

INSTITUTO FEDERAL DE MINAS GERAIS

CAMPUS SÃO JOÃO EVANGELISTA

ALINE PEREIRA CAMELO, JULIANA CÂNDIDO MARIA

**ANÁLISE COMPARATIVA DE FERRAMENTAS DE MONITORAMENTO DE
EQUIPAMENTOS PARA PROPOSTA DE IMPLANTAÇÃO NO DEPARTAMENTO
DE TI DO IFMG-CAMPUS SÃO JOÃO EVANGELISTA**

**SÃO JOÃO EVANGELISTA
2016**

ALINE PEREIRA CAMELO, JULIANA CÂNDIDO MARIA

**ANÁLISE COMPARATIVA DE FERRAMENTAS DE MONITORAMENTO DE
EQUIPAMENTOS PARA PROPOSTA DE IMPLANTAÇÃO NO DEPARTAMENTO
DE TI DO IFMG-CAMPUS SÃO JOÃO EVANGELISTA**

Trabalho de conclusão de curso apresentado ao Instituto Federal de Minas Gerais – Campus São João Evangelista como exigência parcial para obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Prof^o: Fernando Henriques Mafra
Coorientador: Daniel dos Santos Amaral
Prof^o Convidado: Dayler Alves

**SÃO JOÃO EVANGELISTA
2016**

Aline Pereira Camelo, Juliana Cândido Maria

ANÁLISE COMPARATIVA DE FERRAMENTAS DE MONITORAMENTO DE EQUIPAMENTOS PARA PROPOSTA DE IMPLANTAÇÃO NO DEPARTAMENTO DE TI DO IFMG-CAMPUS SÃO JOÃO EVANGELISTA

Trabalho de conclusão de curso apresentado ao Instituto Federal de Minas Gerais – Campus São João Evangelista como exigência parcial para obtenção do título de Bacharel em Sistemas de Informação.

Aprovada em..... / /

BANCA EXAMINADORA

Orientador

Prof. Esp. Fernando Henriques Mafra

Coorientador

Prof. Me. Daniel dos Santos Amaral

Convidado

Prof. Esp. Dayler Vinicius Miranda Alves

Sumário

1. INTRODUÇÃO.....	6
1.1 JUSTIFICATIVA	7
1.2 OBJETIVO GERAL.....	7
1.3 OBJETIVO ESPECÍFICO	7
1.4 ORGANIZAÇÃO DO TRABALHO	8
2 REFERENCIAL TEÓRICO.....	8
2.1 MONITORAMENTO.....	8
2.2 GERENCIAMENTO	10
2.2.1 ÁREAS FUNCIONAIS DE GERÊNCIA DE REDES.....	12
2.2.2 PROTOCOLOS DE GERENCIAMENTO	12
2.2.2.1 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)	13
2.2.2.2 CAMMON MANAGEMENT INFORMATION PROTOCOL (CMIP)	13
3 METODOLOGIA	14
3.1 NAGIOS.....	15
3.2 ZABBIX	16
3.3 CACTI.....	19
3.4 MULTI ROUTER TRAFFIC GRAPHER (MRTG).....	21
3.5 COMPARATIVO DAS FERRAMENTAS ESTUDADAS COM FCAPS	23
3.5.1 NAGIOS.....	23
3.5.2 ZABBIX	24
3.5.3 CACTI.....	25
3.5.4 MULTI ROUTER TRAFFIC GRAPHER (MRTG).....	25
4 RESULTADOS E DISCUSSÕES	27
5 CONSIDERAÇÕES FINAIS	29
6 TRABALHOS FUTUROS.....	30
APÊNDICE A- ENTREVISTA COM COORDENADOR DE TI	31
REFERÊNCIAS.....	32

LISTA DE SIGLAS

ASCE- Association Control Service Element

CMIP- Common Management Information Protocol

FCAPS- Fault, Configuration, Accounting, Performance and Security

GD- Graphics Library

GIF- Graphics Interchange Format

GNU- General Public License

HTML- Hiper Text Markup Language

IETF- Internet Engineering Task Force

IFMG-SJE- Instituto Federal de Minas Gerais Campus São João Evangelista

ISO- International Organization for Standardization

MRTG- Multi Router Traffic Grapher

PNG- Portable Network Graphics

ROSE- Remote Operations Service Element

RRDTool – Round Robin Database Tool

SNMP- Simple Network Management Protocol

TCP/IP- Transmission Control Protocol/Internet Protocol

TI- Tecnologia da Informação

RESUMO

A internet na atualidade se tornou de grande importância para empresas e ambientes escolares. Isso acontece porque, os funcionários conseguem desempenhar melhor seus papéis, de forma rápida e prática. Porém, para que tudo isso possa acontecer é necessário obter uma rede de qualidade, sendo gerenciada no intuito de saber quais são os problemas ocorridos e quais ocorrerão.

Em decorrência do significativo aumento do uso das redes de computadores, monitorá-las tornou-se uma tarefa desafiadora, porém essencial. Ter um ambiente monitorado é de grande importância. Para empresas, o monitoramento e gerenciamento, são capazes de proporcionar o crescimento. Para instituições de ensino, podem oferecer mais agilidade nos processos. Qualquer ambiente necessita ser monitorado, pois, o mesmo relata sobre os problemas que estão acontecendo ou que irão acontecer. O que faz com que grandes transtornos sejam evitados.

Este estudo tem como objetivo abranger o monitoramento de redes de computadores. Foi realizado um estudo de quatro ferramentas que possuem esta função. As ferramentas escolhidas estão entre as mais populares do mercado, sendo elas: Nagios, Zabbix, Cacti e MRTG. Ao final do estudo foi possível conhecer as particularidades de cada ferramenta e assim solucionar e concluir os objetivos, tanto gerais, quanto específicos desse trabalho.

Palavras-Chave: Monitoramento, Gerenciamento, Nagios, Cacti, Zabbix, MRTG.

ABSTRACT

The internet nowadays has become very important for companies and school environments. This happens because employees can better perform their roles in a fast and practical way. However, for all this to happen, it is necessary to obtain a quality network being managed in order to know what problems occurred and what will occur.

Due to the significant increase in the use of computer networks, monitor them has become a challenging task, but essential. Having a monitored environment is of great importance. For companies, monitoring and management are able to provide growth. For educational institutions, they can provide more agility in the processes. Any environment needs to be monitored because the monitoring reports about the problems that are happening or will happen. What causes major disruptions be avoided.

This study aimed to cover the monitoring of computer networks. There was a study of four tools that have these functions. The chosen tools are among the most popular on the market, being them: Nagios, Zabbix, Cacti and MRTG. At the end of the study will be possible to know the peculiarities of each tool and thus solve and complete goals, both general, as specific to this study.

Keywords: Monitoring, Management, Nagios, Cacti, Zabbix, MRTG.

1. INTRODUÇÃO

O uso dos computadores dentro das corporações tem simplificado os trabalhos, melhorando a comunicação e a rapidez na troca de informações. “Nas organizações um percentual considerável de atividades é executado direta ou indiretamente por algum tipo de serviço provido pela rede de computadores” (Albuquerque, 2001). As instituições de ensino também se tornaram dependentes dos serviços de rede, no intuito de fornecer as informações necessárias no tempo certo com maior facilidade e praticidade.

Em consequência do aumento expressivo na utilização das redes de computadores, é necessário o uso de recursos para monitorar todo o tráfego de informações. A palavra monitorar é o mesmo que monitorizar, ou seja, acompanhar por meio de monitor, fazer vigilância e acompanhamento. “Monitorar uma rede é verificar a eficácia do funcionamento de cada serviço, equipamento e processo existente em uma mesma infraestrutura seja ela empresarial ou residencial” (Neto, *et.al*, 2014). Monitorar uma rede de computadores é uma atividade muito séria, a função dos equipamentos de rede é crucial para que outros componentes funcionem acertadamente. Junior, 2012, afirma que um sistema apto a monitorar equipamentos e informar qualquer desvio dos parâmetros pré-estabelecidos pode ter grande importância no auxílio à identificação de problemas, propiciando rápida atuação e, conseqüentemente, a diminuição no tempo de indisponibilidade do sistema. Com o monitoramento é possível detectar os problemas o mais rápido possível e possibilita também que melhor visualização do desempenho dos equipamentos presentes em rede.

“O gerenciamento e monitoração de rede são atividades importantes para a boa operacionalidade de uma rede” (Leite, 2004). O gerenciamento é uma atividade na qual faz o controle e o monitoramento dos equipamentos presentes na rede (Pinheiro, 2002). De acordo com Albuquerque, 2001, a gerência deve manter a rede operacional e aperfeiçoar o seu desempenho, com o monitoramento isso se torna possível e menos trabalhoso, já que os administradores terão informações exatas sobre o estado atual da rede.

Obter informações da rede, examiná-las para detectar eventuais problemas e encaminhar as soluções desses problemas são encargos primordiais da gerência de redes. Uma rede que não dispõe de algum método de gerenciamento ficará exposta, sujeita a congestionamentos no tráfego de dados, problemas com segurança, recursos sobrecarregados, entre outros. De acordo com Stallings (1998), o gerenciamento e monitoração de redes são tarefas extremamente importantes para a saúde de uma rede de computadores, sendo que, sem

operações de gerenciamento, uma rede local não tem como manter-se operacional por muito tempo.

Em instituições de ensino, gerenciar e controlar todos os equipamentos da rede é algo difícil de ser realizado. No entanto, o mercado tem apresentado ferramentas cada vez mais eficientes, capazes de auxiliar na manutenção e controle desses dispositivos. As mesmas possuem capacidade de identificar a ocorrência de falhas nas unidades que estão sendo gerenciadas permitindo que se faça correção em tempo viável, sem que os dados sejam comprometidos. A possibilidade de prever, detectar e reagir a eventuais problemas fundamenta a importância do uso das ferramentas de gerenciamento e monitoramento de redes. Frente à necessidade de garantir sua integridade, e assegurar que tudo funcione de forma correta, sem que imprevistos interfiram no seu funcionamento.

O Instituto Federal Minas Gerais campus São João Evangelista (IFMG-SJE) não possui nenhuma ferramenta de monitoramento implantada, portanto notou-se a importância de se obter um software deste tipo a fim de assegurar a recuperação de problemas de forma menos trabalhosa. Problemas estes relatados pelo coordenador de Tecnologia da Informação (TI) do IFMG-SJE.

Notando a relevância de se obter um monitoramento de equipamentos, este trabalho vem com uma possível proposta de implantar uma ferramenta que faça a verificação e a notificação de possíveis problemas.

1.1 JUSTIFICATIVA

Durante o período de estágio realizado no setor de coordenação de TI do IFMG –SJE foi possível constatar que a instituição tem enfrentado algumas dificuldades para monitorar os equipamentos presentes em sua rede. Sua infraestrutura conta com um grande número de aparelhos distribuídos entre os ambientes de seus diversos setores. Todavia, o administrador não faz uso de nenhuma ferramenta de monitoramento, o que torna o trabalho complexo e enfadonho. Com o intuito de solucionar esse impasse, surgiu a proposta de implantação de um sistema de monitoramento e gerenciamento de redes.

1.2 OBJETIVO GERAL

Realizar um estudo de alguns softwares de monitoramento livres, visando identificar qual a melhor ferramenta, de acordo com as necessidades da instituição, e propor a implantação.

1.3 OBJETIVO ESPECÍFICO

- Realizar estudo sobre a definição de monitoramento e gerenciamento.
- Realizar estudos sobre algumas ferramentas de monitoramento gratuitas mais renomadas no mercado, com base em outros trabalhos de conclusão de curso que tiveram objetivos semelhantes aos nossos.
- Fazer um comparativo teórico para buscar identificar qual a melhor ferramenta para a instituição, em conformidade com os requisitos propostos pelo coordenador de TI, tendo como base também, outras monografias que tiveram objetivos semelhantes aos nossos.

1.4 ORGANIZAÇÃO DO TRABALHO

O presente estudo está dividido do seguinte modo: O capítulo 2 é composto pelo referencial teórico, onde se aborda o conceito de monitoramento e gerenciamento de redes, e sua relevância para o bom funcionamento de uma rede de computadores. São abordados também os protocolos de redes, com ênfase nos protocolos SNMP e CMIP. O capítulo 3 é constituído pela metodologia, onde é elaborado o estudo sobre as características de quatro ferramentas de monitoramento e gerenciamento de redes, sendo elas Nagios, Zabbix, Cacti e MRTG. No capítulo 5, serão apresentadas as conclusões obtidas, no capítulo 6 trabalhos futuros, e por fim, as referências às quais contribuíram para elaboração desse estudo.

2 REFERENCIAL TEÓRICO

O Este capítulo irá abordar sobre o monitoramento e gerenciamento de redes e suas significâncias. Primeiro será tratado o monitoramento, porque só é possível gerenciar, após a monitoração. Tanto o monitoramento quanto o gerenciamento possuem significados que se encontram, porém algumas peculiaridades tratadas nesse capítulo justificam o fato do monitoramento ser tratado antes do gerenciamento.

2.1 MONITORAMENTO

A rede de computadores era utilizada para atividades mais importantes, porém a tecnologia evoluiu muito rápido e os equipamentos se tornaram mais baratos. Isso

desencadeou o crescimento da rede levando a todos mais praticidade (Pinheiro, 2002). À medida que a rede de computadores se expandiu tornou-se necessário monitorá-la. Dias (2008) relata a importância de se monitorar a rede de uma organização no intuito de que o administrador possa ter maior controle dos equipamentos, mantendo a rede em perfeito estado e colocando-o sempre informado sobre os recursos que estão sendo disponibilizados ou não. “O monitoramento de uma rede de computadores torna-se uma atividade essencial para garantir o seu funcionamento contínuo assim como para assegurar um elevado grau de qualidade dos serviços oferecidos” (Neto, *et.al*, 2014).

Balsini, 2009 aborda em seu trabalho que o monitoramento de uma rede é de grande importância sendo muito útil na detecção de futuras falhas dentro de um ambiente corporativo e que é fundamental na administração.

Para Dias, 2008, o monitoramento em tempo real vem sendo utilizado cada vez mais, pois as informações sobre os equipamentos chegam mais rápidas, são precisas e confiáveis o que facilita muito para tomar boas decisões quando necessário.

Com toda essa expansão da rede, torna-se difícil mantê-la funcionando em perfeito estado. Surgem vários problemas, usuários começam a reclamar pela falta de disponibilidade dos recursos, a rede vai se tornando lenta, ocorrem problemas nos downloads, entre vários outros problemas (Neto *et.al*, 2014).

Visando resolver os problemas que são causados quando a rede se torna de grande porte é necessário o uso de ferramentas que faça o acompanhamento de todos os equipamentos presentes na mesma. Fazendo uso de uma ferramenta de qualidade é possível detectar falhas antes mesmo que o usuário possa notar. Através de relatórios e alertas é que se pode prevenir as falhas, pois as informações geradas vão servir para melhorar o serviço, deixando-o de boa qualidade e eficiente sem ter que resolver os problemas depois que os usuários tenham percebido (Neto, *et.al*, 2014).

As ferramentas de monitoramento reduzem o trabalho do administrador, pois somente eles são capazes de controlar tudo que está presente na rede de forma rápida e ágil. Todas as informações coletadas são disponibilizadas ao administrador de forma clara e precisa. João Simões, 2010 relata em seu trabalho que utilizando uma ferramenta para monitorar os dispositivos, recursos e serviços que uma rede possui melhora vários aspectos de uma empresa/organização, pois as mesmas possuem como base de funcionamento verificações periódicas, o recebimento das informações sobre os dispositivos que estão sendo monitorados e o tratamento dessas informações para serem apresentadas ao responsável pelo bom funcionamento da rede (administrador da rede).

2.2 GERENCIAMENTO

“O gerenciamento de rede é o procedimento que consiste em controlar todos os componentes de hardware e software da rede” (RIGNEY, 1996). Ele possui como objetivo fazer o monitoramento e o controle dos equipamentos presentes na rede a fim de garantir bom funcionamento para os usuários (Moqadi, 2011). As atividades fundamentais do gerenciamento de redes, para Santos, 2002, apud Oda, C.S, 1994, se baseiam na detecção de falhas, no menor tempo possível, e em designar procedimentos para a previsão de problemas futuros. O gerenciamento deve ser realizado em qualquer rede, independente de seu tamanho ou complexidade, para assim garantir que os usuários possuam serviços de qualidade (Black, 2008).

A rede que não possui mecanismos de gerenciamento corre o risco de apresentar problemas podendo afetar o tráfego dos dados, interferir em sua integridade, causando problemas de congestionamento do tráfego, recursos sendo mal utilizados e uma série de outros problemas (Pinheiro, 2002).

Obter a rede gerenciada se tornou algo de grande relevância, pois com o gerenciamento a equipe de TI conseguirá acompanhar e resolver da melhor forma os problemas que surgem. “O gerenciamento de rede é essencial dentro da estrutura de uma empresa, ainda mais se o ambiente de TI for grande e complexo” (Candido, 2011).

O gerenciamento é de suma importância, pois com o mesmo obtêm-se bom fluxo no tráfego das informações, permitindo analisar se os recursos estão sendo utilizados da forma correta e não sobrecarregados e os dados possam ser transportados de forma segura e confiável (Moqadi, 2011).

Black, 2008, confirma que o gerenciamento de redes permite além de controlar os recursos que estão disponíveis, identifica e previne problemas, sendo este investimento justificado com controle de recursos, melhoramento nos serviços, dentre outros benefícios que o gerenciamento proporciona. Mas sem uma ferramenta este serviço se torna algo quase impossível ainda mais se a rede for de grande porte.

Fazer esse controle da rede sem o auxílio de uma ferramenta adequada é uma atividade muito difícil, e pode não obter um resultado de boa qualidade. Isso também acontece quando não se utiliza a ferramenta correta, capaz de mostrar os principais elementos da rede (Candido, 2011).

Para o gerenciamento faz-se necessário utilizar a ferramenta específica, isso devido ao aumento de equipamentos que precisam ser controlados, uma vez que não é possível gerenciar cada um de forma individual. Quanto maior a rede, mais complexo se torna o gerenciamento, necessitando usar ferramentas automatizadas para monitorar e controlar (Black, 2008).

Black, 2008, justifica porque investir em um software de gerenciamento através dos seguintes fatores:

- As redes e recursos de computação distribuídos estão se tornando vitais para a maioria das organizações. Sem um controle efetivo, os recursos não proporcionam o retorno que a corporação requer.
- O contínuo crescimento da rede em termos de componentes, usuários, interfaces, protocolos e fornecedores ameaçam o gerenciamento com perda de controle sobre o que está conectado na rede e como os recursos estão sendo utilizados;
- Os usuários esperam uma melhoria dos serviços oferecidos (ou mínimo, a mesma qualidade), quando novos recursos são adicionados ou quando são distribuídos.
- Os recursos computacionais e as informações da organização geram vários grupos de aplicações de usuários com diferentes necessidades de suporte nas áreas de desempenho, disponibilidade e segurança. O gerente de rede deve atribuir e controlar recursos para balancear estas várias necessidades.
- À medida que um recurso fica mais importante para a organização, maior fica a sua necessidade de disponibilidade. O sistema de gerenciamento deve garantir esta disponibilidade.
- A utilização dos recursos deve ser monitorada e controlada para garantir que as necessidades dos usuários sejam satisfeitas a um custo razoável.

Matos, 2006, define os componentes de um sistema de gerenciamento:

- Monitor: é uma estratégia que irá fornecer a interface de monitoramento, também define o centro de controle de toda rede;
- Aplicação de monitoramento: são os módulos do software de gerenciamento;
- Sistema gerente: é o software da estação de monitoramento, que executa as funções básicas de monitoramento;
- Sistema agente: é o software que obtém e envia as informações de gerenciamento para monitor;
- Objetos gerenciados: são as informações de gerenciamento que representam os recursos e suas atividades;
- Agente de monitoramento: é um módulo que gera resumos e análises estatísticas das informações de gerenciamento.

Nota-se que o gerenciamento é de suma importância, isso devido à necessidade de se obter uma rede sempre em bom estado e informações precisas para tomar decisões mais acertadas. Candido, 2011, relata que o gerenciamento de redes tem por finalidade verificar e controlar as informações que são geradas através de softwares de gerenciamento, o que proporciona melhor análise para possível tomada de decisão para se ter bom funcionamento da rede.

2.2.1 Áreas funcionais de gerência de redes

A gerência de redes pode ser classificada em cinco áreas funcionais, segundo a Organização Internacional para Padronização (ISO 7498-4), são elas: A Gerência de Falhas, Gerência de Configuração, Gerência de Contabilidade, Gerência de Desempenho e Gerência de Segurança. Também conhecidas pelo acrônimo FCAPS. Pinheiro, 2002, faz a definição de cada uma dessas áreas funcionais:

- Gerenciamento de falhas: Com este recurso é realizado um rastreamento para auditoria, no qual mostra características de erros da rede.
- Gerenciamento de configuração: este recurso trabalha com a instalação, inicialização, dentre outros.
- Gerenciamento de contabilização: coleta e processa os dados, implementando mecanismos que registrem qualquer ação do usuário, envolvendo consumo de recursos, medindo o uso dos mesmos, para que possa estabelecer métricas, quotas, determinar custos e taxar usuários.
- Gerenciamento de segurança: faz o controle de acesso aos recursos da rede por meio de autenticação e políticas de autorização.
- Gerenciamento de desempenho: informa a taxa de utilização da rede, bem como a taxa de erros, isso em tempo real.

2.2.2 Protocolos de gerenciamento

Devido à expressiva necessidade de gerenciamento, fez-se imprescindível a criação de padrões para as ferramentas. Em virtude dessa necessidade, surgiram dois padrões de protocolo. De acordo com Black, 2008, são eles:

- Família de protocolo SNMP: Este protocolo de gerência foi adotado como padrão para redes TCP/IP sendo um conjunto de padrões para gerenciamento incluindo um protocolo, uma especificação de estrutura de dados e um conjunto de objetos para redes TCP/IP.
- Sistemas de gerenciamento OSI: É um grande conjunto de padrões possuindo grande complexidade e que define aplicações de proposito geral para gerência de rede, serviço de gerenciamento e protocolo, especificação de estrutura de dados e um conjunto de

objetos de dados. Mas para Stallings, 1993, este protocolo é complexo e por ser complexo não é muito popular.

“Os protocolos de gerenciamento têm a função de garantir a comunicação entre os recursos de rede homogêneas ou não”. Existem vários, mas os que se desenvolveram mais foram o SNMP e o CMIP, ambos do modelo OSI e da arquitetura TCP/IP (Pinheiro, 2002).

De acordo com Bueno, 2012, ”Basicamente os modelos de gerencia mais aceitos atualmente são o ISO que faz uso do protocolo CMIP e o modelo SNMP do IETF (Internet Engineering Task Force) que usa o protocolo SNMP[...]”.

2.2.2.1 *Simple Network Management Protocol (SNMP)*

O SNMP é um protocolo de camada de aplicação, sendo desenvolvido para transportar informações de gerência de rede entre os dispositivos gerenciados e os sistemas de gestão de redes. Ele permite que os administradores coordenem o desempenho da rede realizando o monitoramento de interfaces, processadores, memórias de roteadores, switches, dispositivos wireless e servidores. Com isso os administradores visualizam a situação atual das redes, mantendo o histórico de atividade, receber avisos imediatos para ajudar na resolução de problemas (SNMP – Introdução, 2015).

Soares e Fernandes, 2013, diz que o SNMP “... é um protocolo bem simples, de fácil implementação, que gerencia roteadores, servidores, estações de trabalho entre outros dispositivos de redes”. “O protocolo SNMP define como gerente e agente se comunicam, conforme Bueno, 2012, apud COMER, 2007, o SNMP define o formato das requisições que um gerente envia a um agente e o formato das respostas que o agente retorna”.

“Para administração usam-se protocolos padrões de gerenciamento de redes, estes protocolos são usados para troca de mensagens entre o gerente e os agentes. O maior exemplo é o SNMP” (Melo, 2007).

2.2.2.2 *Common Management Information Protocol (CMIP)*

“O protocolo CMIP é o protocolo OSI de Nível de Aplicação, orientado a conexão e utiliza os serviços providos pelo ASCE (Association Control Service Element), ROSE

(Remote Operations Service Element) e pelo serviço de apresentação” (Pinheiro, 2002). “O CMIP tem o objetivo de suprir as limitações do SNMP” (Matos, 2006).

3 METODOLOGIA

Este trabalho contém um comparativo teórico entre algumas ferramentas livres de monitoramento e gerenciamento de redes mais utilizadas, são elas: Nagios, Zabbix, Cacti e MRTG. A metodologia empregada consiste em uma pesquisa descritiva. O comparativo possibilitará saber se há entre as ferramentas estudadas alguma que se adeque aos requisitos levantados e propor a instalação da mesma.

Durante o período de estágio realizado no setor de coordenação de TI do IFMG –SJE foi possível constatar algumas dificuldades no monitoramento dos equipamentos presentes na infraestrutura de redes da instituição. Para a escolha da ferramenta serão utilizados os requisitos propostos durante uma entrevista ao coordenador do setor de TI do IFMG-SJE.

A entrevista buscou saber quais necessidades fundamentais se espera que a ferramenta satisfaça e o que a instituição deseja solucionar com a implantação da mesma. Foram requeridos os seguintes tópicos:

- Ferramenta livre: A ferramenta deverá ser livre devido à falta de recursos para se empregar na compra de um software com essa finalidade.
- Robustez no monitoramento: A ferramenta deverá ter como objetivo o monitoramento, principal problema que se busca solucionar.
- Fácil de configurar: A ferramenta deverá ser fácil de manusear e configurar devido à falta de recursos e disponibilidade de tempo para treinamentos específicos aos profissionais que farão uso da mesma.
- Fácil para criação de templates: ser fácil para criar algum conteúdo (monitoramento de ativos de rede);
- Utilizar protocolo SNMP: protocolo requerido durante a entrevista com o coordenador de TI.

3.1 NAGIOS

Segundo Marco Lima, 2015, o Nagios é uma ferramenta popular e muito conhecida, é uma base para outros sistemas de código aberto. A ferramenta Nagios é um software livre que possui grande potência no monitoramento, desenvolvido por Ethan Galstad e equipe, distribuído sob a licença GPL (Andrade, 2006). Este software possui muitas vantagens, mas em contrapartida possui alguns pontos negativos. São eles: relatórios escassos, a complexidade para adicionar um novo dispositivo na rede, necessitando editar muitos arquivos de configuração (Santos, 2015). Ele coleta as informações dos ativos da rede através do protocolo SNMP que possuem “agentes” configurados para repassar estas informações ao servidor Nagios (Balsini, 2009).

Nagios possui um desempenho incrível seja monitorando redes de grande ou pequeno porte, ressaltando que ele foi desenvolvido para grandes ambientes. Ele alerta quanto há queda de serviços ou hosts que são vigiados através dos arquivos de configuração, seja com monitoramento de equipamentos através do protocolo SNMP, sendo este o agente que realiza a troca de informações entre o Nagios e seus hosts (Andrade, 2006).

O Nagios é uma ferramenta que monitora elementos e serviços de rede. Além de possuir diversos plug-ins disponíveis que podem ser utilizados para testes. Ele permite enviar para o administrador mensagens eletrônicas, alertas, sons notificando o problema que esta acontecendo ou que aconteceu. Esta ferramenta permite montar grupos no qual poderá receber relatórios e alertas sobre o sistema, sendo que a configuração é realizada dentro de arquivos de texto e a interface com o usuário é realizada no console web (Peixinho *et.al*, 2013).

Martins e Lopes, (2015) afirma que o Nagios é uma ferramenta bastante versátil e possui muitas vantagens, quando instalado num sistema, este software proporciona muitos ganhos. Ainda segundo os mesmos autores, através da configuração do Nagios pode-se perceber que esta ferramenta é mais eficiente em empresas, sendo muito útil nesta área. Com ele é possível estar definindo horários de trabalho, quem é responsável pelo quê e quem tem acesso na gestão de sistema.

Majewski, 2009, cita algumas das vantagens da ferramenta Nagios:

- Pode-se monitorar diversos serviços. Com ele é possível monitorar além de computadores e equipamentos presentes na rede outros sistemas, por exemplo, sistema que insere dados em base.

- Monitora desempenho através da CPU e também com o uso de plug-ins, sendo assim ele monitora desde o log do sistema operacional até a carga do processador.
- Monitora os equipamentos em geral com utilização de túneis de criptografados SSH ou SSL, ou seja, o monitoramento é realizado com confiança e segurança a quilômetros de distância.
- Desenvolve plug-ins com as ferramentas C, Perl, PHP e C#. Isso caso queira desenvolver um plugin específico.
- Esta ferramenta manda notificações por e-mail, SMS, etc. dependendo do que o usuário definiu.
- Permite o controle de permissões.
- É de código aberto e distribuído sobre a licença GPL. Isso possibilita que o usuário deixe a ferramenta de acordo com a necessidade do cliente.

De acordo com Neto e Uchôa, (2015), o grande diferencial do Nagios é o esquema de alerta sobre anormalidades que pode ser configurado em sua interface *web*, no entanto, o fato de não usar gráficos para acompanhamento de resultados torna a análise e acompanhamento complexa e desafiadora. Segundo Majewki, 2009, a desvantagem do Nagios consiste em: “Não gerar gráficos de utilização ou desempenho”. Para obter gráficos o Nagios necessita ser integrado com outras ferramentas, como o Cacti , por exemplo.

Segundo Martins e Lopes, 2015, “a instalação do Nagios num dado sistema não é acessível a qualquer utilizador, aliás, sem conhecimentos das redes e das plataformas visadas é aconselhável que contrate profissionais para fazer o trabalho”. Os mesmos autores ainda afirmam que “mesmo pra quem tenha conhecimentos da área, uma adaptação ao Nagios implica a leitura de muita documentação”.

3.2 ZABBIX

Segundo Santos, 2008, Zabbix possui suporte ao protocolo SNMP sendo este nativo da ferramenta e Célestin, 2013, diz que o Zabbix é uma ferramenta adotada sobre a licença *Open Source*. Sendo considerada na atualidade como uma das melhores ferramentas e o que a tornou uma ferramenta poderosa e completa, foi à junção das funcionalidades herdadas do Nagios e do Cacti.

Majewski, 2009, define as vantagens do Zabbix:

- Possui grande capacidade de gerenciar servidor. Somente um servidor é capaz de gerenciar várias máquinas e com um ótimo desempenho.
- Ele é uma ferramenta com interface amigável, fácil de gerenciamento e de fácil customização.
- O servidor, o banco de dados e a interface de administração ficam em servidores distintos, isso impede uma sobrecarga, facilita a manutenção e diminui as despesas computacionais.
- As informações coletadas no monitoramento podem ser armazenadas em bancos de dados como MySQL, PostgreSQL, Oracle e Sqlite.
- A análise das informações é realizada através de gráficos, mapa e visões. Utilizando estes mecanismos a compressão se torna fácil e confiável.
- As informações de alerta são passadas ao administrador através de SMS, e-mail, Jabber.
- Ele executa comandos no servidor que esta sendo monitorado na tentativa de correção dos erros (monitoramento pró-ativo).
- Esta ferramenta não necessita de plug-ins ou scripts adicionais, pois a mesma é completa e única.
- Possui facilidade para integrar com outras ferramentas para realizar análise estatística.
- Esta ferramenta permite realizar monitoramento remoto, ou seja, faz o monitoramento de equipamentos e ativos que estão fora da rede.
- Realiza o monitoramento de desempenho, utilização da CPU, pode realizar a análise do consumo de memória, desempenho do processador, dentre outras possibilidades.
- Quanto às permissões, pode-se defini-las por nível de usuários, grupos e IPs.
- Há possibilidade de acessar o código fonte e código aberto para auditoria.

O Zabbix assim como o Nagios deixa a desejar em alguns quesitos, segundo Roberto Majewski, 2009, as desvantagens do Zabbix são:

- Realiza o monitoramento somente de desempenho e da disponibilidade dos ativos.
- O UNIX é o único sistema operacional que pode responder ao desempenho que se necessita para instalar o Zabbix.

Bonomo, 2006, relata que os relatórios do Zabbix permitem fácil compreensão e visualização dos dados. Com a configuração realizada ele pode monitorar pequenas e grandes companhias com número relevante de servidores.

O Zabbix possui excelentes relatórios e oferece uma visualização dos dados armazenados, permitindo que o usuário acesse a interface web para visualizar os relatórios e as estatísticas da ferramenta. Esta interface garante o estado de bom funcionamento da rede e dos servidores, possibilitando acesso de qualquer lugar. Quando bem configurado o Zabbix pode monitorar toda a infraestrutura de TI. Isso em pequenas empresas que possuem poucos servidores e em grandes empresas que utilizam um número mais elevado de servidores.

O ZABBIX oferece:

- Suporte para ambos mecanismos de *polling* e *trapping*;
- Servidores para Linux, Solaris, HP-UX, AIX, Free BSD, Open BSD, OS X;
- Agentes de alta performance nativos;
- Monitoramento de servidores sem um agente instalado;
- Autenticação de usuário segura utilizando criptografia dos dados;
- Permissões de usuários flexíveis;
- Interface gráfica *web*;
- Flexível notificação e predefinidos eventos por e-mail;
- Alto nível de visualização (Negócios) de recursos monitorados.

Segundo Neto e Uchôa, 2015, o Zabbix é uma ferramenta capaz de agregar funções ao MRTG, Cacti e Nagios. Possui mecanismo de coleta de dados local, remota através do agente Zabbix e SNMP, o que possibilita monitorar o status de servidores, serviços, ativos de rede, banco de dados e alertas e caso de problemas. A individualização na coleta de dados pelo Zabbix é feita através de sua interface *web*, sendo possível incluir qualquer chave SNMP ou agente Zabbix para coleta de gráficos a partir de dados coletados, mapas, eventos e alertas ao administrador.

Ao realizar testes com as ferramentas Nagios, Zabbix, Cacti e MRTG, os mesmos autores abordaram que o Zabbix se destacou como a melhor ferramenta para o uso em ambientes de médio e grande porte. Para os autores citados no parágrafo anterior o Zabbix é equivalente ou melhor que as ferramentas citadas acima. Segundo eles, o Zabbix permite que o administrador obtenha informações minuciosas sobre servidores, serviços, etc. e possui instalação rápida simplificada e uma interface web também simplificada para realizar configuração.

De acordo com Zabbix Documentation 2.4, 2015, a ferramenta Zabbix possui “configuração simplificada: Todo elemento monitorado é um *host*, *hosts* são monitorados assim que inseridos no banco de monitoração, é possível utilizar perfis de monitoração (templates) aos dispositivos monitorados (*hosts*)”.

Santos, 2008, aborda as características do Zabbix:

- Monitoramento de desempenho: consegue-se monitorar a carga do processador, número de processo rodando, atividade no disco rígido, espaço da memória swap e disponibilidade da memória.
- Mecanismo de alerta: as informações podem ser enviadas por e-mail, o administrador pode estar definindo um endereço, ou mesmo através de SMS, notificações por celular, etc.
- Monitoramento de arquivos de log: um alerta pode ser disparado para o administrador quando houve alguma informação impressa em um determinado arquivo de log.
- Verificação de integridade: qualquer arquivo de configuração (binários, kernel, etc.) que for alterado o administrador fica sabendo através de alerta.
- Serviços de auditoria: todas as informações são guardadas em banco de dados, pois as mesmas podem ser utilizadas para algum propósito depois.
- Capacidade de planejamento: observando o funcionamento de hardware e software existentes na infraestrutura, possibilita que o administrador tenha visão clara sobre a necessidade de atualização de um hardware específico, quando estiver sobrecarregado.

Filho, 2010, aborda:

Visando alcançar um diagnóstico mais preciso da infra-estrutura da rede, escolhemos uma ferramenta de monitoramento de rede de nome Zabbix, que se apresentou como uma das soluções mais completas disponíveis do mercado. É especializado em monitorar serviços de rede e também recursos de computadores ou equipamentos de rede.

3.3 CACTI

O Cacti é uma ferramenta livre de monitoramento. Possui uma solução gráfica completa de rede, projetada para aproveitar o poder de armazenamento de dados MySQL e funcionalidade gráfica. A ferramenta permite a criação de gráfico avançado por template, vários métodos de aquisição de dados, gerenciamento de usuários e de possibilidade de adicionar novos recursos. Dispõe de uma interface gráfica intuitiva e fácil de usar. É recomendada para redes simples e até mesmo para redes complexas com centenas de dispositivos (CACTI, 2015).

De acordo com Matos 2009, o Cacti “Foi desenvolvido para ser flexível de modo a se adaptar facilmente a diversas necessidades, bem como ser robusto e fácil de usar”. Segundo Santos 2015, com o Cacti “é possível reproduzir em gráficos, informações referente ao estado dos elementos monitorados na rede através do SNMP”. A interface do Cacti, juntamente com sua estrutura, são voltadas para o *RRDTool*. Oetiker, 2005, define o *RRDTool* como “um sistema de base de dados desenvolvido para armazenar séries de dados numéricos sobre status de redes de computadores, permite o armazenamento de dados como temperaturas, uso de processador, uso de memória, entre outros”.

De acordo com Santos, 2015, o Cacti é uma ferramenta que “permite o monitoramento de informações como: tráfego na rede, uso de memória, espaço em disco, switches, roteadores, etc.”

A arquitetura do Cacti conta com a alternativa de expansão através de plug-ins que adicionam novas funcionalidades. O uso de plug-ins permite aos administradores a possibilidade de incluir outras ferramentas livres ao sistema. Os plug-ins enriquecem a ferramenta, pois, através desse recurso é possível adicionar diferentes funcionalidades. Conforme afirma Majewski, 2009, “um destes plug-ins é o PHP Network Weathermap que mostra um mapa de rede e o estado de cada elemento”.

As vantagens do Cacti, segundo Majewski,2009 são:

- Utilização ilimitado de gráficos;
- Manipulação dos dados do gráfico usando as funções matemáticas incorporado RRDTool;
- Criação das fontes de dados através da utilização do MySQL;
- Coleta de dados através de scripts personalizados definidos pelo usuário;
- Recuperação de dados através de SNMP ou um scripts;
- Criação de hierarquias gráficas;
- Controle de permissões;
- Interface intuitiva e agradável, sendo acessível a qualquer tipo de usuário;
- E escrito em boa parte em PHP, então a infra-estrutura necessária é um servidor http na famosa estrutura LAMP (Linux, Apache, MySQL, PHP).

De acordo com Neto e Uchôa, 2015, “a configuração do Cacti é extremamente simplificada”, pois conta com perfis de coleta de dados básicos e geração de gráficos que facilitam a configuração da ferramenta.

No entanto, o Cacti possui algumas desvantagens, de acordo com Neto e Uchôa, 2015, a principal delas está na dificuldade em incluir novas chaves SNMP ou novos *scripts* para coleta de dados que não estão disponíveis nos perfis padrões. Outra inconveniência é o fato de

não possuir nenhum mecanismo de alerta. Majewski, 2009, também aborda alguns pontos negativos dessa ferramenta, segundo ele, um dos problemas é a existência de apenas uma interface de gerenciamento. Sendo assim, para monitorar gráficos é preciso a utilização de outra ferramenta de captura, como por exemplo, o RRDTool, MRTG ou Nagios.

Em ambientes pequenos ou onde somente é preciso gerar gráficos estatísticos com dados locais ou remotos através do SNMP, sem que seja necessário qualquer outro recurso, o Cacti tem um bom desempenho devido à sua facilidade.

3.4 MULTI ROUTER TRAFFIC GRAPHER (MRTG)

O MRTG (*Multi Router Traffic Grapher*) é um software de monitoramento de redes escrita em Perl. É uma ferramenta livre, licenciada sob a GNU (*General Public License*), usa o SNMP para ler os contadores de tráfego de seus roteadores. É capaz de registrar os dados do tráfego e criar gráficos que representam o tráfego na conexão de rede monitorada. Os gráficos são incluídos em páginas web e podem ser acessados a partir de qualquer navegador. O MRTG gera páginas HTML contendo imagens PNG com uma representação do tráfego da rede. É uma ferramenta portátil e funciona na maioria das plataformas UNIX e WINDOWS NT. Usa implementação SNMP de alta portabilidade, e não é preciso instalar nenhum pacote de SNMP externo. Conta com um conjunto de ferramentas de configuração que tornam sua configuração simples e descomplicada. (MRTG, 2015).

Segundo Matos, 2006, o MRTG é extremamente útil para verificar o tráfego utilizado em sua rede/link. Santos, 2006, afirma que através do MRTG, a coleta de informações é pontual, a visualização das estatísticas geradas nos gráficos pode ser diária, semanal, mensal e anual. Isso é possível porque o MRTG armazena os logs das informações dos equipamentos contendo as respectivas datas.

Ainda de acordo com Santos, 2006, as características do MRTG são:

- Portabilidade: O MRTG trabalha com as plataformas UNIX e Windows NT.
- Perl: O MRTG é escrito nesta linguagem de programação e traz todo o código fonte.
- Portabilidade SNMP: O MRTG faz utilização de implementação de alta portabilidade escrita na linguagem Perl, por isso não é necessário instalar pacote SNMP externo.

- Suporte a SNMPv2c: O MRTG faz a leitura dos contadores de 64 bits do SNMPv2c, por isso os contadores deixaram de ser um problema.
- Interface de identificação confiável: A identificação das interfaces dos roteadores é realizada por IP, Descrição e Endereço Ethernet mais o número de interface normal.
- Tamanho dos arquivos de log fixos: os arquivos onde os logs ficam armazenados no MRTG não crescem, isso devido ao uso de um algoritmo que faz a consolidação de dados únicos.
- Configuração automática: O MRTG traz um conjunto de ferramentas de configuração realizando a mesma de forma bem mais simples.
- Desempenho: As rotinas mais difíceis foram escritas na linguagem C por causa da iniciativa de Dave Rand (Co-Autor).
- Livre de gráficos GIF: Os gráficos gerados são no formato PNG, fazendo uso da biblioteca GD de Thomas Boutell.
- Customizável: O designer das páginas do MRTG é configurável.
- RRDTool: O MRTG foi desenvolvido para funcionar com o RRDTool, caso precise de performance isso pode ajudar.

Para Augusto, 2002, as vantagens do MRTG são:

- A precisão com que os dados são gerados, já que a leitura é feita diretamente nas variáveis SNMP.
- As primeiras informações obtidas, ou seja, as informações mais antigas são armazenadas em forma de média, com isso, os arquivos de registros de utilização não crescem com o tempo.
- A facilidade de acesso e interpretação dos gráficos gerados também é uma vantagem, pois é possível executá-los tanto nas plataformas Windows como Unix. Optar pelo uso de código aberto também é um ponto positivo.
- É possível obter qualquer informação de variáveis SNMP disponíveis nos roteadores, e aplicá-las em qualquer rede que faça o uso do SNMP.

Augusto, 2002 lista também as desvantagens do MRTG, são elas:

- Por padrão, os gráficos não são gerados no momento em que são acessados, e sim, a cada 5 minutos, com isso, os dados apresentados são referentes aos últimos 5 minutos.
- Não é possível medir a largura de banda nominal, somente a utilizada.
- Devido ao fato de utilizar o protocolo SNMP para coletar informações, e este por sua vez utiliza o protocolo UDP, pode ocorrer a perda de informações, e em consequência dessa perda, pode ser gerada informações incorretas.
- Informações de desempenho são obtidas através de variáveis SNMP, consequentemente, as métricas ficam restritas a essas informações.

De acordo com Neto e Uchôa, 2015, a obtenção de resultados logo após a instalação do MRTG é desgastante, porque a ferramenta não conta com uma interface para configuração e exige do usuário conhecimentos da chave SNMP ou a criação de *scripts* para obtenção dos dados e posteriormente a geração de gráficos. Ainda segundo Neto e Uchôa, 2015, tanto o MRTG, quanto o Cacti e o Zabbix são ferramentas que não traz nenhuma informação para acompanhamento logo após sua instalação, porém conta com uma interface web que simplifica a configuração para geração de gráficos.

3.5 COMPARATIVO DAS FERRAMENTAS ESTUDADAS COM FCAPS

3.5.1 Nagios

Possui gerenciamento de falhas, assim que é detectado falha em algum cliente, o Nagios segue uma lista de ações a serem tomadas, que pode ser desde uma mensagem de texto, ou em casos extremos, a reinicialização do servidor. Não possui gerência de configuração, a instalação do Nagios requer conhecimentos específicos em redes. Sua configuração é complexa, exige a instalação e configuração de *plug-ins*. Sendo que, em alguns casos, é necessária a reconfiguração de todos os *scripts* de configuração. Segundo Martins e Lopes, mesmo para quem já possui algum conhecimento na área de redes, “uma adaptação ao Nagios implica a leitura de muita documentação”. Possui gerenciamento de desempenho, sendo possível monitorar a utilização de CPU com o uso de *plug-ins*. Segundo Majewski, 2009, o monitoramento de desempenho do Nagios é capaz de checar, desde uma simples disponibilidade do ativo, a complexa monitoração de log do sistema operacional,

carga do processador, etc. Possui gerenciamento de contabilização, Koch, 2008, destaca em seu trabalho, o poder de contabilização do Nagios. O software conta com o monitoramento de recursos de *hosts*, é capaz de monitorar a carga do processador, utilização de espaço em disco, utilização de CPU, entre outros. Possui gerenciamento de segurança, o Nagios é capaz de definir de forma antecipada os usuários que terão permissão para visualizar o trabalho executado via *web*.

3.5.2 Zabbix

Assim como o Nagios, o Zabbix também possui o gerenciamento de falhas. De acordo com Bonomo, 2006, "O Zabbix gerencia falhas e envia mensagens de texto, *e-mail*, ou alertas sonoros, sendo também capaz de executar comandos remotos, previamente definidos pelo administrador." Possui gerenciamento de desempenho, sendo esse um dos mais importantes usos do Zabbix. Ainda de acordo com Bonomo, 2006, essa ferramenta é capaz de monitorar a carga do processador, o número de processos, atividade no disco rígido, espaço da memória *swap* e disponibilidade da memória, entre outros parâmetros de sistemas. O Zabbix também é capaz de fornecer ao administrador de sistemas de informações, em tempo real, sobre o desempenho de um servidor.

Possui gerenciamento de contabilização, segundo Santos, 2015, é possível escolher vários métodos para realizar a coleta, entre eles, SNMP, IPMI, o item realiza essa coleta que pode referenciar um hardware, rede, sistemas operacionais, *middleware* e aplicações.

Possui gerenciamento de segurança, segundo Bonomo, 2006, "no Zabbix todos os valores dos parâmetros monitorados são armazenados em banco de dados. Os dados coletados podem ser usados mais tarde para algum propósito. O Zabbix gera uma auditoria das mudanças dos valores dos parâmetros para que o administrador possa saber quem as fez, para em caso de algum problema possa tentar identificar os culpados".

Possui gerenciamento de configuração, o Zabbix tem interface gráfica e interface *web*. De acordo com Rocha e Serradourada, 2008, a interface gráfica do Zabbix é bastante fácil de ser utilizada. O software permite a configuração por meio da interface *web*. Através da interface *web* é possível acompanhar o desempenho completo da rede e dos dispositivos gerenciados.

Segundo Santos, 2015, o Zabbix é um software robusto, por oferecer facilidades na configuração, relatórios da rede, suporte a vários tipos de banco de dados, e assim como o Nagios, eles podem ser usados tranquilamente em redes de pequeno à grande porte.

O site oficial do Zabbix traz uma relação das empresas que utilizam o software. Segundo o site, "muitas empresas confiam na ferramenta zabbix para monitoramento por ser uma ferramenta robusta. Os usuários e clientes são instituições e empresas de grande porte. Como exemplo temos: Dataprev, globo.com, RENNEN, Petrobras, dentre várias outras."

3.5.3 Cacti

Não possui gerenciamento de falhas, não é capaz de enviar alertas em caso de paradas de serviço ou qualquer outro evento anormal. Segundo Koch, 2008, o foco principal do Cacti é o gerenciamento de contabilização. Possui Gerenciamento de segurança, conta com o gerenciamento de usuários, e controle de acesso por nível de usuário. Possui gerenciamento de desempenho, pois é capaz de monitorar a largura da banda, utilização de memória, entre outros. No que se refere à gerência de configuração, o Cacti não traz nenhuma informação para acompanhamento logo após sua instalação, ou seja, não possui gerência de configuração. Entretanto, possui uma interface web que torna sua configuração menos trabalhosa. Conforme Meier, 2007, por meio da interface web, é possível realizar por completo, o cadastramento de novos dispositivos, a criação de gráficos, entre outras atividades, sem que seja preciso fazer *restart* para que as novas configurações comecem a funcionar.

3.5.4 Multi Router Traffic Grapher (MRTG)

Não possui gerenciamento de falhas, não identifica nem soluciona problemas na rede. O MRTG possui gerenciamento de desempenho. É utilizado para representar graficamente todos os tipos de dispositivos da rede com o fim de proporcionar o entendimento e a análise do comportamento dos elementos monitorados na rede (MTRG, 2015). Não possui gerenciamento de configuração, Neto e Uchôa, 2015, afirmam que o software não traz nenhuma informação para acompanhamento logo após sua instalação, não conta com uma interface de configuração, possui apenas uma interface web de configuração. Possui gerenciamento de contabilização, segundo Correia, 2004, o MRTG é capaz de verificar o tempo de paralização dos hosts na rede. Não possui gerenciamento de segurança, não existe uma interface que faça controle de nível de acesso.

A tabela a seguir, foi elaborada de acordo com as informações adquiridas, com a finalidade de mostrar quais as ferramentas possuem os requisitos propostos pelo coordenador de TI.

Tabela 1- Comparativo das quatro ferramentas escolhidas para avaliação de acordo com os requisitos propostos.

Parâmetros avaliados				
Requisitos	Nagios	Zabbix	Cacti	MRTG
Ferramenta livre	Sim	Sim	Sim	Sim
Robustez no monitoramento	Sim	Sim	Sim, Integrando outras ferramentas	Informação não encontrada
Facilidade de configuração	Não	Sim	Sim	Não
Utiliza protocolo SNMP	Sim	Sim	Sim	Sim
Fácil para criação de templates	Informação não encontrada	Informação não encontrada	Informação não encontrada	Informação não encontrada

Fonte: Elaborada pelos autores.

4 RESULTADOS E DISCUSSÕES

Após ter estudado sobre as ferramentas citadas neste trabalho, notou-se que todas as ferramentas são livres e fazem uso do protocolo SNMP. Quanto ao quesito robustez no monitoramento o Nagios, Zabbix e Cacti mostraram-se ferramentas bem robustas. Já a ferramenta MRTG, não foi encontrado nenhum autor que confirme essa funcionalidade.

Nagios e MRTG não cumprem o requisito “facilidade na configuração”, o Nagios, embora seja robusto na monitoração, tem configuração e instalação complexas, Segundo Martins e Lopes, 2015, “mesmo pra quem tenha conhecimentos da área, uma adaptação ao Nagios implica a leitura de muita documentação”. A configuração do MRTG também é desafiadora, pois, segundo Neto e Uchôa, 2015, o MRTG não conta com uma interface para configuração e exige do usuário conhecimentos da chave SNMP ou a criação de *scripts* para obtenção dos dados e posteriormente a geração de gráficos.

As ferramentas que mais se aproximaram dos requisitos propostos, foram o Cacti e o Zabbix. No entanto, o Cacti tem algumas limitações, de acordo com Neto e Uchôa, 2015, uma delas consiste no fato “de não possuir nenhum mecanismo de alerta”. Isso pode ser resolvido com o uso de plug-ins, através desse recurso é possível adicionar diferentes funcionalidades. Porém, esse não é o objetivo do trabalho.

O Zabbix é a ferramenta mais completa, dentre as pesquisadas. Segundo Neto e Uchôa, 2015, “O Zabbix é equivalente ou melhor que o uso conjunto de todas as outras ferramentas apresentadas, permitindo ao administrador obter informações extremamente minuciosas...”.

O Zabbix contém uma excelente documentação técnica tanto sobre os recursos quanto a configuração, facilitando muito a tarefa do administrador ou gestor da rede. Além disso, esta ferramenta foi consolidada a mais completa por este estudo, contando com a diversidade de bancos de dados compatíveis, tornando a ferramenta mais atraente para vários administradores de rede (Braga, 2011).

O Zabbix possui três partes distintas: servidor Zabbix, Agente Zabbix e Interface Zabbix.

- Servidor Zabbix: faz a coleta dos dados monitorados e os armazena.
- Agente zabbix: este fica responsável por repassar todas as informações já coletadas para o servidor. Ele fica instalado na máquina e quando o servidor faz uma requisição o agente processa a mesma e retorna o que foi solicitado.

- Interface do zabbix: permite a interação e a administração do sistema pelo administrador. Isso permite facilidade no acesso ao monitoramento dos dados e configurar com utilização de browser que já tenha sido instalado no sistema operacional.

5 CONSIDERAÇÕES FINAIS

Nesse trabalho foi proposto um estudo comparativo entre algumas ferramentas de monitoramento e gerenciamento de redes. Durante a elaboração, foi possível identificar os prós e contras de cada uma, e entender quando é interessante utilizar ou não cada uma delas, de acordo com as necessidades de determinado ambiente.

Todas as ferramentas se mostraram boas para o monitoramento, no entanto, é importante ressaltar que a eficiência de cada uma está mais relacionada com as necessidades do ambiente onde ela será implantada, do que com a própria ferramenta. Pois, quando se opta pelo uso de uma ferramenta de monitoramento de redes, é extremamente importante levar em consideração o tipo de problema que se deseja solucionar, quanto à organização está disposta a investir na compra de um software, ou no treinamento de um profissional, a fim de capacitá-lo para lidar com as complexidades da instalação, configuração e manuseio da mesma. A existência de excelentes softwares, tanto livres como pagos, capazes de dar suporte aos administradores de redes, não anula a necessidade de se buscar entender o tipo de problema enfrentado e a forma como a ferramenta será útil, antes de partir para busca da sua solução. O sucesso na implantação de uma ferramenta pode depender de muitos fatores, portanto, a escolha deve ser feita com base na realidade do local onde ocorrerá a implantação. Consequentemente, é de grande importância a análise dos pressupostos anteriormente citados.

Sendo assim, esse trabalho permitiu constatar, de acordo com os requisitos previamente propostos pelo Coordenador de TI, que dentre os softwares estudados, o que mais se aproximou das necessidades do IFMG-SJE, foi o Zabbix. Suas singularidades fizeram com que se destacasse em relação às outras ferramentas.

6 TRABALHOS FUTUROS

O estudo realizado apresentou limitações importantes durante sua elaboração. Tais dificuldades envolveram hardware e software, o que impossibilitou a instalação e configuração da ferramenta, em tempo aceitável para a defesa desse trabalho. A implantação do software dentro da instituição é complemento desse estudo, e poderá trazer melhorias no desempenho da rede e qualidade nos serviços prestados. Diante disso, a implantação do Zabbix no IFMG-SJE fica como uma proposta para trabalhos futuros.

APÊNDICE A- ENTREVISTA COM COORDENADOR DE TI

1) Pergunta: A instituição possui alguma ferramenta de monitoramento?

Resposta: Não é utilizada nenhuma ferramenta por parte da instituição para monitoramento dos equipamentos.

2) Pergunta: A instituição enfrenta algum tipo de dificuldade para monitorar sua rede, já que não faz uso de nenhuma ferramenta que auxilie durante o processo de monitoramento e gerenciamento? Quais são os problemas?

Resposta: Sim, enfrentamos várias dificuldades. Temos problemas na recuperação de erros, há uma demora excessiva em descobrir onde está o problema, sendo que em alguns casos, o ele só é descoberto através da notificação do próprio usuário. Outro problema é a falta de proatividade, não é possível prever os problemas, então ficamos impossibilitados de agir por antecipação, prevenir ou prever os erros.

3) Pergunta: De acordo com as necessidades da instituição, quais os requisitos que uma ferramenta de gerenciamento deveria possuir? Por quê?

Resposta: A ferramenta deve ser livre, porque não é interessante para instituição investir na compra de um software; Deve ser robusta no monitoramento, porque o que mais carecemos nesse momento é de um monitoramento eficiente; Deve ser fácil de utilizar, porque não temos tempo, nem dinheiro para investir no treinamento e capacitação para dos funcionários que irão utilizá-la; Deve possuir facilidade para criação de templates, por questões de praticidade; Deve fazer o monitoramento utilizando o protocolo SNMP, porque é o protocolo que utilizamos nessa instituição.

REFERÊNCIAS

- ANDRADE, Hetty Alves de. **Nagios como solução de monitoramento de rede**. Lavras, 2006.
- ALBUQUERQUE, Fernando. **TCP/IP Internet Protocolos & Tecnologias 3ª edição**, 2001.
- AUGUSTO, Mario Ezequiel. **Avaliação Experimental de Ferramentas para Medição de Largura de Banda**. Curitiba, 2002.
- BALSINI, Camila Martins. **Aplicação de uma ferramenta de monitoramento : Case Centreon**. Curitiba. 2009.
- BLACK, Tomas Lovis. **Comparação de Ferramentas de Gerenciamento de Redes**, Porto Alegre, 2008.
- BONOMO, Esley. **Gerenciamento e monitoração de redes de computadores utilizando-se zabbix**. Lavras. 2006.
- BRAGA, Jeferson de Oliveira. **Estudo sobre o protocolo SNMP e comparativo entre ferramentas**. Curitiba, 2011.
- BUENO, Edmilson Moreira. **Monitoramento de Redes de Computadores com uso de Ferramentas de Software Livre**. 2012.
- CACTI, **Cacti the complete rrdtool-based graphings solution**. 2015.
- Disponível em: <<http://www.cacti.net/>>
- Acesso em: 01 Mai. 2015
- CANDIDO, Wamilson Luiz. **Gerenciamento de Redes**. Paranaguá. 2011.
- CÉLESTIN, Daniel Paula Pessôa. **Customização do monitoramento de links e redes**. Brasília. 2013.
- CORREIA, Marcelo Fernandes. **Gerência de redes**. Uberlândia, 2004.
- DIAS, Henrique de Lima. **A importância do monitoramento de ativos de redes: Um estudo de caso em o sistema Cacic**. Recife, 2008.
- FILHO, Adilson Galiano. **Avaliação da Ferramenta Zabbix**. Curitiba, 2010.
- JUNIOR, Adriano Roberto Vidal. **Monitoramento De Equipamentos Utilizando O Protocolo Snmp**. 2012.
- PINHEIRO, José Mauricio dos Santos. **Gerenciamento de Redes de Computadores**. Versão 2.0, 2002.
- KOCH, Moisés, **Uma proposta de solução de gerenciamento de contabilização utilizando Nagios e Cacti**. Porto Alegre, 2008.
- LEITE, Silvio Luis. **Integrando ferramentas de software livre para gerenciamento e monitoração de redes locais**. Porto Alegre, 2004.

LIMA, Mario. **Zabbix: O Estado da arte em monitoramento**. 2011

LIMA, Thiago Rian do Nascimento. **Monitoramento de Redes de Computadores: Estudo da Ferramenta Zabbix**. Fortaleza. 2014.

LUIZ, Bruno Campos. **Software no Gerenciamento de Redes: Soluções Eficientes e de baixo custo para gerencia de redes**. 2012.

MAJEWSKI, Roberto. **Sistemas de monitoração de rede**. Curitiba. 2009.

MATOS, Leonardo Kolisnik de. **Um processo de gerência para redes de computadores em ambientes de software livre**. Curitiba. 2006.

MATOS, Leonardo Kolisnik de. **Gerenciamento de equipamentos de rede utilizando o software CACTI**. 2009.

MARTAO, Sergei. **Criando um template customizado para o CACTI**. 2015. Disponível em <<http://www.vivaolinux.com.br/artigo/Criando-um-template-customizado-para-o-CACTI?pagina=7>> Acesso em: 10 Dez. 2015.

MARTINS, Ricardo David e LOPES, Rui Diogo. **Estudo de uma Ferramenta de Gestão de Redes**. Portugal. 2003.

MELO, Tiago Maciel. **Monitoramento de redes de médio porte utilizando software livre**. Palhoça. 2007.

MEIER, Adriano Matos. **Cacti alternativa ao Nagios e ao Zabbix**. 2007.

MOQADI, Kanan Ali Abdulla; CONCEIÇÃO DA SILVA, Verônica. **Uso de Ferramentas de Gerência de Rede para Análise de Desempenho de uma Rede Local**. Canoas. 2011.

MRTG. Disponível em <<http://oss.oetiker.ch/mrtg/doc/mrtg.en.html>>

Acesso em: 27 Mai.2015.

NETO, Ariolino Sabóia Dantas; CARNEIRO, Diego Almeida; RIBEIRO, Normando Gomes;

NETO, Arlindo Follador; UCHÔA, Joaquim Quinteiro. **Ferramentas Livres para Monitoração de Servidores**. Lavras. 2015.

OETIKER, Tobias. **RRDTool**. 2005.

PEIXINHO, Ivo de Carvalho; DA FONSECA, Francisco Marmo; LIMA, Francisco Marcelo **Segurança de redes e sistemas**. 2013. versão 2.1.0, Rio de Janeiro.

Qual a importância do monitoramento de redes, 2016. Disponível em <<http://www.opservices.com.br/qual-importancia-monitoramento-de-redes/#>>

Acesso em: 29 Jan.2016.

RIGNEY, Steve. **Planejamento e gerenciamento de redes**. 1ª edição. Editora Campus, 1996. SALVO, Rodrigo. **SNMP- Introdução**.

Disponível em: <<http://www.ti-redes.com/gerenciamento/snmp/intro/>>

Acesso em: 23. Abr. 2015

ROCHA, Ivandro José de Freitas; SERRADOURADA; Marcel Oliveira. 2008. **Gerência de Redes de Computadores Utilizando o Zabbix: Um Estudo de Caso**. Disponível em http://aldeia3.computacao.net/greenstone/collect/trabalho/import/TCC8/Monografia_Ivandro_Marcel_2008-1.pdf

Acesso em 22 Dez. 2015.

SANTOS, Madson da Silva. **Estudo de Gerenciamento da Rede de Distribuição com o Protocolo SNMP e Tutorial para Implantação de Ferramentas de Gerência**. Teresina. 2008.

SANTOS, Sueli Sateles Nascimento Santos. **Monitoramento de redes: análise e configuração do software zabbix. 2015**. Disponível em <http://zabbixbrasil.org/files/TCC_Analise_e_Configuracao_do_Zabbix.pdf> Acesso em 20 Dez.2015.

SANTOS, Cinthia Cardoso dos, **Gerenciamento de redes com utilização de software livre**. Belém. 2015.

SANTOS, Rodrigo Felício dos. **Uma proposta para a melhoria da qualidade de Acesso Remoto à Rede UFLA**. Lavras, 2002.

SIMÕES, João Miguel Baia. **Monitoração automática de redes de computadores**. Lisboa. 2010.

SOARES, Fábio Monteiro; FERNANDES, Rodrigo. **Consolidação das práticas de monitoramento e otimização de projetos de servidores para permitir o crescimento inteligente das organizações a baixos custos**. 2013.

Teleco. **Gerenciamento e Monitoramento de Rede I**. 2015. Disponível em: http://www.teleco.com.br/tutoriais/tutorialgmredes1/pagina_3.asp

Acesso em: 12/03/2015

The Enterprise-class Monitoring Solution for Everyone. 2015. Disponível em <<http://www.zabbix.com/users.php>>

Acesso em: 20 Dez. 2015.

Zabbix Documentation 2.4. 2015. Funcionalidades do Zabbix. Disponível em: <<https://www.zabbix.com/documentation/2.4/pt/manual/introduction/features>>

Acesso em: 03 Mai. 2015.