMP JMX IPMI	NENHUM
<input type="checkbox"/>	SAMBA	Aplicações 11	Itens 61	Triggers 24	Gráficos 14	Descoberta 2	Web	10.35.88.11: 10050	ServiceTemplateSamba, Template OS Linux (Template App Zabbix Agent)	Ativo	ZBX SNMP JMX IPMI	NENHUM
<input type="checkbox"/>	Zabbix server	Aplicações 14	Itens 97	Triggers 51	Gráficos 17	Descoberta 2	Web	127.0.0.1: 10050	Template App HTTP Service, Template App Zabbix Server, Template OS Linux (Template App Zabbix Agent)	Ativo	ZBX SNMP JMX IPMI	NENHUM

**Figura 39- Hosts configurados para o monitoramento**  
Fonte: Zabbix, 2016

Na figura 40 verifica-se a tela de configuração de ações, que é a tela onde configura-se qual será a ação a ser realizada de acordo com critérios estabelecidos.

Nesta tela configurou-se as ações para reestabelecimento dos serviços monitorados que apresentassem falha.

ZABBIX		
Monitoramento	Inventário	Relatórios
Configuração	Administração	
Grupos de hosts	Templates	Hosts
Manutenção	Ações	Descoberta
Serviços de TI		
Ações		Origem do
<input type="checkbox"/> NOME ▲	CONDIÇÕES	OPERAÇÕES
<input type="checkbox"/> Report problems to Zabbix administrators	Status de manutenção não em <i>manutenção</i> Valor da trigger = <i>INCIDENTE</i>	Enviar mensagem para o grupo de usuários: Zabbix mídias
<input type="checkbox"/> Reset dhcp	Status de manutenção não em <i>manutenção</i> Valor da trigger = <i>INCIDENTE</i> Severidade da trigger = <i>Alta</i> Trigger = <i>MyTemplate_DHCP: Dhcpcd is not running on MyTemplate_DHCP</i>	Executar comandos remotos nos hosts: Dhcpcd
<input type="checkbox"/> {HOSTNAME} Restart Apache Zabbix Server	Status de manutenção não em <i>manutenção</i> Valor da trigger = <i>INCIDENTE</i> Severidade da trigger = <i>Alta</i> Trigger = <i>Zabbix server: HTTP service is down on Zabbix server</i>	Executar comandos remotos no host atual
<input type="checkbox"/> {HOSTNAME} Restart Dns	Status de manutenção não em <i>manutenção</i> Valor da trigger = <i>INCIDENTE</i> Severidade da trigger = <i>Alta</i> Trigger = <i>Template_App_named: named is not running on Template_App_named</i>	Executar comandos remotos nos hosts: Dns1
<input type="checkbox"/> {HOSTNAME} Restart Mysql	Status de manutenção não em <i>manutenção</i> Valor da trigger = <i>INCIDENTE</i> Severidade da trigger = <i>Média</i> Trigger = <i>Apache: MySQL is down</i>	Executar comandos remotos nos hosts: Apache
<input type="checkbox"/> {HOSTNAME} Restart Samba	Status de manutenção não em <i>manutenção</i> Valor da trigger = <i>INCIDENTE</i> Severidade da trigger = <i>Alta</i> Trigger = <i>SAMBA: Samba smbd process</i>	Executar comandos remotos nos hosts: SAMBA

**Figura 40- Lista de ações configuradas**  
Fonte: Zabbix, 2016

## 5. CONCLUSÃO

Com base nos resultados obtidos após a realização dos procedimentos de instalação do Servidor Zabbix e do Agente Zabbix, conclui-se que a aplicação é de fácil instalação e que o simples monitoramento de um servidor ou outro ativo de rede é possível a partir dos *templates* disponíveis após a instalação inicial.

Com base nos testes realizados no ambiente de monitoramento proposto, ficou evidenciado que é possível utilizar o Servidor Zabbix no monitoramento proativo dos serviços de rede, podendo, desta forma, diminuir consideravelmente o tempo que um serviço fica indisponível para o usuário final.

Não há necessidade de alocar pessoal da área de TI para monitorar visualmente os mapas da infraestrutura de rede, uma vez que o Zabbix é capaz de enviar alertas por diversas formas, podendo o gerente utilizar-se dos mapas de monitoramento apenas para melhor situar-se a respeito do problema apresentado.

O uso do Agente Zabbix nos *hosts* monitorados, mostrou-se versátil, adaptável e de simples configuração, uma vez que após instalado, para a maioria dos serviços a serem monitorados, não há necessidade de nenhuma nova configuração do lado do cliente. Os ajustes para atender aos novos serviços a serem monitorados passam a ser feitos somente no Servidor Zabbix.

### 5.1 DIFICULDADES ENCONTRADAS

Foi observado que os *templates* que acompanham a distribuição e que estão disponíveis após a instalação inicial são suficientes para o monitoramento da maioria dos dispositivos e SO existentes, porém, excetuando-se aqueles casos atendidos pelos *templates* que acompanham a instalação, não existe um repositório oficial de *templates* para *download*, sendo necessário, em casos específicos, recorrer ao auxílio externo, em comunidades e fóruns.

## 5.2 TRABALHOS FUTUROS

Para um melhor aproveitamento do potencial de monitoramento que ficou evidenciado após a comprovação dos resultados, ficou evidente a necessidade de aprofundar os estudos relativos ao desenvolvimento de *templates* personalizados, que possibilitem capturar eventos específicos no dispositivo monitorado, possibilitando a execução de testes mais aprimorados e conseqüentemente a realização de ações específicas para cada caso.

## REFERÊNCIAS

COMER, Douglas E. **Computer Networks and Internets**. 5 ed. New Jersey: Pearson, 2008.

FRYE, Rob; LEVI, David B.; ROUTHIER, Shawn A.; WIJNEN Bert, **Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework**, BCP 74, RFC 3584, DOI 10.17487/RFC3584, 2003. Disponível em: <<http://www.rfc-editor.org/info/rfc3584>>. Acesso em: 15 abr. 2016, 14:00.

ITU, **International Telecommunication Union**, 2000. Disponível em: <<https://www.itu.int/rec/T-REC-M.3400-200002-I/en>>. Acesso em: 16 abr. 2016, 15:00.

KUROSE, James F.; ROSS, Keith W., **Redes de Computadores e a Internet - Uma Nova Abordagem**. 5 ed. São Paulo: Addison Wesley, 2010.

LOPES, Raquel V.; SAUVÉ, Jacques P.; NICOLLETTI, Pedro S., **Melhores Práticas para Gerência de Redes de Computadores**. 1 ed. Rio de Janeiro: Campus, 2003.

MAURO, Douglas. R. & SCHMIDT, Kevin J. **Essential SNMP**. Sebastopol: O' Reilly, 2001.

ROSE, Marshall T.; McCLOGHRIE, Keith. **How to Manage Your Network using SNMP: The Network Management Practicum**. New Jersey: Prentice Hall, 1995.

STALLINGS, William, **SNMP, SNMPv2, SNMPv3 and RMON 1 and 2**. 3 ed. Boston: Addison-Wesley, 1998.

VLADISHEV , Alexei, **Manual Zabbix**, Vs 3.0, 2016. Disponível em: <<https://www.zabbix.com/documentation/3.0/pt/manual>>. Acesso em: 15 abr. 2016, 18:00.



ZABBIX BRASIL, **Comunidade Brasileira de Usuários do Zabbix**, 2016.  
Disponível em: <[http://www.zabbixbrasil.org/wiki/tiki-index.php?  
page=Implementando+Zabbix+Proxy](http://www.zabbixbrasil.org/wiki/tiki-index.php?page=Implementando+Zabbix+Proxy)>. Acesso em: 15 abr. 2016, 09:00.

ZABBIX, **Zabbix LLC**, 2016. Disponível em:  
<<http://www.zabbix.com/screenshots.php>>. Acesso em: 15 abr. 2016, 20:00.