UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS QUIXADÁ

TECNÓLOGO EM REDES DE COMPUTADORES

ANTÔNIO SEBASTIÃO LOPES NOGUEIRA

COMPARANDO O TRÁFEGO GERADO PELAS FERRAMENTAS DE MONITORAÇÃO NAGIOS E ZABBIX EM UM AMBIENTE DE REDE REAL

QUIXADÁ
2016

ANTÔNIO SEBASTIÃO LOPES NOGUEIRA

COMPARANDO O TRÁFEGO GERADO PELAS FERRAMENTAS DE MONITORAÇÃO NAGIOS E ZABBIX EM UM AMBIENTE DE REDE REAL

Trabalho de Conclusão de Curso submetido à Coordenação do Curso de Graduação em Redes de Computadores da Universidade Federal do Ceará como requisito parcial para obtenção do grau de Tecnólogo.

Área de concentração: computação

Orientador Prof. Me. Antonio Rafael Braga

QUIXADÁ
2016

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca do Campus de Quixadá

N71c Nogueira, Antônio Sebastião Lopes
Comparando o tráfego gerado pelas ferramentas de monitoração Nagios e Zabbix em um ambiente de rede real / Antônio Sebastião Lopes Nogueira. – 2016.
59 f. : il. color., enc. ; 30 cm.

Monografia (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Tecnologia em Redes de Computadores, Quixadá, 2016.
Orientação: Prof. Msc. Antônio Rafael Braga
Área de concentração: Computação

1. Redes de computadores - Gerência 2. Windows Server (Sistema operacional de computador) 3. Redes de computadores - Tráfego I. Título.

CDD 004.6

ANTÔNIO SEBASTIÃO LOPES NOGUEIRA

COMPARANDO O TRÁFEGO GERADO PELAS FERRAMENTAS DE MONITORAÇÃO NAGIOS E ZABBIX EM UM AMBIENTE DE REDE REAL

Trabalho de Conclusão de Curso submetido à Coordenação do Curso de Graduação em Redes de Computadores da Universidade Federal do Ceará como requisito parcial para obtenção do grau de Tecnólogo.

Área de concentração: computação

Aprovado em: 04 / Fevereiro / 2016.

BANCA EXAMINADORA

_____
Prof. Me. Antônio Rafael Braga (Orientador)
Universidade Federal do Ceará-UFC

_____
Prof. Me. Marcos Dantas de Oliveira
Universidade Federal do Ceará-UFC

_____
Prof. Me. Michel Sales Bonfim
Universidade Federal do Ceará-UFC

Dedico esse trabalho aos meus pais, esposa, filhos, amigos e professores pelo incentivo e apoio, os quais deram sua contribuição para a realização deste trabalho.

AGRADECIMENTOS

Agradeço primeiramente a Deus, criador do universo, pelo dom da vida e a oportunidade que me colocou diante de um mundo cheio de grande descobertas.

Aos meus pais pelo cuidado e dedicação incondicional prestado a mim. Aos meus irmãos, pelo laço de amizade, apoio e reconhecimento de meus esforços.

A minha esposa, meu braço direito, pelo apoio concedido durante os momentos ausentes, abrindo mão de estarmos juntos, na dedicação aos estudos e apoio nas minhas decisões. Aos meus filhos, os quais são razão e motivo da maior parte dessa luta. E aos amigos pelo apoio e colaboração nos momentos difíceis.

Aos professores, pela contribuição nas etapas do conhecimento durante toda jornada e ao meu orientador em especial, por trilhar os caminhos na conclusão deste trabalho.

“O gerenciamento de um sistema consiste em supervisionar e controlar seu funcionamento para que ele satisfaça aos requisitos tanto dos seus usuários quanto dos seus proprietários.”

(Morris Sloman)

RESUMO

Este trabalho apresenta a importância da gerência de redes, através das ferramentas de gerenciamento Nagios e Zabbix, a qual fornece dados do estado da rede. O objetivo é comparar o tráfego gerado pelas duas ferramentas no processo de gerenciamento da rede composta por máquinas *Windows,* levando em consideração a quantidade de tráfego gerado. As ferramentas foram instaladas em ambiente virtual. Por ser uma rede particular, foi preservada sua identidade e algumas máquinas não foram monitoradas por questão de sigilo e segurança. Ao final, através da análise gráfica, a ferramenta Zabbix apresentou melhor desempenho em função da geração do tráfego no processo de gerenciamento de rede.

Palavras chave: Monitoramento, Nagios, Zabbix, Rede Windows, Tráfego de rede.

ABSTRACT

This work shows the importance of the the network management, through the management tools Nagios and Zabbix, which provides network status data. The objective is to compare the traffic generated by the two tools in the network management process comprises Windows machines, taking into consideration the amount of traffic generated. The tools have been installed in a virtual environment. For being a private network, was preserved its identity and some machines were not monitored for reasons of confidentiality and security. In the end, through the graphical analysis, the tool Zabbix showed performed better due to the traffic generation in the network management process.

Keywords: Monitoring, Nagios, Zabbix, Windows Network, network traffic.

LISTA DE ABREVIATURAS E SIGLAS

CGI	***Common Gateway Interface***
CPU	***Central Processing Unit***
DHCP	***Dynamic Host Configuration Protocol***
DNS	***Domain Name System***
FTP	***File Transfer Protocol***
GPL	**General Public License**
HD	***Disk e Hardware***
HTML	***Hiper Text Markup Language***
HTTP	***Hypertext Transfer Protocol***
IP	***Internet Protocol***
IPMI	***Intelligent Platform Management Interface***
MIB	***Management Information Base***
NNTP	***Network News Transfer Protocol***
NRPE	***Nagios Remote Plugins Executor***
NSCA	***Nagios Service Check Acceptor***
NSClient++	***Agente Remoto do Nagios para plataforma Windows***
PING	***Packet Internet Network Group***
POP3	***Post Office Protocol***
SMS	***Short Message Serviçe***
SMTP	***Simple Mail Transfer Protocol***
SNMP	***Simple Network Management Protocol***
TCP	***Transmission Control Protocol***
TI	***Tecnologia da Informação***
UNIX	***Sistema Operacional Multitarefa***
UTP	***User Datagram Protocol***
UTP5e	**Cabo par trançado UTP categoria 5e.**
VM	***Virtual Machine***
VPN	***Virtual Private Network***
WAP	***Wireless Application Protocolo***

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Atualmente, o computador vem cada vez mais tornando-se uma ferramenta indispensável para o trabalho, envolvendo armazenamento de dados, seja ele no disco rígido (*HD*) para uso pessoal no ambiente empresarial ou em bancos de dados em computadores específicos para esse fim, disponibilizando dados e compartilhando-os através das redes de computadores.

Esses serviços necessitam de uma verificação, cabendo tanto o gerenciamento dos computadores como dos serviços disponibilizados, principalmente quando esses serviços fazem parte de um ambiente de rede. Ao encontro disso, Neto e Uchôa (2015) afirmaram que é extremamente necessário ter uma fonte de dados disponível para consulta imediata no caso de quedas, congestionamento, mau funcionamento ou qualquer anormalidade que afete servidores ou redes de computadores.

Para garantir a funcionalidade dessas redes, os profissionais de informática utilizam sistemas de gerenciamento que facilitam o trabalho de monitoração. Santos (2011) destaca que qualquer empresa que tenha uma rede de computadores, independentemente do tamanho irá encontrar dificuldades em manter estabilizada, sendo necessário gerenciá-la para prover os serviços desejados aos seus usuários.

Atualmente, há diversas ferramentas de gerenciamento de *software* livre e proprietários empregados no monitoramento das redes. No entanto, cada ferramenta possui características próprias empregadas no monitoramento. Black (2008) realizou uma pesquisa com várias ferramentas comparando as funcionalidade e características individuais. Nesse caso, as ferramentas com melhor desempenho foram o Nagios e o Zabbix a nível de arquitetura, embora não tenha realizado análise de tráfego. Em virtude disso, este trabalho realizará um comparativo entre essas duas ferramentas quanto ao tráfego gerado no monitoramento da rede, tendo em vista que este tráfego poderá sobrecarregar a rede dependendo do fluxo de dado existente.

No processo de monitoramento, as ferramentas geram carga de tráfego na rede entre as máquinas gerenciadas (agentes) e o servidor (gerente). Este tráfego é uma variável que deve ser controlada para prover serviços compatíveis com o desempenho esperado da rede. Diante desta necessidade, o tráfego será avaliado, em especial a quantidade de pacote gerado por cada ferramenta.

O tráfego será medido com o auxílio do capturador de pacotes *Wireshark*, a partir do gerenciamento das máquinas pelas duas ferramentas simultaneamente, configuradas com os mesmos critérios estabelecidos para coincidir com a quantidade de tráfego de cada uma.

Este trabalho tem como objetivo medir e comparar o tráfego das ferramentas no monitoramento da rede composta por máquinas, através de uma análise estatística, caracterizada pela média, desvio padrão e intervalo de confiança da totalidade do tráfego gerado, coletado pela ferramenta de análise de tr *Wireshark*. Essa análise apresentará qual ferramenta gerará a maior quantidade de tráfego na coleta de dados dos estados das máquinas e dos serviços monitorados.

2 TRABALHOS RELACIONADOS

Este estudo teve como base o trabalho de Black (2008), que realizou um comparativo com oito ferramentas de monitoração, avaliando a arquitetura de cada uma delas. A abrangência do trabalho de Black (2008) focou nas características mais relevantes das ferramentas. Dentre elas: Performance, facilidade de utilização e necessidade de recursos de *hardware* e humanos.

Rossete e Bezelli (2013) apresentaram funcionalidades, funcionamento e configuração, além de apresentar funcionalidades adicionais a fim de contribuir e servir de material de apoio para profissionais que desejarem utilizar a ferramenta de monitoramento Nagios. (Franca et. al, 2013) utilizaram o Zabbix para avaliar o tráfego e construir gráficos da ocupação de banda *multicast* nas redes monitoradas.

Neto e Uchôa (2015) realizaram um estudo comparativo das ferramentas assim como Black (2008) e ambos os trabalhos observa-se uma ênfase maior dos estudos realizados em questões relacionadas à arquitetura das ferramentas. Este trabalho tem como proposito acrescentar a análise do tráfego gerado pelas ferramentas em estudo mais voltado para a quantidade média do tráfego gerado no processo de monitoração da rede.

Com isso, será determinado a quantidade média, o desvio padrão e o intervalo de confiança do tráfego na rede monitorada, o que causa uma alteração no fluxo de dado da rede.

3 FUNDAMENTAÇÃO TEÓRICA

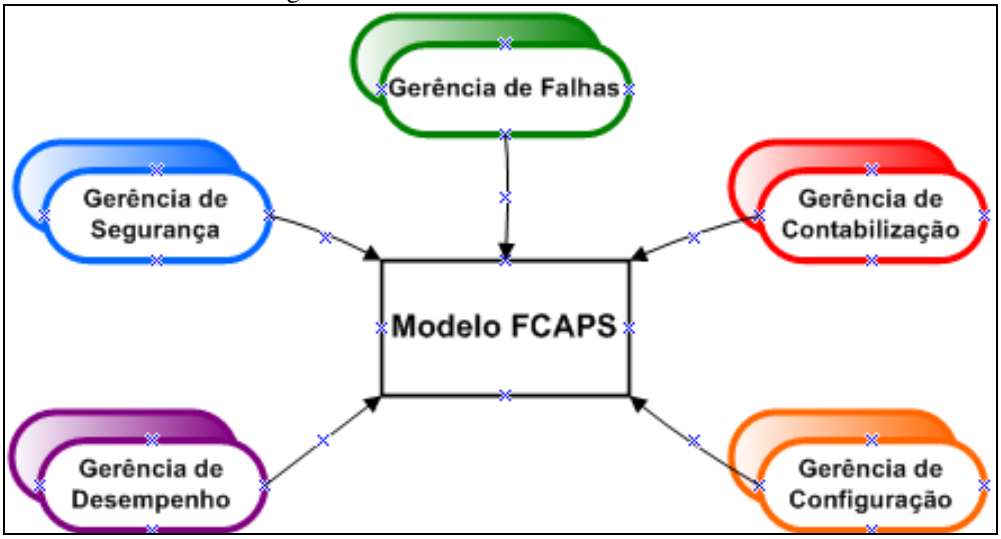
Neste estudo foi abordado conceito sobre o gerenciamento de redes, as ferramentas Nagios e Zabbix para o monitoramento da rede, a ferramenta de captura de pacote *Wireshark* e os conceitos de análise de tráfego envolvendo média, desvio padrão e intervalo de confiança.

3.1 Gerenciamento de Redes

É comum no setor de TI, a equipe técnica levar horas para descobrir onde um problema ocorreu para que possa solucioná-lo e entregar de volta todas as funcionalidades aos seus usuários. Apesar de todo empenho da equipe em atender as expectativas dos usuários, não é uma postura adequada procurar saber do usuário através dos meios de comunicação como está à disponibilidade dos serviços; se a máquina está funcionando adequadamente, como está o desempenho da máquina, pedir para o usuário verificar o espaço disponível em disco, como está à memória. Esses procedimentos não fazem parte de uma postura adequada para o administrador de uma rede gerenciável.

No processo de gerenciamento o principal protocolo é o SNMP. Segundo Santos (2010), é o protocolo que atende as exigências operacionais de desempenho e de qualidade de serviços em tempo real e a baixo custo. Conforme Santos (2010), no protocolo SNMP foram definidos cinco áreas de gerenciamento do modelo FCAPS de acordo com afigura abaixo.

Figura 1 - Áreas do Gerenciamento de redes



Adaptado: Santos (2010)

a) Gerencia de Falhas: É o tratamento imediato de falhas transitórias da rede, causadas por uma interrupção do serviço em enlaces, hospedeiros, ou em hardware e software de roteadores.

b) Gerência de Contabilização: Corresponde à especificação, registro e controle do acesso de usuários e dispositivos aos recursos da rede. Também fazem parte deste gerenciamento: quotas de utilização, cobrança por utilização e alocação de acesso privilegiado a recursos.

c) Gerência de Segurança: Trata do controle do acesso aos recursos da rede de acordo com a política definida. Através dela, os elementos são protegidos, monitorando-se e detectando-se possíveis violações, da política de segurança estabelecida, podendo, o administrador de rede ser alertado através de alarmes. Mantém logs de segurança tanto para a posterior análise e geração de relatórios como para detectar violações não óbvias manualmente.

d) Gerência de Configuração: É a área responsável pela descoberta, manutenção e monitoração de mudanças à estrutura física e lógica da rede. As funções básicas desta área de gerência são: coleta de informações sobre a configuração, geração de eventos, atribuição de valores iniciais aos parâmetros dos elementos gerenciados, registro de informações, alteração de configuração dos elementos gerenciados, início e encerramento de operação dos elementos gerenciados.

e) Gerência de Desempenho: A única forma de desenvolver ações proativas é construindo uma base de dados do comportamento da infraestrutura, buscando identificar os critérios de estabilidade do ambiente monitorado, garantindo que a rede opere em conformidade e com a qualidade proposta pelo administrador.

Ao referir-nos a gerenciamento, Santos (2011) afirma que os gerentes de rede devem possuir uma vasta quantidade de informação sobre as redes manuseadas e os problemas desta pelo crescimento do número e da heterogeneidade dos equipamentos envolvidos, o número de problemas potenciais e a complexidade envolvida. Dessa forma, o gerenciamento de redes é necessário para auxiliar os gerentes a trabalhar com a complexidade dos dados envolvidos, de modo a garantir a máxima eficiência e transparência da rede para os seus usuários. Neste aspecto, é necessário o entendimento de gerenciamento.

Kurose e Ross (2010) definem que gerenciamento é um conjunto de ações e procedimentos necessários para manter uma rede sempre funcionando, de preferência a contento.

> O gerenciamento de uma rede inclui o oferecimento, a integração e a coordenação de elementos de hardware, software e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar recursos da rede, além de elementos para satisfazer às exigências operacionais de desempenho e de qualidade de serviço, em tempo real a um custo razoável. (Kurose e Ross, 2010, p. 556).

Vale notar a contribuição de Santos (2010), em seu trabalho na descrição de gerenciamento como fornecedor de ferramentas capazes de monitorar equipamentos, analisando os dados de modo a garantir o funcionamento e operação dentro dos limites especificados; controlar reativamente o sistema fazendo ajustes de acordo com as modificações ocorridas no sistema ou em seu ambiente e gerenciar pró-ativamente o sistema, detectando tendências ou comportamentos anômalos que permitam executar uma ação antes que surjam problemas mais sérios. Neste contexto, qualquer rede deve ser bem gerenciada para ser capaz de prover suas funcionalidades adequadamente e atender os requisitos de seus usuários.

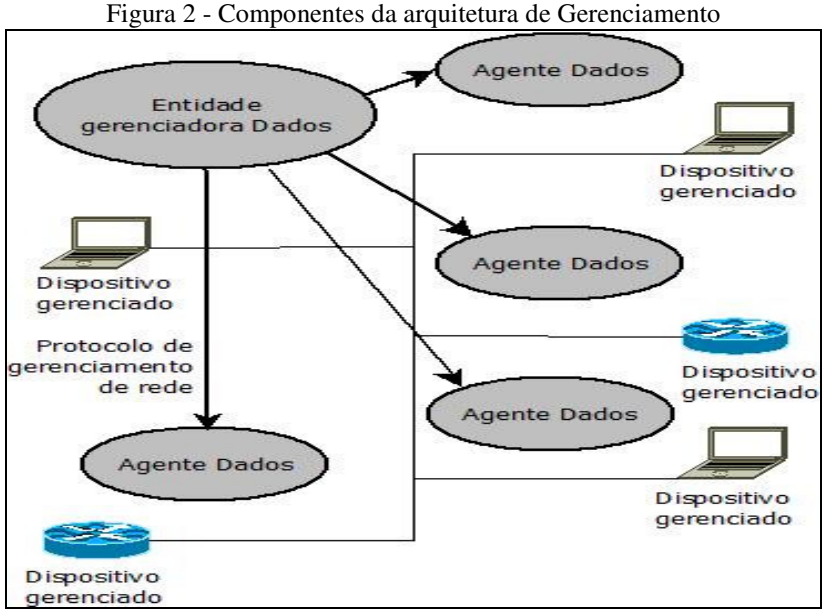
Ainda em Kurose e Ross (2010), o sistema de gerenciamento de rede é composto por três componentes principais na arquitetura de gerenciamento: A entidade gerencial, uma aplicação que em geral tem um ser humano no circuito, que controla a coleta, o processamento, a análise e apresentação das informações do gerenciamento, controlando o comportamento da rede e é aqui que o administrador interage com os dispositivos.

O segundo componente é o agente de gerenciamento, contido nos dispositivos gerenciados. Os dispositivos podem ser *bridges*, roteadores, *switches*, impressoras podendo conter os agentes SNMP controlados pela estação de gerenciamento. No interior destes dispositivos pode haver diversos agentes gerenciados. Os objetos gerenciados têm informações associados que são coletados dentro de uma base de informação de gerenciamento (MIB).

O terceiro componente da arquitetura de gerenciamento é o protocolo SNMP. Ele é executado entre a entidade gerenciadora e o agente de gerenciamento, que permite a entidade gerenciadora investigar o estado dos dispositivos gerenciados, executando ações sobre eles mediante seus agentes. O protocolo obtém informações através dos agentes espalhados em redes TCP/IP e usa o protocolo UDP para enviar mensagens através da rede,

onde os gerentes enviam requisições a seus agentes para obtenção dos dados (Becker e Moura, 2012). A figura abaixo representa os componentes do sistema de gerenciamento.

Figura 2 - Componentes da arquitetura de Gerenciamento



Adaptado: Becker e Moura (2012)

De acordo com Black (2008), o agente de gerenciamento responde a estação de gerenciamento através da solicitação de dados ao agente e por sua vez o agente responde com os dados solicitados. No entanto, a solicitação e resposta destas mensagens podem sobrecarregar o tráfego na rede, através dos dados enviados e recebidos na estação de gerenciamento. Para prevenir essa sobrecarga, evitando que a estação de gerenciamento envie requisições aos agentes a intervalos determinados e contínuos, são definidos limites no dispositivo de gerenciamento e ao ultrapassar esses limites (inferior e superior), é enviada uma mensagem de alerta a estação de gerenciamento. Com isso, elimina a necessidade de enviar requisições aos agentes, reduzindo a quantidade de tráfego SNMP na rede para fornecer mais largura de banda para a transferência de dados.

3.2 Ferramentas de Gerenciamento de Redes

Conforme Santos (2010), a maioria das ferramentas disponíveis para monitoramento de rede é baseada no modelo cliente-servidor. Neste caso, há uma máquina com aplicação servidora e as outras máquinas com seus serviços ou dispositivos de rede sendo monitorados. Para evitar conflitos, os sistemas de gerência evitam termos “cliente” e “servidor”. Em vez disso, usam “Gerente” para a aplicação servidora e “Agente” para a aplicação cliente que corre no dispositivo de rede.

Existem no mercado várias ferramentas de monitoramento, eis aqui algumas delas: Cacti, Nagios, ZenOSS, OpManager, BigBrother4, Spiceworks, Look@LAN e Zabbix, tanto de licença livre como proprietários, auxiliando o administrador na detecção de falhas ou desempenho da rede.

Neste trabalho, foi dada ênfase às ferramentas totalmente gratuitas. Essa foi a principal característica da escolha, seguida da apresentação gráfica para melhor comparação dos dados monitorados e da interface para melhor interação do administrador da rede com a ferramenta.

Este aspecto foi abordado em Black (2008), que avaliou oito ferramentas de monitoramento, incluindo as de licença GPL e comercial. E na avaliação das ferramentas gratuitas, o Zabbix tornou-se superior a todos as outras, ficando em seguida a ferramenta Nagios. Em função disso, foram escolhidas para análise neste trabalho as ferramentas Nagios e Zabbix.

3.2.1 Nagios

O Nagios é um software livre sob a licença GPL (*General Public Licence*) desenvolvido por *Ethan Galstad* com o objetivo de monitorar e gerenciar redes de computadores, ou seja, monitorar e gerenciar dispositivos, aplicativos, protocolos e demais dispositivos gerenciáveis que seja possível implementar um *script* (*plugins*) para ler um estado e retornar essa informação no formato esperado pelo Nagios.

O Nagios é uma ferramenta de monitoração de aplicações ou condições de recursos computacionais das organizações. Permite alertar aos administradores ou grupos de administradores através de alguns meios de comunicação como e-mail e SMS etc. O programa gera estatísticas diversas como queda de serviços e conexões, disponibilidades e desempenho, fornecendo uma topologia da rede monitorada. (Nagios, 2015).

Segundo Black (2008) e Nagios[1] (2015), o Nagios é um sistema de monitoramento poderoso que permite às organizações identificar e resolver problemas de infraestrutura de TI antes que eles afetem os processos críticos de negócios, através de diversos *plugins* disponíveis em sua comunidade. Ele verifica *hosts* e serviços especificados,

[1] http://nagios.sourceforge.net/docs/nagioscore/4/en/plugins.html

gerando alertas quando algo está fora dos padrões pré-definidos. Originalmente desenvolvido para rodar em Linux, porém hoje, há pacotes personalizados para distribuições comuns como *Fedora, Ubuntu, Debian e Windows*.

O Nagios foi originalmente desenvolvido para rodar no Linux, apesar dele poder funcionar na maioria dos *Unix*. Algumas das várias ferramentas do Nagios incluem:

- Monitoramento de rede e serviços (SMTP, POP3, HTTP, NNTP, PING, etc.);
- Monitoramento dos recursos de clientes (carga de processador, uso do disco rígido, uso da memória, processos sendo executados, arquivos de logs e etc.);
- Organização simples de *plugins* que permite aos usuários desenvolverem seus próprios serviços de checagem;
- Checagem paralela de serviços;
- Habilidade para definir hierarquia de redes de clientes usando clientes pais (*parent hosts*), permitindo a detecção e distinção entre clientes que estão desativados e aqueles que estão inalcançáveis;
- Notificação de contatos quando problemas em serviços e clientes ocorrerem ou forem resolvidos (via *email*, *pager*, ou métodos definidos pelo usuário);

Habilidade para definir tratadores de eventos (*event handlers*) que serão executados durante eventos de serviços ou clientes na tentativa de resolução de problemas;

- Rotatividade automática de arquivos de logs;
- Suporte para implementação de clientes de monitoramento redundantes;

Interface *web* para visualização do status atual da rede, histórico de notificações e problemas, arquivos de log e etc. (NAGIOS, 2015).

3.2.1.1 *Arquitetura do Nagios*

A ferramenta Nagios é composta basicamente por uma interface gráfica de monitoramento, somada aos *plugins* que são responsáveis pela execução das checagens. Esses plugins retornam respostas numéricas seguidas de informações sobre a checagem. A despeito disso, MAGNANI (2009), apresenta os valores numéricos retornados que serve de base para que o sistema determine se aquele serviço se encontra em funcionamento ou com alguma anormalidade. São os chamados *retval* (valores de retorno), códigos de saída de comandos. Os códigos mais comuns são: 0 (zero) para determinar um estado *OK/UP*; 1 (um) para determinar

um estado *WARNING* e 2 (dois) para determinar um estado *CRITICAL/DOWN* e 3 (três) para o estado *UNKNOWN*. Esses valores estão definidos nos de configuração (Nagios 2015[2]).

Outra funcionalidade do Nagios é o envio de alertas emitindo o estado dos agentes e serviços. O Nagios pode alertar visualmente alterando as cores de acordo com os estados e sonoramente, além de enviar e-mails ou outros tipos de notificação que estejam configurados, SMS (*Short Message Service*), WAP (*Wireless Application Protocol*). Da mesma forma, pode também tomar ações automáticas com objetivo de solucionar o problema, como executar um *script* para reiniciar um serviço, essa função é conhecida com *event handlers* ou tratadores de eventos (ROSSETE; BEZELLI, 2013).

A interface de gerenciamento utiliza HTML (*Hiper Text Markup Language*) e arquivos executáveis do tipo CGI (*Common Gateway Interface*) para exibição e manipulação das informações, além de utilizá-los para enviar comandos ao sistema principal. Os CGI´s utilizados são descritos no quadro 1.

CGI	**Descrição**
avail.cgi	Executável responsável pela geração de relatórios de disponibilidade.
cmd.cgi	Gerencia comandos externos para o sistema principal.
config.cgi	Apresenta os grupos de hosts, serviços, contatos e os prazos definidos nos arquivos de configuração.
extinfo.cgi	Gerencia os comandos externos e as informações do sistema, como comentários, agendamentos e informações de processos.
histogram.cgi	Gerador de relatórios de histogramas da disponibilidade de hosts e serviços.
history.cgi	Exibe os relatórios gerados de histórico dos hosts.
notifications.cgi	Exibe as notificações dos serviços dos hosts enviados aos contatos.
outages.cgi	Produz uma lista de problemas causadores de interrupções na rede.
showlog.cgi	Exibe os arquivos de logs do sistema.
status.cgi	Principal CGI do sistema, responsável por gerenciar o estado dos hosts e serviços monitorados através dos plugins assim como as checagens dos grupos de hosts e serviços.
statusmap.cgi	Cria o mapa da rede baseado nas configurações de hosts pais e filhos.
statuswml.cgi	Interface WAP de gerenciamento das informações da rede.
statuswrl.cgi	Cria um mapa de rede com tecnologia 3D dos hosts definidos.
summary.cgi	Fornece relatório genérico de alertas de hosts e serviços.
tac.cgi	Visão panorâmica de toda a atividade de monitoramento da rede.
trends.cgi	Gera relatórios de tendências dos hosts e serviços.

Quadro 1 - Arquivos CGI do Nagios.
Fonte: Adaptado Nagios (Site Oficial, 2015)

[2] Disponível em: <http://nagios.sourceforge.net/docs/nagioscore/4/en/plugins.html>

A configuração do sistema se dá por meio de arquivos de texto, desde as informações principais até as definições de *hosts* e serviços. A manipulação desses arquivos é considerada complexa como explica o seu criador (Nagios, 2015).

Os arquivos de configuração principal são os *cgi.cfg* e *nagios.cfg*. O primeiro é responsável pelas definições referentes ao funcionamento da interface gráfica, também dos arquivos CGI e das permissões de acesso. O segundo arquivo possui a configuração principal do sistema, contendo o caminho dos diretórios dos arquivos de configuração de *hosts*, serviços, comandos, períodos de monitoramento e notificações.

A configuração principal permite criar uma estrutura de arquivos e diretórios da forma que o usuário desejar, podendo especificar quais arquivos serão lidos para definir as diretrizes do monitoramento. O usuário pode optar por utilizar apenas um arquivo para todas as informações que serão incluídas. O Nagios denomina como objetos os elementos monitorados, no caso os *hosts* e *services*. Esses objetos estão definidos nos arquivos de configuração, e cada elemento configurado é um objeto. Nagios (2015).

O quadro 2 exemplifica uma estrutura de arquivos simplificada. Dependendo da versão o nome do arquivo agrega novas palavras.

Arquivo	**Definições**
commands.cfg	Arquivo contendo todas as definições de comandos a serem executados pelo Nagios, desde os comandos de plugins até de notificação. Todos os comandos que o sistema executar deve estar definido nesse arquivo.
contacts.cfg	Contém os contatos dos envolvidos a serem notificados, bem como seus grupos.
hostgroups.cfg	Configura a criação do(s) grupo(s) de host(s).
hosts.cfg	Definição dos hosts para criação de grupos de hosts que serão monitorados.
servicegroups.cfg	Configuração de grupos dos serviços monitorados.
services.cfg	Definição dos serviços a serem monitorados.
templates.cfg	Apresenta os modelos de configuração que podem ser utilizados como padrão.
timeperiods.cfg	Definição dos períodos a serem utilizados para checagens e notificações.

Quadro 2 - Arquivos de Configuração.
Fonte: Adaptado Nagios.

Para que o sistema funcione e os arquivos de configuração sejam lidos e executados, é necessário ter um *daemon*, ou seja, um arquivo executável responsável por fazer com que todas essas configurações sejam integradas e funcionais. O executável do Nagios, dependendo da versão, e neste caso está localizado em "*/etc/init.d/nagios/*" e se chama nagios. Portanto, para execução do Nagios é preciso iniciá-lo com o comando "*/etc/init.d/nagios*

start", que nada mais é do que fazer com que o binário execute com base no arquivo principal de configuração toda vez que houver uma alteração nos arquivos de configuração. Para checar se há erro nas configurações basta executar o comando "*nagios -v /etc/nagios/nagios.cfg*" (Nagios, 2015).

A documentação do Nagios *Core*, declara que depois da inicialização do sistema, é feito um agendamento automático das checagens, e estas são escalonadas de acordo com um mecanismo interno e suas configurações. As checagens geram registros que são armazenados em arquivos de *log*, o que mantém um histórico de tudo que ocorre no monitoramento. Com base de armazenamentos de *logs* em arquivos de texto, o sistema gera relatórios de disponibilidade, tendências, históricos, notificações, alertas e eventos.

Com o sistema funcionando, é permitido interagir com a ferramenta por meio da sua *interface web*. As principais funções que podem ser executadas são: reagendamento de checagem; habilitar/desabilitar checagens e notificações; reconhecimento de problemas; agendamento de manutenção; adição de comentários. Essas opções facilitam o monitoramento através dos históricos de problemas, adotando soluções, além de documentar os eventos e potencializar com relatórios.

O Nagios permite criar grupos de *hosts* e de serviços que auxiliam na visualização e gerenciamento, pois o usuário pode utilizar das opções listadas acima a partir de um grupo, executando-as uma só vez ao invés de uma para cada *host* ou serviço. No entanto há uma diferença básica entre grupos de *hosts* e grupos de serviços. Nos grupos de *hosts*, o sistema analisa o estado de todos os serviços pertencente aos *hosts* daquele grupo. Enquanto em grupos de serviços, apenas são gerenciados os serviços específicos que foram agrupados no grupo destes serviços.

As checagens ocorrem por meio de *plugins* (*scripts*) instalados nos *hosts* monitorados, que podem ser os já desenvolvidos pela comunidade Nagios ou por colaboradores. O Nagios exige a instalação de um pacote básico de *plugins* disponível em seu *site* Nagios (2015). Esse pacote contém alguns dos principais *scripts* para o monitoramento da rede, possibilitando a partir deles checar serviços como PING, HTTP, SMTP, POP, SNMP, DHCP, DNS, FTP, além de checagem de serviços em máquinas *Windows*, checagens via *ssh* (executando remotamente outros *scripts*), entre outros. O diretório padrão dos *plugins* é "*/usr/local/nagios/libexec*". As checagens são classificadas em dois tipos: As ativas, onde servidor de monitoramento executa um *plugin* e aguarda o retorno da checagem e as passivas, onde o *host* ou serviço monitorado envia um estado para o servidor de monitoramento.

Cabe citar o trabalho de Carvalho (2010), em relação à funcionalidade da checagem passiva. Ela possui uma vantagem em relação à checagem ativa pelo fato dos *hosts* ou serviços monitorados enviarem o estado sem que o servidor de monitoramento realize as consultas. Com isso, há um uso minimizado do tráfego na rede.

Para realizar as checagens remotas existem duas opções mais utilizadas: checagem via *ssh* e checagem via *nrpe*. Na checagem via *ssh* não é necessário que a máquina remota possua algum agente específico instalado, apenas é preciso que exista um servidor *ssh* em funcionamento e, para garantir uma maior segurança na conexão se pode fazer uso de autenticação por chaves públicas e privadas evitando que a senha trafegue pela rede. No caso das checagens via *nrpe* é imprescindível que haja um agente na máquina remota aceitando conexões do servidor de monitoramento e, por segurança, aceitar apenas conexões do *IP* desse servidor com uma senha de autenticação.

Após configurar os arquivos de *hosts, services* e os *deamons* nas máquinas remotas, em pleno funcionamento, o monitoramento se faz sem a intervenção humana, bastando o operador verificar os alertas e tomar as decisões baseadas nos gráficos apresentados na interface web do Nagios.

3.2.1.2 *Agentes do Nagios*

O Nagios é uma ferramenta poderosa e flexível, e essa questão é fortalecida devido ao desenvolvimento de projetos adicionais a ele. Por ser um software livre, permite a colaboração de toda a comunidade *opensource*. Dessa forma, surgiram funcionalidades criadas por usuários da comunidade que facilitam e potencializam o monitoramento. Muitas delas podem ser encontradas na página *exchange.nagios.org* (Nagios[3], 2015).

O Nagios, diferentemente de outras ferramentas de monitoramento, não inclui nenhum mecanismo interno de verificação de *status* de máquinas ou serviços de rede, o sistema utiliza-se de programas externos chamados *plugins.*

Balsemão (2008) dá uma definição de *plugins*, conforme citação abaixo:

> *Plugins* são executáveis compilados ou *scripts* (Perl, shel, etc.) que podem ser rodados por linha de comandos. Esses *plugins* serão executados sempre que o Nagios precisar fazer uma checagem no serviço ou máquina, retornando os

[3]Disponível em: < http://nagios.sourceforge.net/docs/nagioscore/4/en/plugins.html>

> resultados para o Nagios que irá processá-los e tomar as ações necessárias, rodando algum aplicativo, mandando notificações e etc.

3.2.1.2.1 Agente *NRPE*

É utilizado principalmente quando há necessidade de checar recursos locais a pedido do Nagios, como uso de disco, memória, processos e CPU. Essa funcionalidade também possibilita executar *plugins* em máquinas remotas, comunicando com outros *plugins* do agente *Windows*, assim como pode executar *scripts* para verificar métricas remotamente nestas máquinas. Cabe citar (BITTENCORT et al, 2010), no que refere ao agente NRPE, ele é um *software* que tem como objetivo executar *plugins* locais em *hosts* remotos a pedido do Nagios. O plugins *check_nrpe* é executado no servidor de monitoramento e envia pedidos de execução de *plugins* ao agente *nrpe* alojado no *host* cliente.

3.2.1.2.2 Agente *NSCA*

Implementa as checagens passivas, permitindo que um *host* ou serviço envie seu estado ao *daemon* do Nagios. Útil para o processamento de alertas de segurança, bem como nas configurações redundantes e distribuídas do Nagios (Nagios[4], 2015).

3.2.1.2.3 Agente NSClient++

É um agente instalado em máquinas *Windows* que permite a checagem de serviços do sistema, como disco, memória, processos, serviços, entre outros. Esse agente está disponível para plataformas 32 e 64 bit e deverá ser instalado em cada máquina monitorada.

Esse agente traz em si uma quantidade limitada de checagem, sendo necessário o desenvolvimento de outros *plugins* para o monitoramento. Porém é necessária a instalação deste agente para o monitoramento de máquinas *Windows*.

---

[4] http://nagios.sourceforge.net/docs/nagioscore/4/en/plugins.html

Balsemão (2008, p. 20), "[...] para o monitoramento de uma máquina *Windows* é necessária à instalação de um agente, que irá atuar como um *proxy* entre um *plugin* Nagios e o real serviço na máquina *Windows*. Não é possível o monitoramento via Nagios sem este agente. "

3.2.2 Zabbix

O Zabbix é uma ferramenta utilizada para realizar o monitoramento e controle dos componentes de rede. Com ela o administrador de redes pode trabalhar de forma proativa e reativa no gerenciamento de rede e assim prevenir possíveis falhas, ativar e desativar serviços remotamente, monitorar o tráfego, controlar o acesso de usuários e monitorar demais serviços.

Este *software* foi desenvolvido por Alexei Vladishev em 1998. A ideia surgiu quando trabalhava em um banco na Letônia como administrador de sistemas, pois não estava satisfeito com os sistemas de monitoração que estava trabalhando. O Zabbix efetua o inventário de rede coletando dados e informações dos dispositivos gerenciados, faz o monitoramento dos ativos de rede, tais como roteadores, *switches*, impressoras e *nobreaks*, além de verificar se os serviços oferecidos pela administração de redes estão ativos e funcionando da forma planejada e configurada. (LIMA 2014).

3.2.2.1 *Arquitetura do Zabbix*

Lima (2014) em seu livro classifica a arquitetura do Zabbix no contexto dos serviços de rede, seguindo o modelo de três camadas; Aplicação, banco de dados e *interface web*. A camada de aplicação faz a coleta dos dados nos ativos de rede, a camada de banco de dados é representada pela base de dados e a *interface web* responsável por dá ao administrador o acesso às informações de monitoramento.

Conforme Zabbix[5] (2015), a configuração, o monitoramento e controle dos componentes da rede, são feitos através de *interface WEB,* possibilitando que o administrador de redes possa acessar o servidor pela sua estação de trabalho, sem que ele se desloque até a entidade gerenciadora, onde o *software* e o processo gerente foram instalados, para fazer modificações e acessar dados e informações referentes ao gerenciamento de redes.

[5] https://www.zabbix.com/documentation/2.0/manual/introduction

Essa ferramenta trabalha com mecanismos de *polling* e *trapping*, aonde *polling* é uma comunicação de requisição/resposta em tempo real e *trapping* são alarmes enviados pelos agentes fazendo notificações sem que haja a requisição do processo gerente.

O Zabbix envia alerta via e-mail, por SMS (*Short Message Service*) para o administrador de redes. Esses alertas informam que algum evento, não esperado, aconteceu em um de seus dispositivos gerenciados. Os alertas são gerados através das *triggers*, que são mecanismos de determinação de avisos quando algo ultrapassar os limites determinados para cada serviço (ZABBIX[6], 2015).

Através da *interface WEB* é possível criar o mapa da rede gerenciada. Esse mapa auxilia o administrador de rede a entender como está à topologia da rede, o estado dos agentes em cada um dos dispositivos e objetos gerenciados, ou seja, se estão *up* ou *down,* mostrando se existe ou não alertas ativos dentro da rede gerenciada. Assim como também a visualização dos gráficos gerados, os relatórios dos eventos realizados e das tarefas realizadas pelo administrador de rede.

Na aba administração, é possível criar usuários e grupos de usuários e seus níveis de acesso e permissões ao sistema de gerenciamento de redes. O Zabbix traz como padrão, os usuários: *admin* e *guest*. Os níveis de acesso e permissões que estão definidos são: Zabbix Super Admin, Zabbix Admin e Zabbix User. No entanto é possível criar novos grupos de usuários. Após a instalação é necessário que o gerente modifique as senhas dos usuários *admin* e *guest*, pois as mesmas veem em branco. Para um melhor controle é sugerido que o administrador de redes crie um usuário para si e para algum outro colaborador de sua equipe, com o nível de acesso que melhor julgar necessário.

O controle de acesso gera *logs* que indicam qual usuário realizou modificações, quem está logado no momento e ainda para quem o sistema enviou um alerta.

Os meios de notificações: e-mail, mensagem instantânea e SMS, são configurados de acordo com a necessidade do administrador de redes. A distribuição desse serviço é feita especificamente por usuários ou por grupos de usuários.

Em suas configurações são feitas alterações de como o processo gerente irá trabalhar para requisitar as coletas de dados e informações dos agentes. Nessas configurações, é possível ativar, desativar, criar e apagar tarefas, ações e alertas de acordo com necessidade

[6] https://www.zabbix.com/documentation/2.0/manual/introduction

do administrador. Além disso, é possível buscar novos *hosts,* descobrir novos agentes, montar gráficos específicos mesclando os dados e informações de diferentes categorias.

O Zabbix oferece uma vasta lista de sistemas operacionais com o qual os seus agentes podem operar coletando dados e informações para a entidade gerenciadora. São eles:

- Linux;
- Solaris;
- HP-UX;
- AIX;
- Free BSD;
- Open BSD;
- OS X, Tru64/OSF1;
- Windows.

Para cada um são oferecidas *Templates* com configurações específicas e diferentes para realizar o monitoramento de cada dispositivo.

O Zabbix oferece uma *interface* padrão de trabalho e na parte superior é possível selecionar a ação de que se pretende executar através do menu que possui opção como *Monitoring, Inventory* e *Reports*. Na parte posterior abaixo é possível selecionar de forma mais especifica ações como *Overview, Web e Latest data*. Feita essa seleção, é listado uma série de paramentos no qual é possível consultar os objetos gerenciados dentro dos dispositivos gerenciados. As estatísticas desse dispositivo podem ser obtidas no modo texto ou de um gráfico gerado pelo Zabbix. (ZABBIX[7], 2015).

3.2.2.2 *Agentes do Zabbix*

Dentro da arquitetura do Zabbix, existem três elementos que realiza todo trabalho pesado da ferramenta. Isso vem ao encontro das informações aludidas por Lima (2014) e Zabbix (2015).

[7] Disponível em: <https://www.zabbix.com/documentation/2.0/manual/introduction>

3.2.2.2.1 Zabbix Server

O zabbix *server* é o agente que armazena os dados coletados na base de dados dos ativos monitorados que são acessíveis através da interface web.

3.2.2.2.2 Zabbix Agente

O zabbix agente é o responsável por responder as requisições do Zabbix *server* ou enviar dados do monitoramento dos ativos de rede. Está disponível para a maioria das plataformas Unix e Windows, com pacotes pré-compilados, podendo também ser visualizados com agentes externos tais como: SNMP, IPMI, SSH, etc. (ZABBIX, 2015).

3.2.2.2.3 Zabbix Proxy

O Zabbix *proxy* é uma parte opcional de implantação Zabbix. No entanto, pode ser muito benéfico para distribuir a carga de um único servidor Zabbix.

O Zabbix *proxy* é um *host* responsável por fazer a coleta em clientes remotos em nome do Zabbix server. Após a coleta o Zabbix *proxy* consolida os dados e transmite um pacote com todos os dados para o Zabbix *server*.

3.3 Tráfego de Rede

Tráfego de rede é a quantidade de informações trocadas entre o servidor e os computadores que realizam o acesso. Informações enviadas pelo visitante ao servidor e pelo servidor ao visitante irão somar à contagem do tráfego de informações.

Cisco (2015) tem uma definição de tráfego:

> O tráfego é definido como a quantidade de dados ou o número de mensagens em um circuito durante um determinado período de tempo. O tráfego também inclui a relação entre as tentativas de chamada em equipamento sensível ao tráfego e a velocidade em que a chamada é completada [...] (Cisco, 2015, p. 02).

3.3.1 Análise de Tráfego

A análise de tráfego tem por objetivo avaliar os principais parâmetros de tráfego existente numa rede de computadores, que são: atraso (Latência), variação do atraso (*jitter*), perda de pacotes (confiabilidade) e vazão (capacidade).

Stahlschmidt (2010), afirma que apesar da maioria das redes *IP* não fornecerem qualquer garantia de serviços e no caso de algumas aplicações exigirem restrições, é necessário incorporar a essas redes a qualidade de serviço, mantendo as tolerâncias permitidas para cada parâmetro do tráfego.

Prado et al (2012), frisou a importância do uso de cálculo estatísticos em todo processo de medição. Inevitavelmente, por mais criterioso que seja a medição sempre há presença de erros. Nesta linha, (Kamienski et al. 2005), utilizou em seu trabalho a média e o intervalo de confiança para representar a precisão das medidas.

"Numa distribuição estatística o erro associado a uma estimativa define um intervalo de variação ou incerteza em torno da média ao qual se pode atribuir um nível probabilístico (percentual) de confiança..." (PRADO et al. 2012)

3.4 Ferramenta de Análise de Pacotes

Dentre as ferramentas de análise de pacote disponíveis, será usada neste trabalho a ferramenta de captura e análise de pacote *Wireshark*. Esta ferramenta visualiza todas as interfaces de rede disponíveis na máquina onde está instalada, possibilitando capturar e analisar os pacotes gerados.

3.4.1 Wireshark

O *Wireshark* é um analisador de protocolo que permite a captura e a navegação interativa do tráfego na rede de computadores em tempo de execução usando a interface de rede do computador desde que seja configurada de acordo com a interface escolhida. Esta ferramenta instalada na mesma rede é capaz de capturar todo o tráfego originado nas interfaces rede.

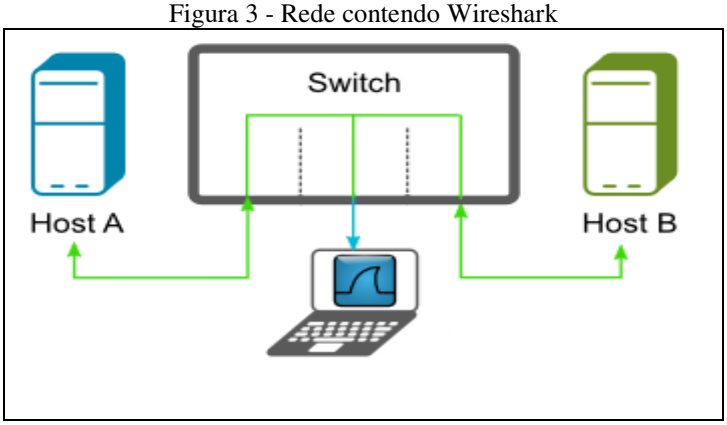
Wireshark faz analogia como sendo um dispositivo de medição usado para examinar o que está acontecendo dentro de uma rede, assim como um voltímetro é usado por um eletricista para determinar a tensão nos terminais de um fio condutor. Ele é caracterizado como uma das melhores ferramentas de captura de pacotes de código aberto disponível atualmente (Farruca 2009).

A aplicação do *Wireshark* abrange diversas situações. Para os administradores, é usado na solução de problemas na rede, enquanto para os engenheiros de segurança, a principal função é examinar os problemas envolvendo segurança. Os desenvolvedores utilizam o *Wireshark* para depurar implementação de protocolos e o usuário comum, pode utilizar para conhecer os protocolos internos.

3.4.1.1 *Captura de pacotes com o Wireshark*

A ferramenta *Wireshark* deverá ser instalada em uma máquina pertencente à rede que contenha o tráfego a ser capturado, conforme ilustrado na Figura 1. O *Wireshark* captura todos os tipos de tráfegos existentes na rede, desde que a captura esteja configurada em modo promiscuo. Wireshark[8] (2015) apresenta a configuração em modo promíscuo que é realizada na própria interface gráfica da ferramenta.

Figura 3 - Rede contendo Wireshark



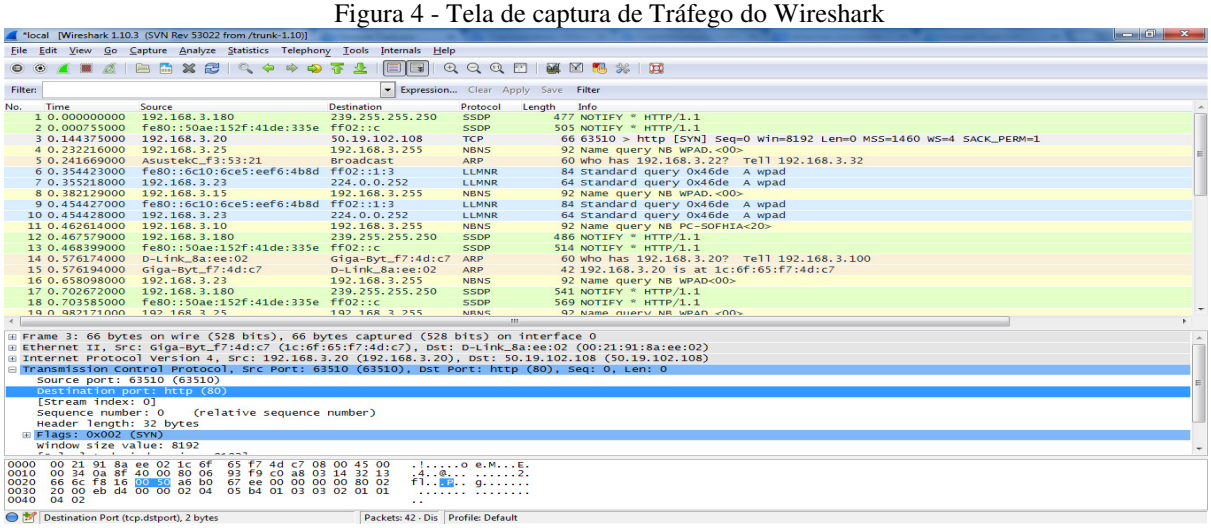
3.4.1.2 *Identificado e analisando o tráfego da rede*

Ao iniciar a captura, o *Wireshark* apresenta o tráfego na rede analisada, através de uma tela de captura conforme Figura 4.

[8] https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs

Nesta tela é possível visualizar os pacotes de origem e destino pelos protocolos usados, além da informação contida em cada pacote. Este trabalho não abrange as configurações da ferramenta, pois é de fácil entendimento e está disponível no *site* do próprio *Wireshark*.

Figura 4 - Tela de captura de Tráfego do Wireshark



Fonte: autor.

A tela de captura do *Wireshark* é composta basicamente por três painéis. O painel da lista dos pacotes, contendo todo tráfego capturado. O painel de detalhes dos pacotes que contém os cabeçalhos, o tipo de protocolo utilizado, portas de origem e de destino. Por último tem o painel dos pacotes em *bytes* conforme Figura 4.

A análise realiza-se através dos *menus Statistics* e *Analyze*. Em *Statistics* no campo *Endpoit List*, clicando em *TCP (IPv4 & IPv6)* depois em *Port* na janela *TCP Endpoit* visualiza-se todas as portas usadas no tráfego, os pacotes, as taxas em bytes e etc.

4 PROCEDIMENTOS METODOLÓGICOS

Este trabalho visa realizar um estudo da análise de dados do monitoramento da rede de computadores utilizando as ferramentas Nagios e Zabbix, buscando-se determinar a quantidade de tráfego gerado na rede, utilizando a ferramenta de captura *Wireshark*.

O gerenciamento será realizado usando a infraestrutura existente da rede interna de uma empresa, composta por máquinas com sistema operacional *Windows*, a qual não haverá alteração na topologia da rede e a validação ocorrerá da comparação tráfego gerado pelas ferramentas utilizando o *Wireshark* para capturar o tráfego e com ajuda do *excel*, versão 2010, calcular a média, desvio padrão e intervalo de confiança.

A estrutura da rede analisada neste trabalho é mostrada na Figura 5 e o trabalho objetiva comparar entre as ferramentas Nagios e Zabbix e definir qual possui menor quantidade de tráfego na rede no processo de monitoramento.

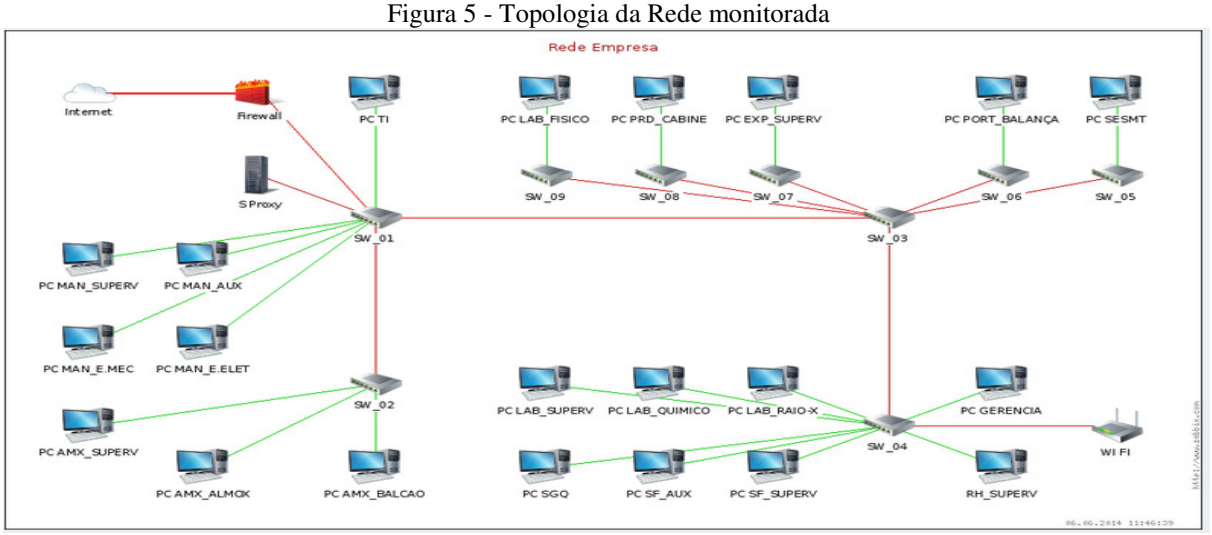
A validação será determinada pela análise de três cenários de monitoramento, envolvendo uma quantidade diferente de máquinas monitoradas em cada cenário. Os cenários foram definidos em três momentos de monitoramento com as duas ferramentas.

O desempenho das ferramentas será obtido através da medição da média, do desvio padrão e do intervalo de confiança estabelecido pelo nível de confiança de 95 % do tráfego gerado na monitoração. Ou seja, a chance da média ocorrer no intervalo de confiança determinado é de 95 %.

4.1 Rede Monitorada

A Figura 5 representa a topologia da rede composta por máquinas com sistema operacional *Windows*. O levantamento das características da rede foi coletado realizando visitas técnicas a empresa, acompanhado do responsável pela administração da rede.

Figura 5 - Topologia da Rede monitorada



Fonte: autor. Adaptado: Mapa Zabbix.

A empresa utiliza a topologia estrela segmentada, dispondo de um link de internet, um servidor de arquivos Debian, um Firewall com Proxy e uma VPN.

A rede de dados foi reformada no início de 2011, quando foi ampliando o número de pontos de acesso e a substituição de cabos UTP5e que conectavam cada *switch* dos setores por uma estrutura de fibra ótica Monomodo conforme descrito na Tabela 1.

Tabela 1 - Estrutura de Backbone

Representação	**Descrição**
SW - 01 – SW – 02	TIC – Almoxarifado
SW - 01 – SW – 03	TIC – Escritório
SW - 03 – SW – 05	Escritório – SESMT
SW - 03 – SW – 06	Escritório – Portaria
SW - 03 – SW – 07	Escritório – Expedição
SW - 03 – SW – 08	Escritório – Forno
SW - 03 – SW – 09	Escritório – Lab. Físico

A conexão dos sistemas finais é feita via cabo UTP5e, dispondo de um ponto de acesso *wireless* localizado no escritório administrativo. Utiliza uma máscara de rede de 24 bits, onde o endereçamento é feito de modo estático conforme descrito na Tabela 2.

Tabela 2 - Estrutura Secundária UTP5e1
Fonte: Autor.

Identificação	**Descrição**	**Configuração**	**Ponto Acesso**
PC TI	Encarregado de TI	192.168.3.10/24	SW – 01
PC MAN_SUPERV	Supervisor de manutenção	192.168.3.30/24	SW – 01
PC MAN_AUX	Auxiliar administrativo	192.168.3.18/24	SW – 01
PC MAN_E.MEC	Encarregado da mecânica	192.168.3.35/24	SW – 01
PC MAN_E.ELET	Encarregado da elétrica	192.168.3.31/24	SW – 01

PC AMX_SUPERV	Supervisor de suprimentos	192.168.3.17/24	SW – 02
PC AMX_ALMOX	Almoxarife	192.168.3.23/24	SW – 02
PC AMX_BALCAO	Balcão do almoxarifado	192.168.3.29/24	SW – 02
PC SGQ	Assistente da qualidade	192.168.3.11/24	SW – 04
PC SF_SUPERV	Encarregado do setor fiscal	192.168.3.12/24	SW – 04
PC SF_AUX	Auxiliar de escritório	192.168.3.27/24	SW – 04
PC GR	Gerência	192.168.3.13/24	SW – 04
PC RH_SUPERV	Encarregado de RH	192.168.3.14/24	SW – 04
PC LAB_SUPERV	Encarregado de laboratório	192.168.3.20/24	SW – 04
PC LAB_RAIOX	Bancada do Raio – X	192.168.3.16/24	SW – 04
PC LAB_QUIMICO	Bancada do laboratório químico	192.168.3.15/24	SW – 04
PC LAB_FISICO	Bancada do laboratório físico	192.168.3.33/24	SW – 09
PC SESMT_TEC	Téc. de segurança do trabalho	192.168.3.34/24	SW – 05
PC PORT_BALANCA	Balança	192.168.3.24/24	SW – 06
PC EXP_SUPERV	Encarregado de expedição	192.168.3.21/24	SW – 07
PC PROD_CABINE	Cabine do forno	192.168.3.28/24	SW – 08
PC PROD_ENC	Encarregado de Produção	192.168.3.40/24	SW – 08
PC PROD_CABINE	Supervisor de Produção	192.168.3.149/24	SW – 08

Ressalta-se que por motivo de segurança, o acesso e monitoramento foram restritos para alguns computadores e serviços. As máquinas disponíveis para monitoramento são aquelas usadas pelos usuários onde armazenam dados e realizam suas tarefas diárias pertinentes as suas funções individuais. Apesar da rede conter *switches* na sua topologia, estes não foram monitorados por não serem gerenciáveis, ficando de fora do monitoramento.

Conforme o objetivo do trabalho, não faz parte do escopo o monitoramento da totalidade dos ativos de rede. O que interessa é o comparativo entre as ferramentas de monitoramento, tendo em vista que ao analisar um conjunto de máquinas, isso possa aplicar para rede em geral. As máquinas e serviços monitorados estão definidos nas seções 5.1 e 5.2 e apresentados nas figuras 7 e 9.

A análise dar-se-á pelo comparativo do tráfego gerado no monitoramento da rede com as ferramentas Nagios e Zabbix determinando a média, o desvio padrão e o intervalo de confiança de cada ferramenta.

4.2 Instalação do Nagios

O Nagios[9] foi instalado num ambiente virtual, usando a VM *Virtualbox*[10]. Este trabalho não contempla o estudo da instalação e configuração do *Virtualbox*, tendo vista que há disponíveis inúmeros tutoriais a respeito. O site do *virtualbox* disponibiliza todo o processo de instalação, configuração e a criação de sistemas virtualizados.

O *Virtualbox* foi instalado sobre a plataforma *Windows*, virtualizando o sistema operacional Ubuntu no qual o Nagios foi instalado e configurado para monitoramento. A partir desta máquina virtual, as ferramentas de monitoramento monitoram a rede.

Para o monitoramento da rede de computadores *Windows* e seus serviços, foi instalado e configurado em cada computador um agente de monitoramento especifico para as máquinas *Windows*, neste caso o *NSClient++*.

4.2.1 Configuração dos Computadores e Serviços Monitorados pelo Nagios

Como toda a configuração do Nagios é realizada via arquivo de configuração, conforme Quadro 2, foi criado os arquivos para cada máquina *Windows*[11] monitorada com seus respectivos serviços ("*pc_lab_quimico.cfg*"). Na linguagem do Nagios, ele refere a computadores com a denominação *host*. Aqui, utilizou-se computador e máquina.

Os computadores foram identificados conforme identificação na Tabela 2 e agrupados em grupos de monitoramento, objetivando determinar o período de monitoramento, os envios de alertas e os horários de notificação. Os computadores pertencem ao grupo chamado de "máquinas Windows".

Depois de criados os arquivos dos computadores e serviços, esses arquivos são referenciados no arquivo principal do Nagios, o *nagios.cfg,* em seguida reiniciado o Nagios para atualizar os arquivos de monitoramento.

No arquivo de configuração *hostgroups.cfg* foi inserido a identificação dos computadores para que eles pertençam a este grupo, aonde foi definido ações de monitoramento.

---

[9] Versão da ferramenta Nagios: 4.0.8
[10] Versão da Virtualbox: 4.2.16 r86992
[11] SO Windows 7 e Windows XP

4.3 Instalação do Zabbix

Assim como o Nagios, a ferramenta de monitoramento Zabbix também foi instalada e configurada na máquina virtual Ubuntu[12], compartilhando o mesmo sistema operacional.

4.3.1 Configuração dos Computadores e Serviços Monitorados pelo Zabbix

A configuração foi realizada usando a *interface web*. A identificação das máquinas seguiu conforme nomeação na Tabela 2. Foi criado um grupo chamado Empresa onde todos os computadores foram agrupados. Nesse grupo foi definido o *e-mail* de contato para notificações, período de monitoramento e intervalo de checagem dos computadores e serviços.

A configuração dos serviços utilizou os *Templates* definidos e existentes no Zabbix, específico para o sistema operacional *Windows*. Esses *templates* contemplaram em sua totalidade todos os serviços monitorados nas máquinas *Windows,* de forma que a quantidade de serviços em cada ferramenta fosse igual para as consultas às máquinas e serviços monitorados.

4.4 Instalação do *Wireshark*

A instalação do capturador de tráfego de rede *Wireshark* foi realizada na própria máquina virtual, no sistema operacional *Ubuntu*.

A decisão foi pelo fato da máquina virtual hospedar as ferramentas de monitoramento e possuir a interface de rede por onde ocorrerá toda comunicação entre os agentes e gerentes no processo de monitoramento da rede.

[12] Versão do sistema operacional Ubuntu: 14.04 LTS

4.4.1 Configuração da interface de rede monitorada

A configuração da interface de rede teve como ponto decisivo a questão do modo promíscuo. Esse modo habilita o capturador a visualizar todo tráfego gerado na rede, segundo *Wireshark* (2015).

A interface de rede escolhida é aquela que terá todo tráfego realizado por ela. Sendo assim, deverá ser escolhida para que o capturador de tráfego consiga visualizar todo tráfego gerado.

Cada captura teve um intervalo de seis minutos e a apresentação dos dados foi em *Bytes* por minuto. Para isso foi necessário a quantidade em *bytes* dos seis minutos para bytes por minuto. Ou seja, a totalidade em *bytes* divido por seis.

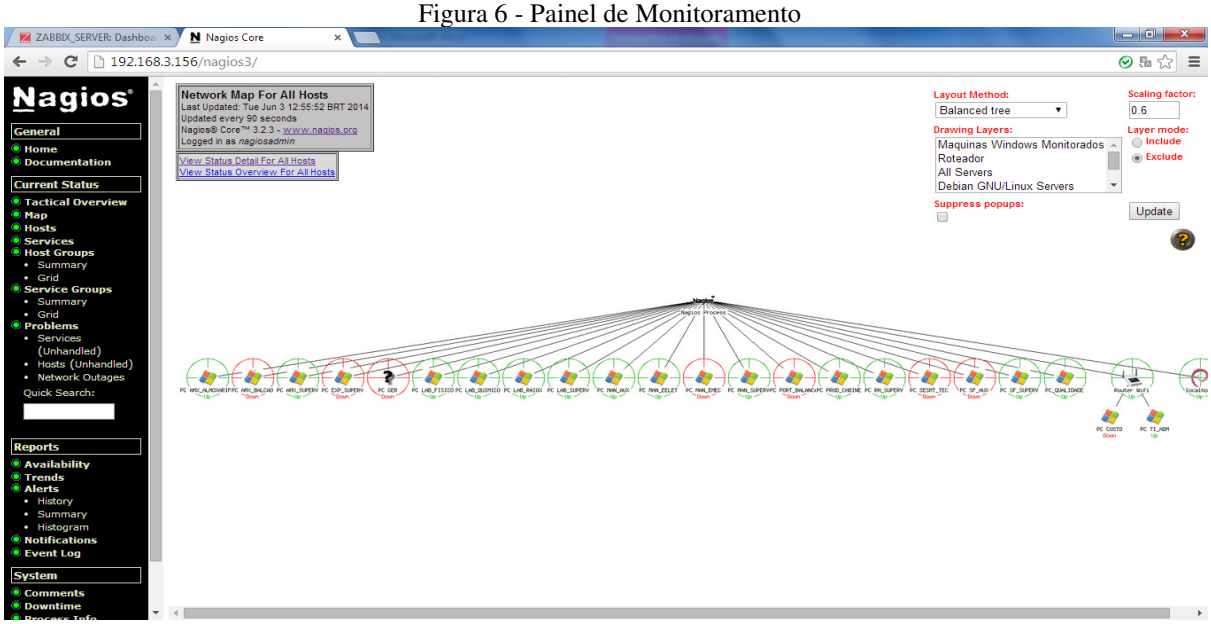
5 DESENVOLVIMENTO/RESULTADOS

O monitoramento da rede foi realizado, configurando os serviços de ambas as ferramentas na mesma quantidade de serviços a fim de atribuir as mesmas consultas para cada ferramenta. Com isso espera-se que a quantidade de tráfego gerado pelas duas ferramentas seja semelhante pela mesma quantidade de serviços.

5.1 Monitoramento com o Nagios

A rede foi monitorada, seguindo a identificação dos computadores conforme descrito na Tabela 2 e os serviços de acordo com o monitoramento realizado pelo agente *NSClient* (NAGIOS[13], 2014). A Figura 5 apresenta a rede monitorada pelo Nagios.

Figura 6 - Painel de Monitoramento



Fonte: Autor. Adaptado: Nagios

Os serviços monitorados pelo Nagios nas máquinas *Windows*, conforme Figura 6, foram: espaço em disco, carga da CPU, verificação de serviços ativos do Windows (Explorer), uso da Memória, versão do agente de monitoramento e tempo de atividade do sistema.

[13] http://nagios.sourceforge.net/docs/3_0/monitoring-windows.html

Figura 7 - Serviços monitorados pelo Nagios no PC LAB_QUIMICO

LAB QUIMICO	C:\ Drive Space	OK	05-21-2015 10:11:57	10d 0h 0m 26s	1/3	c: - total: 24.41 Gb - used: 15.47 Gb (63%) - free 8.95 Gb (37%)
	CPU Load	OK	05-21-2015 10:11:57	10d 0h 0m 26s	1/3	CPU Load 13% (5 min average)
	Explorer	OK	05-21-2015 10:11:58	10d 0h 0m 26s	1/3	Explorer.EXE: Running
	Memory Usage	OK	05-21-2015 10:11:58	10d 0h 0m 26s	1/3	Memory usage: total:3811.44 MB - used: 1096.52 MB (29%) - free: 2714.92 MB (71%)
	NSClient++ Version	OK	05-21-2015 10:11:57	10d 0h 0m 19s	1/3	NSClient++ 0.3.9.327 2011-08-16
	Uptime	OK	05-21-2015 10:12:06	10d 0h 0m 10s	1/3	System Uptime - 3 day(s) 11 hour(s) 37 minute(s)

Fonte: Autor. Adaptado: Nagios

Para realizar o monitoramento, foi necessário instalar os *plugins* no servidor Nagios. O *plugin* responsável por requisitar o estado das máquinas na rede *Windows* é o *check_nt*. Este requisita os estados dos computadores e serviços em paralelo com o *NSClient*.

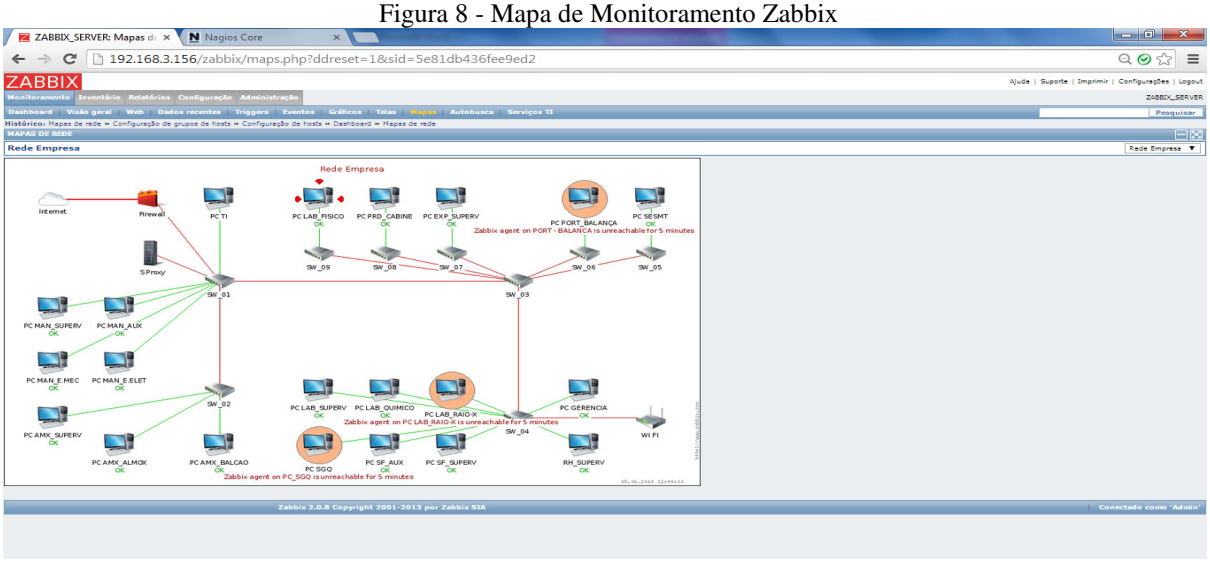
5.2 Monitoramento com o Zabbix

O mapa do Zabbix apresenta uma visão geral do estado de monitoramento. Nesta ferramenta foi visualizada a parte dos favoritos; Gráficos, Telas e Mapas. Ainda nesta tela, foi disponibilizado o estado da ferramenta Zabbix, o estado do sistema composto pelos grupos de computadores, o estado dos computadores estando ou não com incidentes ocorridos.

Assim como no Nagios a rede foi monitorada utilizando o mesmo padrão de identificação dos computadores monitorados e a mesma quantidade de serviços monitorados para uma carga equivalente na geração de tráfego na rede.

A figura abaixo apresenta o mapa de monitoramento fornecido pelo Zabbix.

Figura 8 - Mapa de Monitoramento Zabbix



Fonte: Autor. Adaptado: Zabbix

Os serviços monitorados pelo Zabbix nas máquinas Windows, conforme Figura 8, foram: número de Processos, número de Threads, número de Usuários, tempo de atividade do sistema, total de Memória e versão do Agente de monitoramento.

Figura 9 - Serviços monitorados pelo Zabbix no PC LAB_QUIMICO

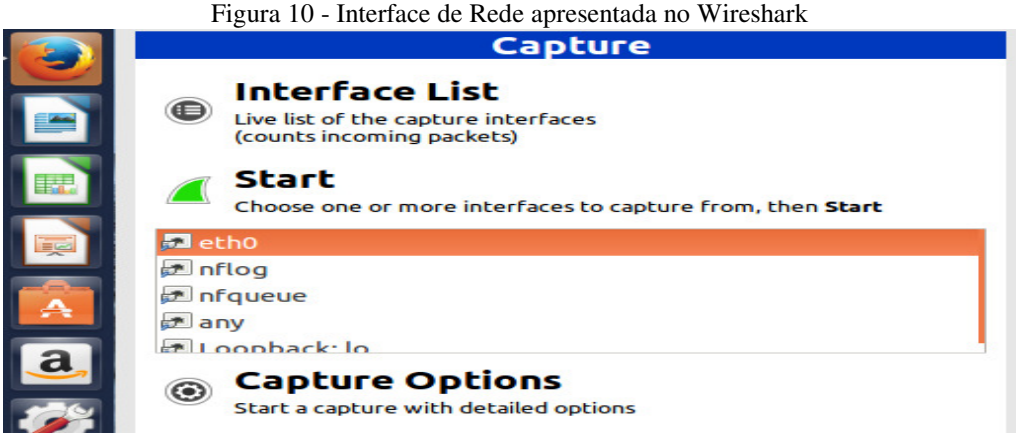
Fonte: Autor. Adaptado: Zabbix.

Para realizar o monitoramento, foi instalado na máquina cliente *Windows* o agente *zabbix*, tendo em vista que o monitoramento foi realizado via agente. Com este agente o *Zabbix* envia consultas para as máquinas e o agente responde as consultas com estado das máquinas e dos serviços.

5.3 Análise do Tráfego com o *Wireshark*

A captura do tráfego de rede foi realizada com a ferramenta *Wireshark* e se deu na *interface eth0* conforme ilustra Figura 9 abaixo. Esta interface foi escolhida por ser a interface da máquina gerente do sistema de gerenciamento.

Figura 10 - Interface de Rede apresentada no Wireshark



Fonte: Autor. Adaptado: *Wireshark*.

Os dados foram coletados em três momentos distintos denominados de cenários 1, cenário 2 e cenário 3, obtidos através da captura do tráfego com o *Wireshark* no processo de

monitoração das máquinas. Cada captura com o *Wireshark* durou seis minutos e foram realizadas trinta capturas por máquina em cada cenário. A captura foi realizada simultaneamente com as duas ferramentas, objetivando tornar a análise mais homogenia possível para as ferramentas, evitando que uma falha na rede, como por exemplo, uma máquina que não esteja respondendo, contribuísse para reduzir a quantidade de tráfego pelo do agente não conseguir responder ao agente.

Os cenários envolvidos no monitoramento com as ferramentas foram realizados com quantidade de máquinas diferente e com a mesma quantidade de serviços em cada ferramenta, objetivando encontrar variações pela quantidade de máquinas inseridas em cada cenário. Conforme abaixo, segue a descrição das máquinas envolvidas em cada cenário.

a) Cenário 1 - Maquinas: PC LAB_QUIMICO, PC LAB_FISICO, PC LAB_SUPERV e PC EXP_SUPERV.

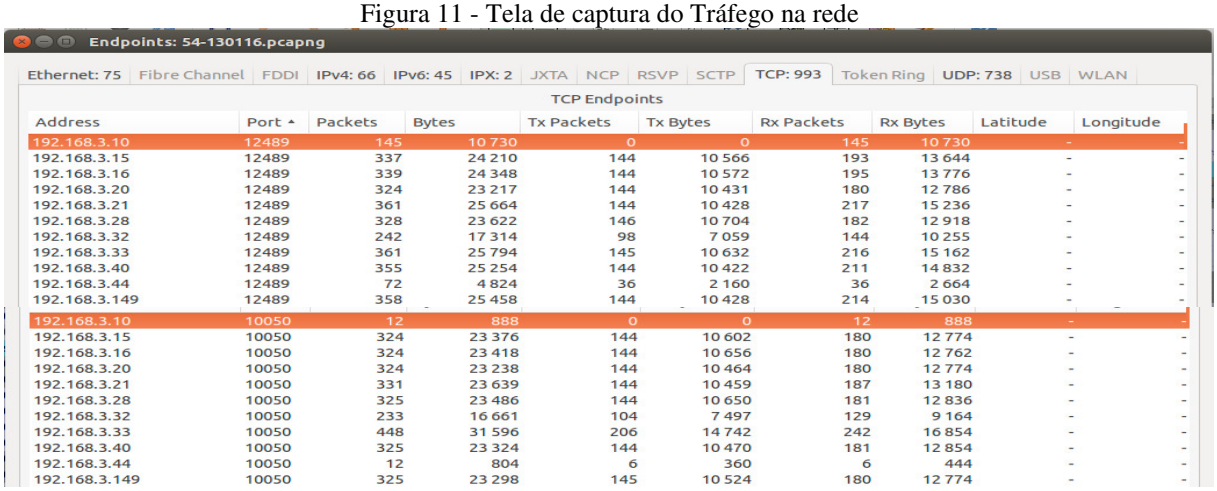
b) Cenário 2 - Maquinas: PC LAB_QUIMICO, PC LAB_FISICO, PC LAB_SUPERV, PC EXP_SUPERV, PC PROD_CABINE e PC RH_SUPERV.

c) Cenário 3 - Máquinas: PC LAB_QUIMICO, PC LAB_FISICO, PC LAB_SUPERV, PC EXP_SUPERV, PC PROD_CABINE, PC RH_SUPERV, PC PROD_ENC e PC PROD_SUPERV.

Os dados das capturas foram coletados usando o filtro *Endpoint List* do *menu Statistics* do *Wireshark,* escolhendo o tipo de tráfego (*TCP IPv4 e IPv6)*, já que o tráfego gerado pelas ferramentas é do tipo *TCP*, depois clicando em *Port*, para escolher as portas usadas pelas ferramentas, 10050 pelo Zabbix e 12489 pelo Nagios. Na aba *Endpoint List,* foi quantificado os pacotes transmitidos assim como também a quantidade em *Bytes*.

Em seguida foi criada uma tabela para cada cenário, contendo a quantidade de pacotes gerados pelas duas ferramentas. As figuras abaixo ilustram as capturas realizadas na aba *Endpoint List* do *menu Statistics*.

Figura 11 - Tela de captura do Tráfego na rede



Endpoints: 54-130116.pcapng

Ethernet: 75 | Fibre Channel | FDDI | IPv4: 66 | IPv6: 45 | IPX: 2 | JXTA | NCP | RSVP | SCTP | TCP: 993 | Token Ring | UDP: 738 | USB | WLAN

TCP Endpoints

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude
192.168.3.10	12489	145	10 730	0	0	145	10 730	-	-
192.168.3.15	12489	337	24 210	144	10 566	193	13 644	-	-
192.168.3.16	12489	339	24 348	144	10 572	195	13 776	-	-
192.168.3.20	12489	324	23 217	144	10 431	180	12 786	-	-
192.168.3.21	12489	361	25 664	144	10 428	217	15 236	-	-
192.168.3.28	12489	328	23 622	146	10 704	182	12 918	-	-
192.168.3.32	12489	242	17 314	98	7 059	144	10 255	-	-
192.168.3.33	12489	361	25 794	145	10 632	216	15 162	-	-
192.168.3.40	12489	355	25 254	144	10 422	211	14 832	-	-
192.168.3.44	12489	72	4 824	36	2 160	36	2 664	-	-
192.168.3.149	12489	358	25 458	144	10 428	214	15 030	-	-
192.168.3.10	10050	12	888	0	0	12	888	-	-
192.168.3.15	10050	324	23 376	144	10 602	180	12 774	-	-
192.168.3.16	10050	324	23 418	144	10 656	180	12 762	-	-
192.168.3.20	10050	324	23 238	144	10 464	180	12 774	-	-
192.168.3.21	10050	331	23 639	144	10 459	187	13 180	-	-
192.168.3.28	10050	325	23 486	144	10 650	181	12 836	-	-
192.168.3.32	10050	233	16 661	104	7 497	129	9 164	-	-
192.168.3.33	10050	448	31 596	206	14 742	242	16 854	-	-
192.168.3.40	10050	325	23 324	144	10 470	181	12 854	-	-
192.168.3.44	10050	12	804	6	360	6	444	-	-
192.168.3.149	10050	325	23 298	145	10 524	180	12 774	-	-

Fonte: Autor. Adaptado: *Wireshark*

5.4 Comparação das Ferramentas usadas

Após a monitoração, as ferramentas apresentaram muita semelhança entre si, sendo bastante recomendadas para o monitoramento da rede e em geral atendem a maioria das necessidades do monitoramento. Porém, cada ferramenta tem suas particularidades e ao refinar o processo comparativo de ambas, há uma visível diferença singular de cada uma.

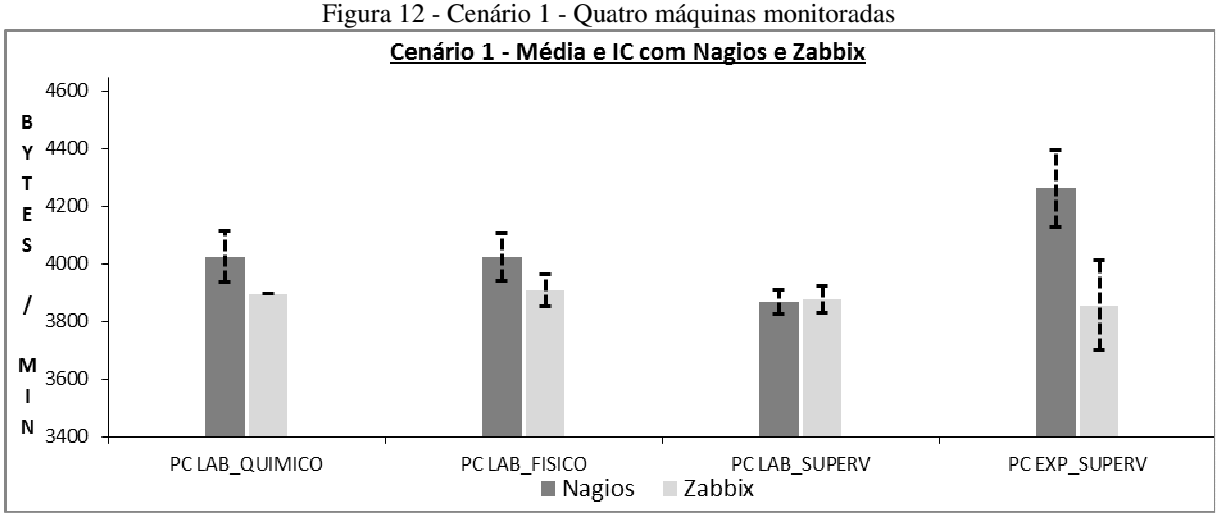
Para a coleta de dados, foram realizados três cenários de coleta. Embora, tanto o Nagios quanto o Zabbix monitorem uma elevada quantidade de máquinas, estes cenários revelaram a repetitividade dos dados monitorados em momentos aleatórios de trinta coletas cada e usando quantidade de máquinas diferente.

5.4.1 Dados coletados

Os dados obtidos das coletas contribuíram para comparar as duas ferramentas quanto à carga de tráfego gerada por ambas. Os dados foram coletados em três momentos distintos, gerando três cenários e envolvendo as ferramentas Nagios e Zabbix: Cenário 1 (4 Máquinas), Cenário 2 (6 Máquinas) e Cenário 3 (8 Máquinas), conforme descrito anteriormente.

As Figuras 12, 13 e 14 apresentam os gráficos das variáveis medidas nos três cenários do monitoramento com o Nagios e o Zabbix. Os dados foram apresentados nos gráficos em *Bytes* por minutos (Bytes/min), transformado em bytes por minuto pelo fato do tempo de captura ter sido de seis minutos.

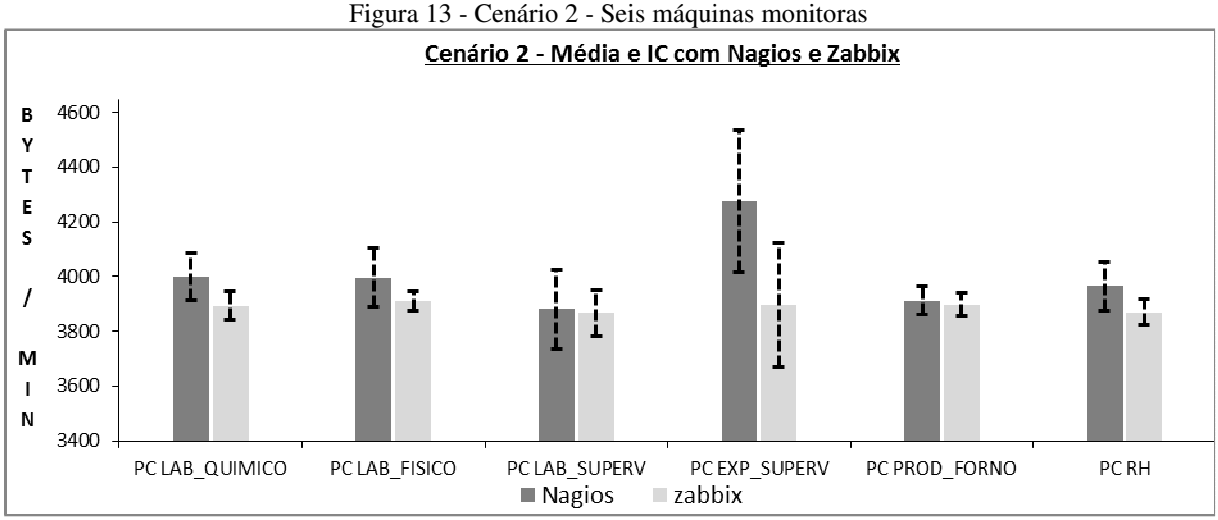
Figura 12 - Cenário 1 - Quatro máquinas monitoradas



Fonte: Autor.

A figura 12 apresenta o cenário 1. A coleta de dados foi realizada contendo quatro máquinas monitoradas na rede com as duas ferramentas. Este gráfico mostra que a média e o intervalo de confiança do tráfego em Bytes/min da ferramenta Nagios foi superior ao gerado pelo Zabbix, ou seja, o Nagios gerou um maior tráfego no processo de monitoramento.

Figura 13 - Cenário 2 - Seis máquinas monitoras

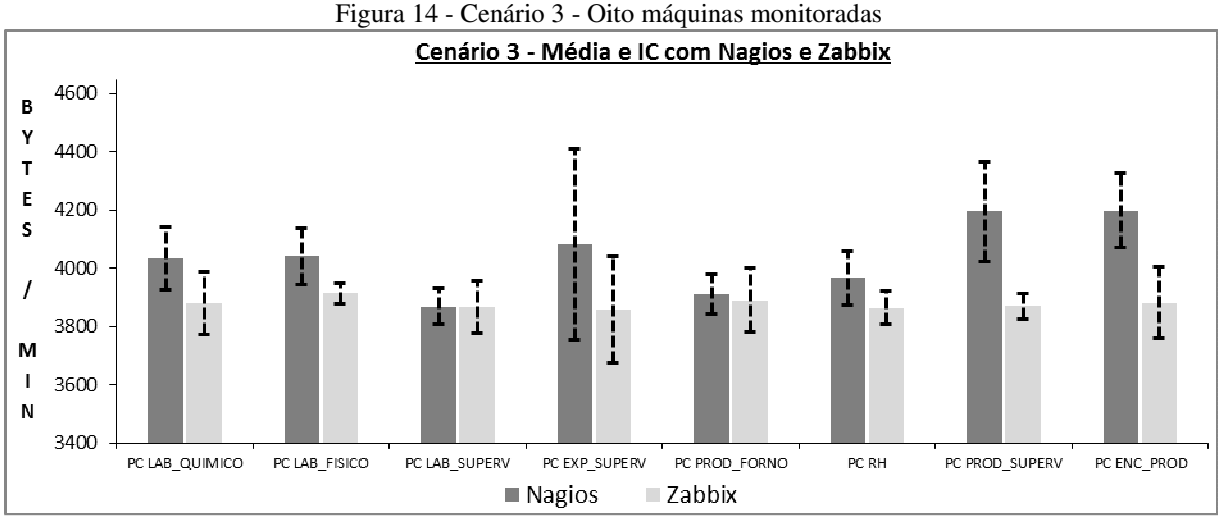


Fonte: Autor

O gráfico da figura 13, apresenta o cenário 2, que além das quatro máquinas do cenário 01, foram adicionadas mais duas máquinas, totalizando seis máquinas monitoradas pelas ferramentas. Neste cenário, houve a repetição semelhante do resultado encontrado no cenário 1. A média e o intervalo de confiança ficaram similares. Pouca oscilação ocorreu neste cenário em relação ao anterior.

Neste cenário, assim como no cenário 1, a máquina PC LAB_SUPERV, apresentou tráfego médio praticamente igual para as duas ferramentas, enquanto as demais oscilaram consideravelmente.

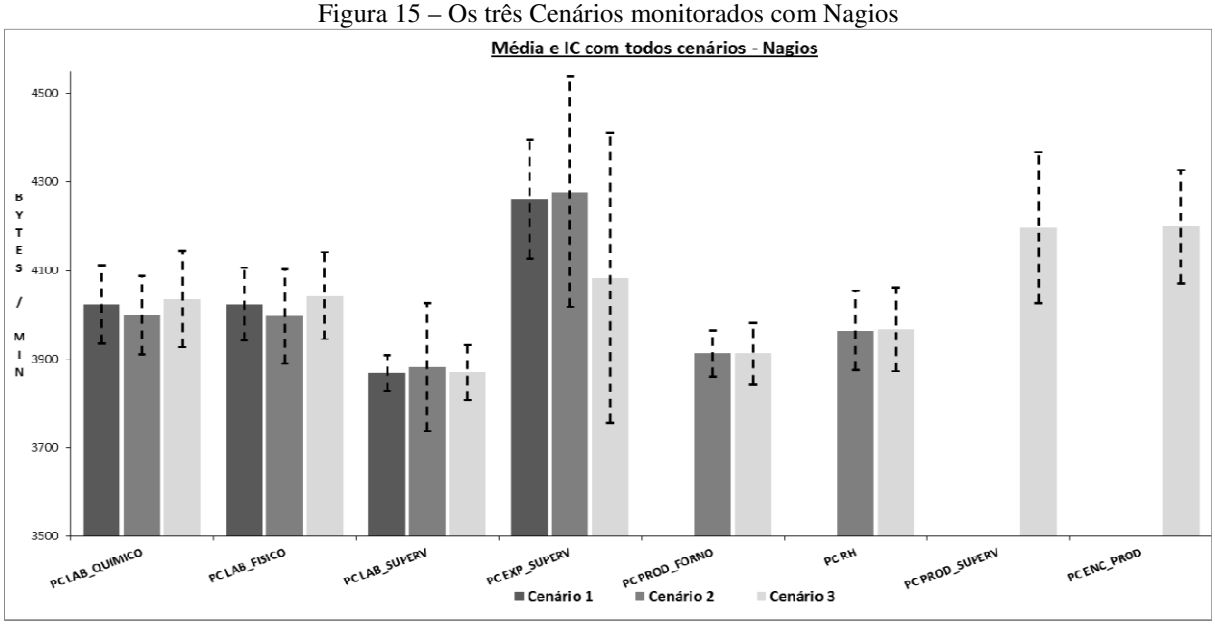
Figura 14 - Cenário 3 - Oito máquinas monitoradas



Fonte: Autor.

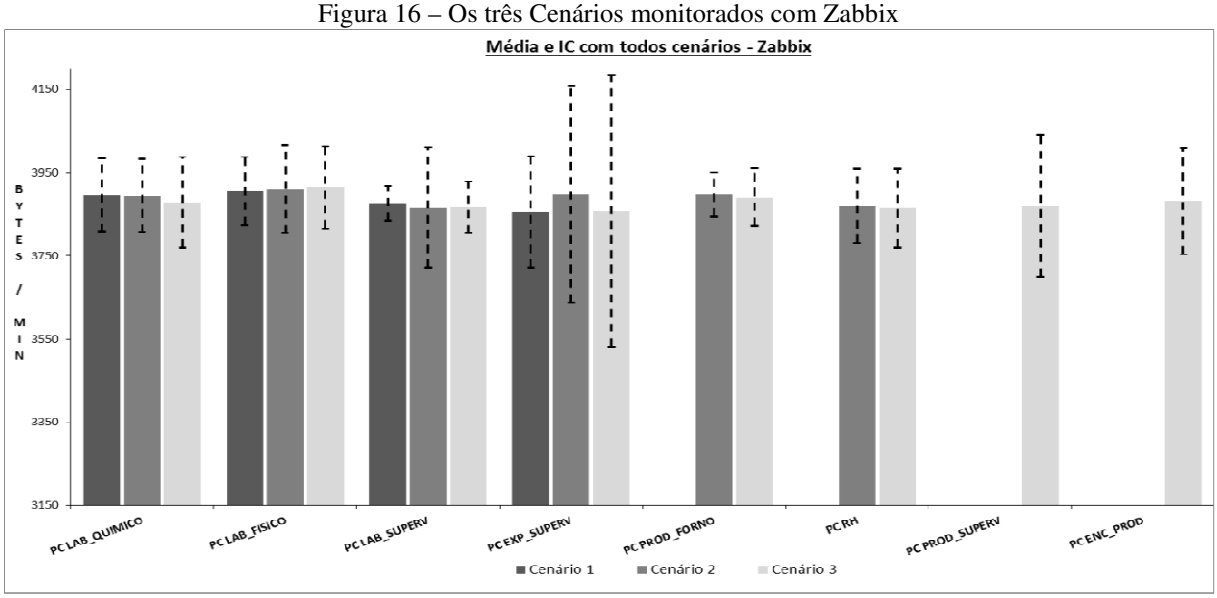
A figura 14 mostra o cenário 3 que foi adicionado mais duas máquinas as já monitoradas no cenário 2, totalizando oito máquinas monitoradas por ambas as ferramentas. Similarmente aos cenários 1 e 2, o cenário 3 também apresentou oscilação na média de tráfego e no intervalo de confiança em maior quantidade no Nagios do que em relação ao Zabbix. Neste cenário, manteve-se a repetição dos cenários anteriores, mostrando que em diferentes momentos a variação permaneceu a mesma e que o Nagios, nestes experimentos, apresentou maior tráfego no monitoramento de rede.

Figura 15 – Os três Cenários monitorados com Nagios



Fonte: Autor.

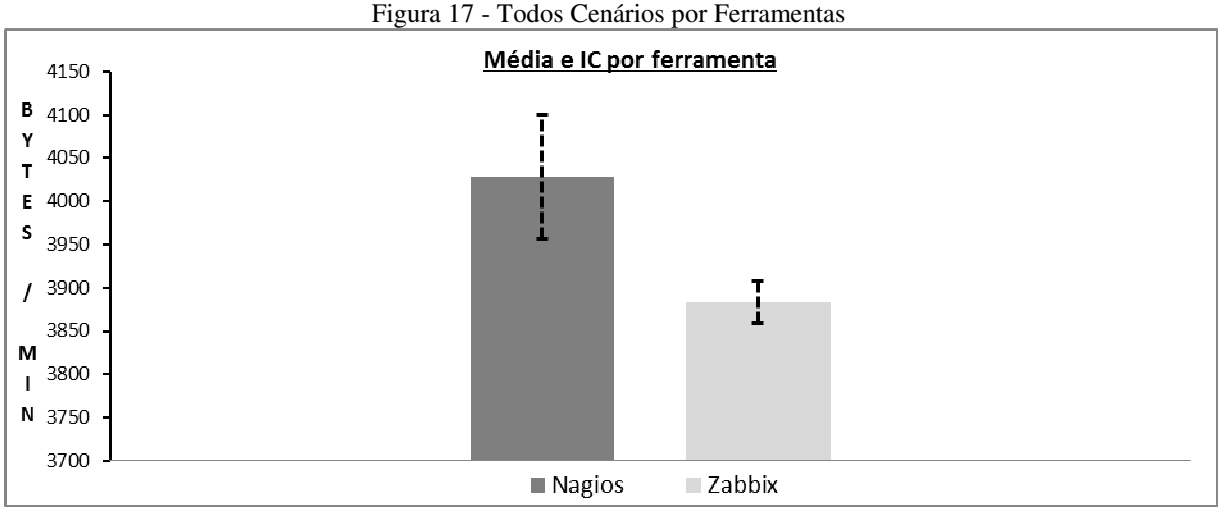
Figura 16 – Os três Cenários monitorados com Zabbix



Fonte: Autor

Apresentação dos gráficos das figuras 15 e 16 elucidaram os três cenários junto, a intenção foi facilitar a visualização dos gráficos unificados. Nestes gráficos, os cenários foram apresentados por cada máquina monitorada nos três cenários tanto pelo Nagios quanto pelo Zabbix. Notadamente, o Nagios apresentou uma maior variação na média, assim como também um maior valor médio do tráfego e intervalo de confiança em relação ao Zabbix.

Figura 17 - Todos Cenários por Ferramentas



Fonte: Autor.

O gráfico da figura 17 exibe a média e o intervalo de confiança por cada ferramenta no processo de monitoramento dos três cenários monitorados. O Nagios contribuiu com maior média e intervalo de confiança que o Zabbix, ficando claro que no monitoramento o Zabbix contribuiu com uma carga menor de tráfego na rede.

A tabela 3 expõe o comparativo entre as duas ferramentas, conforme foi objetivado neste trabalho. É apresentado um resumo da análise das duas ferramentas, levando em consideração os resultados das variáveis medidas através da coleta de dados do monitoramento das ferramentas, envolvendo os três cenários de monitoramento. A tabela contém a média do tráfego, intervalo de confiança e desvio padrão calculados através da planilha do apêndice E.

Tabela 3 - Comparativos das Ferramentas.
Fonte: Autor.

VARIÁVEIS MEDIDAS	NAGIOS	ZABBIX
Média do tráfego em Bytes por minuto (Bytes / min)	4029	3858
Intervalo de confiança	3957 a 4100	3858 a 3908
Desvio padrão	71,434	24,997

5.4.2 Nagios versus Zabbix

Na análise de tráfego, o Nagios apresentou uma média de 4029 bytes por minuto de tráfego na rede, com um desvio padrão de 71,434 e intervalo de confiança compreendido entre 3957 a 4100 bytes por minutos. Enquanto o Zabbix contribuiu com uma média de 3858 bytes por minuto de tráfego na rede, um desvio padrão de 24,997 e intervalo de confiança compreendido entre 3858 a 3908 bytes por minutos.

Do ponto de vista dos objetivos do trabalho, através do fluxo de dados que cada ferramenta faz ao enviar os pacotes de solicitação e resposta do estado das máquinas e serviços no processo de monitoração, fica evidente que o Nagios possui uma carga de tráfego maior que o Zabbix. Sendo assim, torna-se viável a utilização do Zabbix em vez do Nagios.

6 DISCUSSÃO

Este trabalho realizou uma pesquisa quantitativa, e os dados foram obtidos da avaliação do tráfego gerado na rede monitorada.

A partir dos trabalhos pesquisados, fez com que a escolha das ferramentas analisadas ficasse mais evidente. No entanto, é necessário saber que a escolha de qual ferramenta depende de cada aplicação em particular, necessitando avaliar qual poderá impactar na escolha e ainda em muitos casos é necessário um conjunto de ferramentas para obter um monitoramento mais amplo e eficaz.

As duas ferramentas ofereceram bom desempenho quanto ao monitoramento da rede. Porém o Nagios inferiorizou-se em relação ao Zabbix, principalmente em quatro pontos, levando em consideração a instalação, configuração e execução real das ferramentas:

a) Configuração dos Arquivos – Configuração das máquinas e serviços via arquivo de texto;

b) Monitoramento da rede *Windows* – Envolvimento do agente (*NSClient*);

c) Relatórios gráficos – Recursos e exposição gráfica ainda de modo escasso.

d) Tráfego – quantidade de pacotes trafegados no processo de monitoração.

O fato que limitou consideravelmente foi no monitoramento de máquinas *Windows*. O Nagios contempla enormemente o sistema *UNIX*, onde seus *plugins* são na maioria destinados ao monitoramento destes sistemas, enquanto ao sistema *Windows* deixa a desejar, pois seu agente não contempla tantos serviços de maneira simples e prática para o administrador configurar.

O Zabbix foi superior ao Nagios em sua arquitetura, principalmente no armazenamento de dados envolvendo mais de um tipo de banco de dados e a interface *web* onde é possível remotamente acessar o servidor da ferramenta. Os gráficos apresentaram de forma clara todo monitoramento realizado, contemplando as tendências dos serviços monitorados dando maior confiabilidade nas ações preventivas, detectando antes de ocorrer uma falha.

No processo de monitoramento, o tráfego gerado por cada ferramenta em cada máquina monitorada contribuiu com uma quantidade de tráfego diferente. A média de tráfego

em bytes gerados pelo Zabbix foi inferior ao Nagios em cada máquina. Assim como também menor variação representada pelo intervalo de confiança, aplicando um mesmo nível de confiança para ambas as ferramentas, determinado a partir dos dados de monitoramento por cada máquina monitorada.

7 CONSIDERAÇÕES FINAIS

A conclusão do trabalho finalizou com as metas atingidas, estabelecidas pelos objetivos, vindo ao encontro da caracterização realizada por Black (2008). O trabalho conseguiu atingir seus objetivos, onde foi dada uma atenção para a quantidade de tráfego gerado por ambas as ferramentas contribuindo para o fluxo de dados na rede.

No monitoramento realizado pelas duas ferramentas, o Nagios apresentou um grau de dificuldade pelo número de serviços monitorados através do agente *NSClient*, além de exigir um nível de conhecimento mais evoluído na configuração dos arquivos de texto.

A análise gráfica realizada mostrou que ambas as ferramentas dispõem destes recursos, porém, o Zabbix contempla uma variedade maior de recursos capazes de fornecer dados para tomada de ações preventivas, o que facilita a administração da rede, minimizando eventuais custos indesejáveis.

Contudo, os dados fornecidos pela análise, mostrou que torna mais viável o monitoramento pela ferramenta Zabbix em vez de utilizar o Nagios pela variação do fluxo de dados na rede. Partindo deste ponto, este trabalho dá subsídio para os administradores na escolha dentre o nagios e o Zabbix para monitoramento de rede.

Para a realização deste trabalho foi necessário um empenho de vínculo prático, onde envolveu a necessidade do conhecimento de gerência de redes, ferramentas de gerenciamento, desde instalação e configuração, virtualização de sistemas operacionais e configuração dos ativos de rede e serviços monitorados pelas ferramentas de gerenciamento e monitoramento. Todo este estudo deu-me grande contribuição no campo do conhecimento. A visão de gerenciamento adquirida a partir deste trabalho possibilitou-me olhar com outra direção. Foi uma contribuição recompensável pelo esforço despendido.

REFERÊNCIAS

BALSEMÃO, Fábio Torres. Gerência e Monitoramento de Redes Através de Dispositivos Móveis. Trabalho de Especialização. **Universidade Federal do Rio Grande Do Sul – Instituto de Informática.** Porto Alegre. 2008.

BEZELLI, M. A.; ROSSETE L. R. Monitoramento e Gerenciamento de Redes Computacionais utilizando o Software Livre Nagios. **Departamento de Comutação – Universidade Federal de São Carlos.** São Carlos. v. 2, n. 2, p. 89-96, mai-ago 2013.

BITTENCORT, B. J; OE, R. H; SANTANNA, J. GERÊNCIA E MONITORAMENTO DE REDES DE COMPUTADORES COM O SOFTWARE LIVRE NAGIOS. **Engenharia de Computação em Revista**, v. 1, n. 1, 2010.

BLACK, T. L, **Comparação de Ferramenta de Gerenciamento de Redes.** Monografia (Especialização em Tecnologia, Gerência e Segurança de Redes de Computadores). Universidade Federal do Rio Grande do Sul. Porto Alegre, 2008.

CARVALHO, M. B. **Adaptação da Ferramenta Nagios para o Monitoramento de Servidores Virtuais.** Trabalho de Graduação. Universidade Federal do Rio Grande do Sul – Instituto de Informática. Porto Alegre 2010.

CISCO. **Análise de tráfego.** 04 abr. 2015. Disponível em: <http://www.cisco.com/cisco/web/support/BR/9/91/91508_tech_tk652_tk701_tech_white_paper09186a00800d6b74.html>. Acesso em: 08 abr. 2015.

FARRUCA, N. M. G. **Wireshark para sistemas distribuídos**. 2009. Disponível em: < http://run.unl.pt/bitstream/10362/2288/1/Farruca_2009.pdf>. Acesso em: 08 mai. 2015.

FRANCA, B. W.F., JUNIOR, E. J. S., BRITO, R. F. **Análise de Tráfego e Simulação de Redes Multicast**. Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

Kamienski, C., Souza, T., Fernandes, S., Silvestre, G., & Sadok, D. (2005). Caracterizando propriedades essenciais do tráfego de redes através de técnicas de amostragem estratificada. SBRC. Disponível: <http://www.cin.ufpe.br/~cak/publications/sbrc2005_amostragem_estratificada_final.pdf.> Acesso: 03/01/2016.

KOCH, M. **Uma Proposta de Gerenciamento de Contabilização utilizando Nagios e Cacti.** Instituto de Informática. Universidade Federal do Rio Grande do Sul. Porto Alegre, 2008.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet**. 5.ed. São Paulo: Pearson 2010.

LIMA, Janssen dos Reis. **Monitoramento de Redes com ZABBIX.** 1.ed. Rio de Janeiro: Brasport, 2014. 192p.

MAGNANI, T. D, **Estudos de Monitoramento de Redes: Nagios.** Monografia (Título de Tecnólogo em Processamento de Dados). Faculdade de Tecnologia de Taquaritinga – Centro Paula Souza. Taquaritinga, 2009.

MOURA, D. M.; BECKER, P. C. **Utilização da Ferramenta Nágios para monitoramento de Sinal de Antena de Rede Wireless.** III Simpósio de Tecnologia da Informação da Região Nordeste do Rio Grande do Sul (STIN). Disponível em: < http://sites.setrem.com.br/stin/2012/anais/Pedro.pdf >. Acessado em: 07 de Mai. 2015.

NETO, A. F.; UCHÔA, J. Q. Ferramentas Livres para Monitoração de Servidores. Fisl7.0. **Centro de Pesquisa e Desenvolvimento em Engenharia Elétrica - (UFMG)**. Belo Horizonte, Minas Gerais. 2015. Disponível em: <http://repositorio.ufla.br/handle/1/9641>. Acesso em: 02/05/2015.

SANTOS, C. C. **Gerenciamento de Redes com a utilização de Software Livre.** Instituto de Estudos Superiores da Amazônia. Belém, 2010.

SANTOS, C. J. M. **Sistema de Monitoramento para Redes Sem Fio**. Monografia (Especialização em Teleinformática e Redes de Computadores). Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

STHALSCHMIDT T. **Controle de admissão de Conexão para servidores de Vídeo sob demanda utilizando a Teoria assintótica de muitas Fontes**. Dissertação (Pós-Graduação em Engenharia Elétrica e Informática Industrial como requisito parcial para obtenção do Grau de Mestre em Ciências.). Universidade Tecnológica Federal do Paraná. Curitiba, 2010.

W. Prado, L. Mundim, J. U. Cinelli, J. R. Mahon, A. Santoro e U. Oguri. **Tratamento de dados e análise de Erros.** Física Experimental I. Texto adaptado em: IF UFRJ.

APÊNDICES

APÊNDICE A – Planilha de Coletas de Dados Cenário 1

COLETA DE DADOS - CENÁRIO 01									
ID PACOTES	HORA	NAGIOS				ZABBIX			
		PC LAB_QUIMICO	PC LAB_FISICO	PC LAB_SUPERV	PC EXP_SUPERV	PC LAB_QUIMICO	PC LAB_FISICO	PC LAB_SUPERV	PC EXP_SUPERV
85-271015	16:44	3924	4000	3868	4176	3896	3900	3872	3871
01-091215	08:35	4035	4000	3868	4176	3896	3900	3872	3713
02-091215	09:23	3980	4002	3869	4145	3896	3902	3894	3871
03-091215	09:50	4024	4035	3870	4254	3896	3902	3895	3871
04-091215	10:16	4046	4057	3870	4265	3896	3902	3873	3872
05-091215	10:29	4057	4046	3772	4254	3896	3795	3873	3872
06-091215	10:41	4013	3914	3870	4266	3896	3902	3917	3872
07-091215	10:55	3991	3969	3881	4265	3896	3902	3895	3872
109-150116	08:11	4034	4045	3879	4253	3896	3901	3872	3871
110-150116	08:18	4111	4034	3868	4276	3896	3901	3894	3897
111-150116	08:25	4045	4067	3868	4328	3896	3901	3872	3823
112-150116	09:01	4045	4067	3868	4328	3896	3901	3872	3823
113-150116	09:09	4023	4056	3868	4323	3896	3901	3872	3871
114-150116	09:19	4012	4067	3868	4047	3896	3901	3872	3547
115-150116	09:26	4045	4056	3868	4291	3896	3901	3894	3899
116-150116	09:35	3946	4012	3868	4294	3896	3901	3894	3871
117-150116	09:42	4036	4045	3897	4244	3896	3945	3873	3983
118-150116	10:02	4036	4045	3881	4244	3896	3945	3873	3883
119-150116	10:19	3958	3990	3869	4339	3896	3923	3873	3883
120-150116	10:35	4090	4012	3869	4269	3896	3923	3873	3899
121-150116	10:42	4057	4100	3869	4291	3896	3901	3873	3860
122-150116	10:51	4068	4045	3869	4265	3896	3901	3895	3872
123-150116	11:01	4057	3979	3869	4243	3896	3923	3778	3872
124-150116	11:07	4024	3990	3869	4266	3896	3941	3873	3884
125-150116	11:14	4024	4023	3869	4292	3896	3945	3873	3872
126-150116	11:20	4013	4045	3869	4375	3896	3923	3873	3872
127-150116	11:27	4046	4001	3869	4277	3896	3901	3873	3872
128-150116	13:08	3947	3979	3869	4305	3896	3901	3873	3763
129-150116	13:16	4024	4034	3869	4232	3896	3901	3873	3872
130-150116	13:27	4024	3990	3870	4265	3896	3901	3873	3872

APÊNDICE B – Planilha de Coletas de Dados Cenário 2

COLETA DE DADOS - CENÁRIO 02													
		NAGIOS						ZABBIX					
ID PACOTES	HORA	PC_LAB_QUIMICO	PC_LAB_FISICO	PC_LAB_SUPERV	PC_EXP_SUPERV	PC_PROD_FORNO	PC_RH	PC_LAB_QUIMICO	PC_LAB_FISICO	PC_LAB_SUPERV	PC_EXP_SUPERV	PC_PROD_FORNO	PC_RH
78-140116	11:00	4012	4102	3870	4254	3945	3967	3896	3925	3873	3872	3902	3873
79-140116	11:08	4045	4047	3870	4265	3926	3968	3896	3903	3895	3872	3902	3873
80-140116	11:15	4023	3891	4203	4290	3904	3990	3896	3903	3895	3872	3902	3873
81-140116	11:27	4023	4080	3870	4145	3904	3979	3788	3903	3873	3765	3902	3873
82-140116	12:58	4056	4025	3914	4261	3926	3958	3896	3903	3768	3922	3902	3873
83-140116	13:06	4045	4027	3870	4191	3937	3967	3896	3903	3895	3932	3794	3873
84-140116	13:15	4056	3981	3870	4352	3915	4001	3896	3903	3873	3731	3902	3873
85-140116	13:25	3990	3992	3870	4363	3904	3935	3896	3903	3873	4040	3902	3873
86-140116	13:29	4056	3992	3869	4563	3937	3924	3896	3903	3789	3902	3902	3872
87-140116	13:35	3990	3944	3870	4196	3893	3946	3896	3903	3873	3886	3902	3872
88-140116	13:43	3968	4036	3869	4326	3926	3957	3896	3925	3764	4258	3902	3872
89-140116	13:50	4001	4014	3869	4271	3915	4005	3896	3903	3873	4019	3902	3902
90-140116	13:57	4012	3992	3869	4402	3926	3935	3896	3903	3873	3760	3902	3872
91-140116	14:04	4012	3981	3869	4274	3893	3968	3963	3903	3873	3922	3902	3872
92-140116	14:20	3979	4069	3869	4320	3893	4098	3889	3947	3873	3927	3902	3873
93-140116	14:27	3968	4025	3869	4574	3937	4076	3896	3903	3903	3951	3902	3873
94-140116	14:33	3968	3948	3870	4106	3926	3957	3896	3925	3873	3958	3902	3756
95-140116	14:45	4001	3959	3870	4531	3926	3946	3896	3903	3895	4053	3902	3873
96-140116	14:55	3946	3992	3869	4254	3893	3946	3896	3925	3895	3872	3902	3873
97-140116	15:04	3985	3992	3974	4031	3807	3946	3896	3925	3873	3872	3902	3872
98-140116	15:12	4034	4036	3870	4260	3915	3957	3896	3925	3895	3872	3902	3872
99-140116	15:15	3996	3970	3869	4254	3904	3979	3896	3903	3873	3702	3902	3873
100-140116	15:29	3957	4036	3869	4143	3915	3990	3896	3903	3895	3898	3902	3872
101-140116	15:46	3946	3959	3869	4254	3926	3957	3896	3936	3873	3872	3902	3872
102-140116	15:54	4001	4003	3869	4266	3926	3924	3896	3903	3873	3897	3902	3873
103-140116	16:02	3870	3981	3761	4156	3904	3924	3896	3903	3873	3765	3902	3872
104-140116	16:10	4067	3981	3870	4265	3915	3935	3889	3925	3766	3872	3902	3872
105-140116	16:17	4001	3970	3869	4243	3915	3924	3896	3925	3895	3912	3902	3873
106-140116	16:27	4001	3873	3869	4254	3904	3902	3896	3925	3873	3872	3902	3873
107-140116	16:34	3979	4014	3869	4265	3926	3979	3896	3853	3873	3872	3902	3873

APÊNDICE C – Planilha de Coletas de Dados Cenário 3

COLETA DE DADOS - CENÁRIO 03																		
		NAGIOS								ZABBIX								
ID PACOTES	HORA	PC_LAB_QUIMICO	PC_LAB_FISICO	PC_LAB_SUPERV	PC_EXP_SUPERV	PC_PROD_FORNO	PC_RH	PC_PROD_SUPERV	PC_ENC_PROD	PC_LAB_QUIMICO	PC_LAB_FISICO	PC_LAB_SUPERV	PC_EXP_SUPERV	PC_PROD_FORNO	PC_RH	PC_PROD_SUPERV	PC_ENC_PROD
48-130116	14:16	3996	3942	3981	4254	3806	3870	4210	4115	3896	3925	3764	3872	3902	3873	3874	3872
49-130116	14:34	4046	4047	3870	4328	3948	4011	4221	4232	3896	3903	3873	3567	3902	3873	3874	3872
50-130116	14:41	4002	4036	3869	4265	3904	3913	4244	4255	3896	3903	3873	3884	3902	3873	3874	3872
51-130116	14:50	4012	4003	3869	4265	3904	3989	4274	4233	3896	3903	3917	3872	3902	3873	3874	3872
52-130116	14:57	4056	4025	3869	4292	3926	3990	4189	4254	3955	3925	3873	3775	3902	3873	3874	3872
53-130116	15:04	4046	4047	3869	4353	3904	3979	4254	4222	3896	3925	3873	3872	3902	3873	3874	3872
54-130116	15:30	4035	4058	3870	4277	3937	3886	4209	4243	3896	3903	3873	3940	3914	3777	3887	3883
55-130116	15:42	4090	3981	3870	4302	3904	3933	4254	4266	3918	3903	3873	3897	3902	3870	3874	3872
56-130116	15:52	4024	4047	3869	4265	3904	3978	4254	4233	3896	3903	3873	4032	3902	3871	3765	3872
57-130116	16:02	4002	3992	3869	4254	3904	4011	4189	4222	3896	3925	3917	3872	3902	3871	3874	3872
58-130116	16:08	4046	3981	3870	4137	3828	3934	3958	4123	3786	3903	3895	4032	3794	3764	3874	3872
59-130116	16:25	4112	4091	3869	3956	3904	3956	4249	4277	3896	3947	3873	3765	3902	3871	3874	3872
60-130116	16:32	4112	4003	3869	3978	3948	3978	4222	4244	3788	3903	3873	3763	3902	3871	3874	3872
61-130116	16:41	4123	4102	3869	3967	3904	3967	4374	4266	3788	3925	3873	3828	3902	3871	3874	3883
62-130116	16:48	4035	4102	3869	3934	3915	3934	4295	4255	3896	3925	3873	3929	3902	3871	3874	3872
63-130116	16:54	4079	4047	3762	3956	3926	3956	4265	4244	3896	3903	3788	3872	3902	3871	3874	3872
64-130116	17:01	4134	4102	3869	3945	3915	3945	4275	4266	3918	3903	3873	3872	3902	3871	3874	3872
65-130116	08:24	4057	4124	3870	4076	3948	4076	4198	4198	3918	3903	3873	3871	3902	3873	3874	3871
66-140116	08:33	4034	4058	3868	3956	3959	3956	4189	4209	3896	3969	3763	3871	3902	3872	3874	3871
67-140116	08:41	4023	4025	3868	3978	3904	3978	4222	4199	3896	3903	3872	3871	4009	3872	3874	3871
68-140116	08:48	3979	4014	3869	3956	3904	3956	4166	4188	3896	3903	3766	3871	3902	3872	3874	3871
69-140116	09:04	4045	4047	3869	4011	3937	4011	4123	4133	3789	3903	3916	3871	3792	3872	3874	3871
70-140116	09:16	4023	4003	3869	4000	3915	4000	4100	4111	3896	3925	3872	3871	3902	3872	3874	3871
71-140116	09:31	3979	4102	3869	3912	3915	3912	4101	4177	3896	3903	3894	3871	3902	3872	3874	3871
72-140116	09:38	4001	4091	3869	3999	3937	3999	4133	4144	3896	3903	3894	3764	3902	3872	3874	3871
73-140116	09:44	4067	4102	3869	3968	3904	3968	4123	4133	3896	3925	3894	3871	3902	3873	3874	3871
74-140116	09:52	4045	4036	3869	4023	3904	4023	4124	4046	3896	3925	3872	3762	3902	3873	3874	3871
75-140116	10:07	3979	3981	3869	3912	3959	3912	4177	4203	3729	3925	3872	3871	3698	3872	3874	4186
76-140116	10:15	3893	4058	3870	4011	3915	4011	4175	4133	3896	3925	3895	3871	3902	3873	3874	3871
77-140116	10:22	3990	4025	3870	3979	3893	3979	4101	4144	3896	3903	3873	3872	3902	3873	3874	3871

APÊNDICE D – Cálculo da média, desvio padrão e intervalo de confiança

Cenário 3	PC LAB_QUIMICO	PC LAB_FISICO	PC LAB_SUPERV	PC EXP_SUPERV	PC PROD_FORNO	PC RH	PC PROD_SUPERV	PC ENC_PROD	PC LAB_QUIMICO	PC LAB_FISICO	PC LAB_SUPERV	PC EXP_SUPERV	PC PROD_FORNO	PC RH	PC PROD_SUPERV	PC ENC_PROD
Número de Amostra	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
Desvio Padrão	303,605	273,624	172,847	915,041	192,672	263,330	474,984	357,875	298,614	96,399	248,377	505,785	302,509	155,270	120,792	344,409
Nível de Confiança	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%
Margem de Erro	108,642	97,913	61,851	327,437	68,946	94,230	169,968	128,062	106,856	34,495	88,879	180,989	108,250	55,562	43,224	123,243
Limite inferior	3927	3944	3807	3756	3844	3873	4026	4071	3773	3880	3778	3677	3784	3810	3828	3760
Média	4036	4042	3869	4084	3913	3967	4196	4199	3880	3915	3867	3858	3892	3865	3871	3883
Limite Superior	4144	4140	3931	4411	3981	4061	4366	4327	3987	3949	3956	4039	4000	3921	3914	4006

Cenário 2	PC LAB_QUIMICO	PC LAB_FISICO	PC LAB_SUPERV	PC EXP_SUPERV	PC PROD_FORNO	PC RH	_	_	PC LAB_QUIMICO	PC LAB_FISICO	PC LAB_SUPERV	PC EXP_SUPERV	PC PROD_FORNO	PC RH	_	_
Número de Amostra	30	30	30	30	30	30			30	30	30	30	30	30		
Desvio Padrão	248,004	296,130	404,083	727,223	147,870	249,124			141,052	100,617	236,254	636,363	118,125	133,322		
Nível de Confiança	95%	95%	95%	95%	95%	95%			95%	95%	95%	95%	95%	95%		
Margem de Erro	88,746	105,967	144,596	260,229	52,914	89,146			50,474	36,005	84,541	227,715	42,270	47,708		
Limite inferior	3911	3891	3737	4017	3860	3876			3844	3875	3782	3670	3856	3822		
Média	4000	3997	3882	4278	3913	3965			3894	3911	3866	3897	3898	3870		
Limite Superior	4088	4103	4027	4538	3966	4054			3945	3947	3951	4125	3941	3917		

Cenário 1	PC LAB_QUIMICO	PC LAB_FISICO	PC LAB_SUPERV	PC EXP_SUPERV	_	_	_	_	PC LAB_QUIMICO	PC LAB_FISICO	PC LAB_SUPERV	PC EXP_SUPERV	_	_	_	_
Número de Amostra	30	30	30	30					30	30	30	30				
Desvio Padrão	248,335	229,853	114,446	376,149					0,183	156,347	131,034	437,985				
Nível de Confiança	95%	95%	95%	95%					95%	95%	95%	95%				
Margem de Erro	88,864	82,250	40,953	134,601					0,065	55,947	46,889	156,728				
Limite inferior	3936	3941	3827	4127					3896	3850	3829	3699				
Média	4024	4024	3868	4261					3896	3906	3876	3856				
Limite Superior	4113	4106	3909	4396					3896	3962	3923	4013				

APÊNDICE E – Cálculo global da média, desvio padrão e intervalo de confiança

ATRIBUTOS DAS FERRAMENTAS	NAGIOS	ZABBIX
Número de Amostra	540	540
Desvio Padrão	846,938	296,370
Nível de Confiança	95%	95%
Margem de Erro	71,4337	24,9968
Limite inferior	3957	3858
Média	4029	3883
Limite Superior	4100	3908