Comparativo das funcionalidades das ferramentas open-source Zabbix e Cacti

Luzia N. Santos, Henrique P. Martins

Faculdade de Tecnologia de Bauru – Redes de Computadores (FATEC-Bauru)

CEP 17.015-171 – Bauru, SP – Brasil

{luzia.santos4,henrique.martins01}@fatec.sp.gov.br

Abstract. *To manage and monitor networks of business computers, diverse tools are available on the internet. This study has the objective to implement the available tools on the internet in order to conduct a comparative thereof. Those tools have been installed and configured in virtualized environments, where can they also be utilized by administrators of computer networks in non-virtualized environments, since it provides a user friendly interface through web and with diverse graphs, reports, commands and tests for checking health of any computer network. It concludes that the analyzed tools they demonstrated of form efficiently and effectively the goals proposed at work.*

Resumo. *Para gerenciar e monitorar redes de computadores empresariais, diversas ferramentas estão disponíveis na internet. Este estudo tem como objetivo implementar as ferramentas disponíveis na internet, a fim de realizar um comparativo das mesmas. Essas ferramentas foram instaladas e configuradas em ambientes virtualizados, onde pode ser utilizada também por administradores de redes de computadores em ambientes não virtualizados, pois fornece uma interface amigável através da web e com diversos gráficos, relatórios, comandos e testes para verificar a saúde de qualquer rede de computadores. Conclui-se que a ferramentas analisadas demonstraram de forma eficiente e eficaz os objetivos propostos no trabalho.*

1. Introdução

Para gerenciar uma rede de computadores é necessária uma plataforma que tenha um controle unificado dos elementos *hardware*, *software* e ferramenta adequada. O *hardware* pode ser um servidor ou desktop. O servidor coleta dados e armazenada as informações que vem de outros equipamentos que são gerenciadas e analisadas. O desktop e usado pelo usuário e é um elemento gerenciado. O *software* e ferramentas são programa que auxilia no monitoramento e gerenciamento entre servidor e desktop e entre outros equipamentos e dispositivo (Kurose e Ross, 2006).

A *internet* ocupa um espaço importante nas empresas, e com troca de informações interna e externa entre cliente e fornecedores, por isso o *Simple Network Management Protocolo* (SNMP) Protocolo Simples de Gerenciamento de Rede é um protocolo padrão para gerenciamento entre o dispositivo da rede. O grande problema das empresas são a quantidade de colaboradores utilizando a rede ao mesmo tempo, como computadores e impressoras, acesso a *internet* site impróprio e jogos que causa

congestionamento, lentidão e até mesmo paralisa a rede, prejudicando o desempenho da rede. Verificar todos os equipamentos leva tempo, causando prejuízo e gasto atrapalhando o desenvolvimento da empresa.

Gerenciar e monitorar utilizando ferramentas adequadas contribui no desempenho e melhora a disponibilidade da rede, com isso ajuda o administrador de rede a detectar a maior parte dos problemas com antecedência.

Por isso neste trabalho iremos investigar o gerenciamento de redes no ramo empresarial.

Através de implantação de duas ferramentas de monitoramento de redes de computadores utilizando o protocolo SNMP, a fim de verificar suas funcionalidades e compara-las.

Analisar os gráficos e relatórios diversos gerados pelas ferramentas a fim de fazer um comparativo das ferramentas.

2. Redes de Computadores

Segundo Maia (2009), redes de computadores é um conjunto de dispositivos interconectados onde ocorre a troca de informações e compartilha recursos. As empresas utilizam essas redes para trocar informações entre colaboradores, compartilhamento de recursos como impressoras, conexões a outras redes, espaço em disco e processadores.

2.1.1 Protocolos e Modelos de Camadas

Salienta Maia (2009) que os protocolos têm regra definida e compatível, também existem vários protocolos com funções específicas e precisam se comunicar para o processo de comunicação ser efetivo como Taxa de Transferência (V.92), utilizado por modem para conexões discadas; *Point-to-Point Protocol* (PPP), utilizado para conexões ponto-a-ponto; *Internet Protoco* (IP) utilizada para transportar a informação da origem ao destino; *Transmission Control Protocol* (TCP) utilizado para manter a confiabilidade da transmissão; *Yper Text Transfer Protocol* (HTTP), utilizado para transportar páginas da internet.

Segundo Maia (2009), o modelo de camada é dividido em cinco camadas e com funções diferentes e isoladas independente de cada nível, caso ocorra um problema é fácil de corrigir, também pode colocar novas funções sem que as outras camadas sejam afetadas, também existem vantagens comerciais em adquirir o modelo em camadas, principalmente quando tem um modelo padrão a serem seguidas pelo fornecedor da rede, e assim, diferentes empresa podem oferecer soluções para uma ou mais camada de acordo com Figura 1.

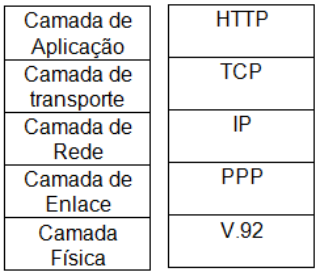

Figura 1 - Modelo de camadas

FONTE: Maia, 2009

2.1.2 Redes Local, Metropolitana e Distribuída

Salienta Tanenbaum (2007) que as redes podem ser classifica conforme a distância física entre os dispositivos que compõe a rede, entre elas a rede *Local Area Network* (LAN) é de redes privadas contidas em um único edifício, podem ser em uma sala ou indústrias, permitindo compartilhamento de recursos, têm um tamanho restritos, seu pior tempo de transmissão é limitado com antecipadamente, a velocidade é de 10 Mbps a 100Mbps, taxa de transmissão é de 10 Gbps e menor custo.

A rede *Metropolitan Area Network* (MAN) é interligada dentro da cidade, a taxa de transmissão é alta, com menor taxa de erro, também é padronizada pelo IEEE 802 e *American National Standards Institute* (ANSI) e existem outras mais conhecidas são *Distributed Queue Dual Bus* (DQDB), *Fiber Distributed Data Interface* (FDDI) e a TV a cabo. A rede distribuída *Wide Area Network* (WAN) são dispositivos interligados entre cidades estados e países e sua velocidade é de Kbps ou Mbps e podem chegar à taxa de Gbps (Maia, 2009).

2.1.3 Topologias de Rede

Segundo Maia (2009), as topologias de uma rede define entre dois dispositivos interligados um ao outro e é classificada em ponto a ponto, tem a conexão dedicada é quando um ponto e ligado a ao outro dispositivo sem a ajuda de outro compartilhamento físico para comunicar, também tem a rede multiponto que é compartilhado entre todos os dispositivo da rede.

Para Torres (2013) na topologia totalmente conectada os computadores tem a conexão individual, por isso eles conversão diretamente, caso ocorrer falhas entre os computadores podendo mudar de rota, maior nível de redundância e é inviável por ter que utilizar muito cabos.

A topologia em anel é utilizada em concentradores que cria internamente um anel e as arquiteturas *Token Ring* e FDDI, utilizam dois anéis em sentido contrario, com redundância, caso o anel principal falhar o secundário entra em ação (Torres, 2013).

Salienta Torres (2013) que a topologia estrela e os dispositivos ficam ligados em um concentrador, todos os dispositivos que quiserem comunicar entre eles têm que enviar uma mensagem para a central e depois retransmitir aos demais, caso um cabo romper a rede continua funcionando, o problema só vai ficar no computador que ocorrer a falha.

Segundo Maia (2009) na topologia hierárquica existe uma hierarquia que organiza os dispositivos, a vantagem é que tem vários concentradores podendo expandir a rede, também é possível distribuir pontos de falhas devido à quantidade de concentradores, ganha no desempenho por ter vários concentradores dividindo o trafego da rede.

Topologia distribuída também existe caminhos alternativos entre vários dispositivos, oferece boa disponibilidade e escalabilidade, tendo uma boa relação custo-desempenho, e por isso que a topologia é utilizada em redes do tipo WAN. Na internet é conhecido por comutação por pacotes e os responsáveis são os roteadores (Maia, 2009).

Para Maia (2009) a topologia barra tem um barramento onde são compartilhados os dispositivos tanto para enviar quanto para receber mensagens, baixo custo, fácil de instalar, as desvantagens são quando romper o barramento e todos os dispositivos não funcionar, é limitado à instalação com muitos dispositivos, diminuindo o desempenho.

2.2. Gerenciamento de Redes de Computadores

De acordo com Tanenbaum (2007) as empresas têm números significativos de computadores, um independente do outro, trabalhando de forma diferente para monitorar a produção, controlar estoque, elaborar folha de pagamento e o compartilhamento de recurso tem por objetivo que todos os programas como equipamentos e dados chegam ao alcance de todas independentemente da localização física do recurso e do usuário, por exemplo, a impressora não dever ser individual e sim uma impressora para todos os computadores.

2.3 Conceitos de Gerenciamento em Redes de Computadores

Segundo Kurose e Ross (2006), o gerenciamento da rede inclui o oferecimento, a interação e a coordenação de elementos de *hardware*, *software* e humanos, para monitorar, testar consultar, configurar, analisar, avaliar e controlar os recursos da rede muito antes de gerenciar uma rede já resolvia com teste ping ou reiniciava um *software* ou *hardware*. A internet púbica e privada cresceram e se transformam de pequenas redes em grandes infraestruturas globais, e com necessidade de gerenciar enorme quantidade de componentes de hardware e software.

No gerenciamento e importante utilizar ferramentas adequadas como a detecção de falhas em uma placa de interface em um hospedeiro ou roteador; Monitoração de hospedeiro, caso ocorra falhas; Monitoração de trafego para auxiliar o oferecimento de recurso, segmentação de LAN; Detecção de mudanças rápidas em tabelas de roteamento; Monitoramento *Service Leve Agreements* (SLAs) Acordos de Nível de Serviço são contratos que define parâmetros e desempenho do provedor da rede; Detecção de intrusos de ataques à segurança (Kurose e Ross, 2006).

Segundo Kurose e Ross (2006), a International Organization Standardization (ISO) modelo de gerenciamento de rede determina cinco áreas como o gerenciamento de desempenho de diferentes componentes da rede; Gerenciamento de Falhas; Gerenciamento de Configuração do hardware e software; Gerenciamento de contabilização, controlando o acesso de usuário e dispositivo da rede; Gerenciamento de segurança, restringindo a política definida e temos o firewall para controlar o trafego da rede.

A infraestrutura da rede tem com o intuito de monitorar, testar consultar, configurar, analisar avaliar os elementos da rede. Para que o responsável possa coletar os dados, monitorar, fazer acessar remotamente, controlar filiais, protocolo de comunicação, transporta relatórios e dados pessoais, mede quantidade de atividades, produtividade e orçamentos (Kurose e Ross, 2006).

Para Kurose e Ross (2006) são utilizados três tipos de componentes da arquitetura. A entidade gerenciadora que tem um responsável para gerencia a estação central *Network Operations Center* (NOC) Centro de Operações de Rede que verifica todos os computadores e dispositivos gerenciados, controlando e coletando os processamentos e análise das informações. Dispositivo gerenciado é um *hardware* com *software* de uma estação que inclui o roteador, hospedeiro, fonte, hub, impressora e modem, as partes internas do hardware contem placa de interface de rede e conjunto de parâmetros de configuração para as peças de *hardware* e *software*, também um protocolo de roteamento, intradomínio, como o *Routing Information Protocol* (RIP) protocolo de roteamento vetor de distância e *Management Information Base* (MIB) Base de Informações de Dados. Protocolo de gerenciamento de rede é executado para buscar informações nos agentes, utilizando o protocolo (SNMP) para gerenciar e transmitir as informações solicitadas pela gerencia.

2.4. Gerenciamento de Rede SNMP e Gerentes e Agentes

Para Forouzan (2008) os componentes do SNMP é uma estrutura de gerenciamento entre dispositivo por uma equipe monitorada via internet, também é um protocolo responsável para transmitir informações através de pacotes entre gerente e agente. A estação gerenciadora é chamada de gerente e pode ser um host e executada por um agente SNMP, verifica periodicamente valores e os dados vindos do agente. O agente pode ser um host e ou roteador é gerenciado por um gerente SNMP, que mantém informações no banco de dados, também auxilia no gerenciamento através de uma resposta Trap para o gerente (Figura 2).

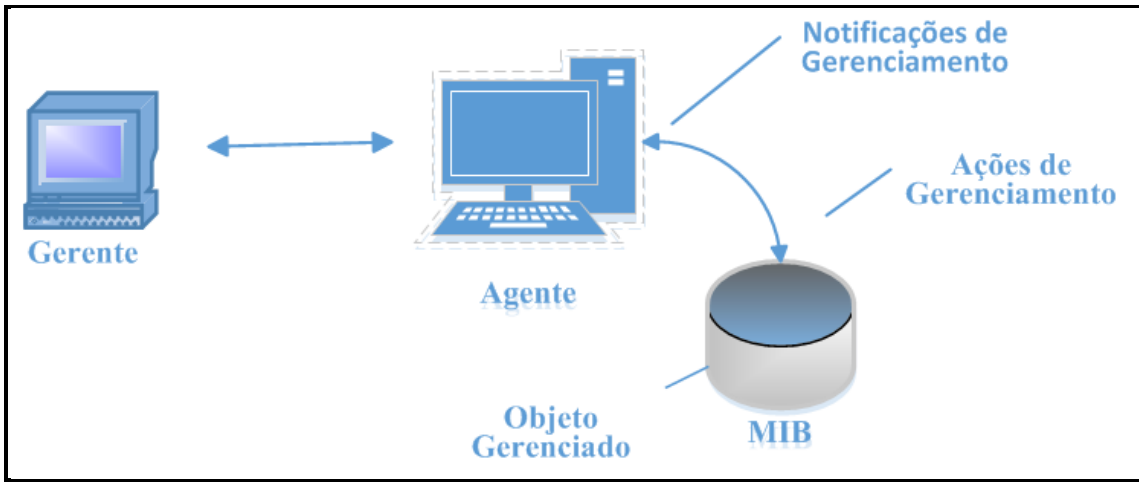

Figura 2 - Conceito Simple Network Management Protocolo (SNMP)

FONTE: Adaptado, Forouzan, 2008

2.4.1 Componente do SNMP *Structureof Management Information* (SMI) e MIB

Para executar tarefas no SNMP são utilizados SMI e MIB. A SMI é um componente para gerenciamento da rede com funções de nomear objetos, o nome é único; Declarar tipos de dados, um subconjunto com um superconjunto de *Abstract Syntax Notation* (ASN.1) com categoria simples extraídos direto da ASN.1 e a estrutura combinando tipos de dados; Método codificado tem padrão *Basic Encoding Rules* (BER), específica que esta sendo codificado em formato de trinca como o Tar declara tipo de dados. O comprimento declara dado. O valor codifica valor conforme a regra BER (Forouzan, 2008).

Segundo Kurose e Ross (2006), a MIB guarda objetos gerenciados, cujos valores, coletivamente, esses valores são gerenciados pela entidade gerenciado através do envio de uma mensagem SNMP, sendo que o agente fica em um dispositivo que por sinal quem gerencia e a entidade gerenciadora, o objeto utiliza o OBJET-TYPE do SMI que se agrupa em módulos MIB que utiliza MODULE-EDENTITY. Os objetos são nomeados hierarquicamente, um programa baseado na web, que percorre a rede identificando os objetos.

O componente MIB tem por função que cada agente tem uma MIB2 (versão 2) e varias objetos para o gerente gerenciar, e são classificadas sob dez grupos: sistema; interface; tradução de endereço; ip; Internet *Control Message Protocol* (icmp); tcp; *User Datagram Protoco* (udp); *Expert Group on Development Issues* (egp); transmissão; snmp e esses grupos estão sob os MIB2 na arvore de identificação e cada grupo tem variável ou tabelas definida. Acessar a MIB tem que usar um grupo UDP protocolo simples da camada e existem quatro tipos de variáveis simples, e sequência de tabela, e para acessar uma variável simples utiliza a Identidade do grupo *udpInDatagrams, udpNoPorts, udpErros e udpOutDatagrams*, e também tem sequência de tabela com uma identidade da tabela *udpEntry* (Forouzan, 2008).

2.4.2 Protocolo SNMP

Segundo Kurose e Ross (2006), o SNMPv2 é utilizada para transportar a MIB entre as entidades. A utilização mais comum é a modo comando resposta, a entidade gerenciadora envia uma requisição ao agente que recebe é enviar uma resposta de requisição, geralmente e para consultar ou modificar um valor na MIB, também existe um segundo envio de mensagem que é o a mensagem trap, o agente envia uma mensagem a entidade gerenciadora para uma eventual mudança na MIB.

O SNMPv3 define oito tipos de *Professional Development Unit* (PDUs) Unidade de Desenvolvimento Profissional como *GetRequest*, *GetNexRequest, GetBulkRequest, SetRequest, Response, Trap, InformRequest e Report*. O formato *GetBulkRequest* tem diferença em duas áreas, uma o valor do status zera o erro de todas as mensagens *GetBulkRequest*e a outra o campo do status de erro substituiu por um campo não repetidor e substitui pelo campo máximo de *GetBulkReque.* Os campos são dos tipos de PDU que identidade o pedido, status de erros e não repetidores. Essas PDU incorpora a mensagem no Snmpv3 e é constituída da versão que define a versão atual e o cabeçalho identifica a mensagem. O parâmetro de segurança compila a mensagem e criptografa, caso não criptografar ele baseia na PDU utilizando o serviço UDP em duas portas 161 e 162. As versão SNMPv2 e SNMPv3 é mais segura, SNMPv3 tem dois tipos de

segurança geral e especifica, fornece autenticação de mensagem e privacidade e autorização do gerente (Forouzan, 2008).

3. Ferramentas de Gerenciamento de Redes

As ferramentas de gerenciamento de redes são necessárias e importantes para atividades de gerenciamento das redes e monitoramento, detecta erro antes mesmo de acontecer. Existem diversas ferramentas para todas as finalidades como ferramentas acoplado no sistema operacional da rede e as plataformas oferecem aplicações de monitoramento e controle da rede.

3.1 Zabbix

Zabbix é o software de nível empresarial final projetado para disponibilidade e desempenho de componentes de infraestrutura de tecnologia da informação de monitoramento, e é *open-source* e sem custo (Zabbix, 2015).

O Zabbix é possível ser virtualizado em tempo real e monitorado com dezenas e milhares de servidores, maquina virtual e dispositivo da rede simultaneamente, podendo armazenar dados e recursos de visualização como (descritivos, mapas, gráficos, telas, etc.) com flexibilidade em analisa dos dados e com alertas. Oferece coletas de dados e escalonados em ambiente muito grande. Com monitoramento distribuído estão disponíveis com o uso de proxies Zabbix (Zabbix, 2015).

Segundo Adilson (2010) o Zabbix coleta informações de todos os dispositivos que estão interligados na rede, por meio de scripts, através do agente Zabbix e até mesmo o protocolo SNMP. A interface é baseada na web, autenticação e permissão segura do usuário.

Polling e aprisionamento são suportados, com agentes de alto desempenho nativas de coleta de dados de qualquer sistema operacional; métodos de monitoramento sem agentes também estão disponíveis. Monitoramento Web, máquinas virtuais VMware é possível identificar automaticamente os servidores e dispositivos de rede, bem como realizar a descoberta de baixo nível com os métodos de atribuição automática de desempenho e disponibilidade cheques às entidades descobertos (Zabbix, 2015).

3.2. Cacti

Para Costa (2006) o Cacti é uma ferramenta que possibilita coleta e exibe informações sobre a saúde de uma rede de computadores através de gráficos e foi desenvolvido para ser maleável e com facilidade de ser adaptado a diversas necessidades, ele é poderoso e fácil de usar.

Segundo Eduardo (2009) o Cacti verifica a condição dos elementos de um programa assim como a largura de banda utilizada e o uso da CPU e também mostra uma interface e uma infraestrutura para RRDIool, que responsável por armazenar dados recolhidos que são gerados dos gráficos.

Cacti é uma ferramenta que repassa a informações através de scripts ou outro programa que o usuário escolhe que fica responsável de obter dados. Com a ajuda do Protocolo SNMP consulta informações em elementos de redes e sua arquitetura prevê e facilita a expansão através de plugins que adicionam novas funcionalidades, o *Personal Home Page* (PHP) que visualiza o mapa da rede (Costa, 2006).

4. Materiais e Métodos

Para alcançar o objetivo proposto foram realizados inicialmente pesquisas bibliográficas em diversas bases de conhecimento como internet, livros e artigos a fim de abordar os temas de gerenciamento e monitoramento de redes, em seguida foram analisadas e testadas às ferramentas Cacti e Zabbix com o intuito de fazer um comparativo das mesmas.

Para simular um ambiente de monitoramento foram utilizadas seis máquinas virtuais sendo que três maquinas foram utilizada no cacti um Server_AD, um Server_AG1 e um Wind7_AG2 e três maquinas foram utilizada no Zabbix foram utilizado um Server_AD, um Server_AG1 e um Wind7_AG2 e assim foi realizada a instalação dos softwares Cacti e Zabbix, sendo que o primeiro passo foi realizar o download dos pacotes de instalação pela internet, e o segundo passo foi a configurações dos softwares. Vale ressaltar que no software Zabbix foi utilizado o mesmo procedimento que o Cacti com uma diferença, foi instalado no Server_AG1 o Agente Zabbix ao invés do pacote do SNMPv3.

Para implementar as ferramentas Zabbix e Cacti foi utilizado um notebook com placa processador Intel Core i5 6GB de memória RAM, disco rígido de 750 Gb, com Windows 7 Home Premium 64 bits como Sistema Operacional. Para simular os ambientes de gerenciamento, foi utilizado o software Oracle VM Virtual Box, onde foram instalados o Microsoft Windows 7 e o Linux Ubuntu Versão 12.

De acordo com a Figura 3 pode-se observar a topologia do ambiente que foi montado para realização os testes das ferramentas de gerenciamento. Foi utilizado dois Server para a entidade gerenciadora, dois Server para agente e dois Windows 7 para agente.

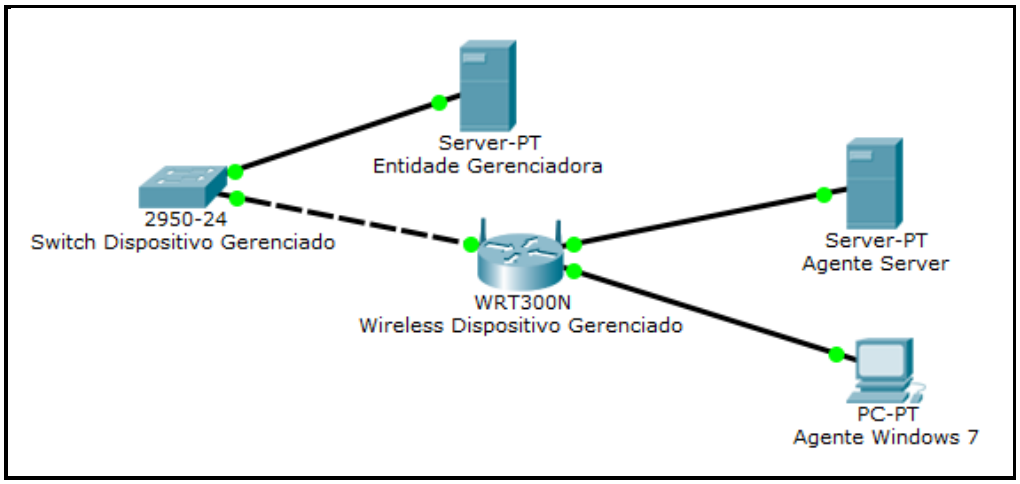

Figura 3. Topologia do ambiente da pesquisa

Fonte: Elaborada pelo Autora, 2015

5. Resultados Obtidos

5.1 Zabbix

Para executar o Zabbix é necessário utilizar um browser, e em seguida digitar o caminho para acessar a pagina (http://192.168.56.102/zabbix/), após aberta a primeira pagina tela login é solicitado o usuário e senha. Depois de autenticado é aberta a tela inicial com todas as opções da ferramenta e a partir da tela inicial é possível navegar por todo o ambiente da ferramenta Zabbix. Na aba monitoramento apresenta o painel que mostra o monitoramento resumido de todo o sistema; Visão geral mostra o monitoramento mais detalhado; Monitora a pagina da Web; Dados mais recentes são as ultimas ocorrência de falhas; Triggers é um alerta de nível critico; Os eventos são as informações das falhas; Os gráficos são as informações contidas nos hosts em forma de gráficos. A tela e mapa mostra o servidor Zabbix. Inventario é uma visão geral dos hosts. Relatório e Status do Zabbix apresentam se o servidor esta em execução; Numero de hosts (monitorando / não monitorado/ modelos); Números de itens (monitorado/ desabilitado/ não suportado); Números de triggers (Habilitado/ desabilitado) [problemas/ ok]; Números de usuário (online); Desempenho do servidor valores por segundo. Configuração cria e configura host, grupo de hosts, período de manutenção; ações reladas das falhas, tamanho da tela, apresentação de slides e o mapa da rede. Administração configura o proxies, usuário, tipo de mídia, scripts, autenticação da parte interna do zabbix; Auditoria filtra o administrador e usuário; A fila monitora elementos por minutos e segundos; Notifica diariamente, semanal, mensal e anual conforme a Figura 4.

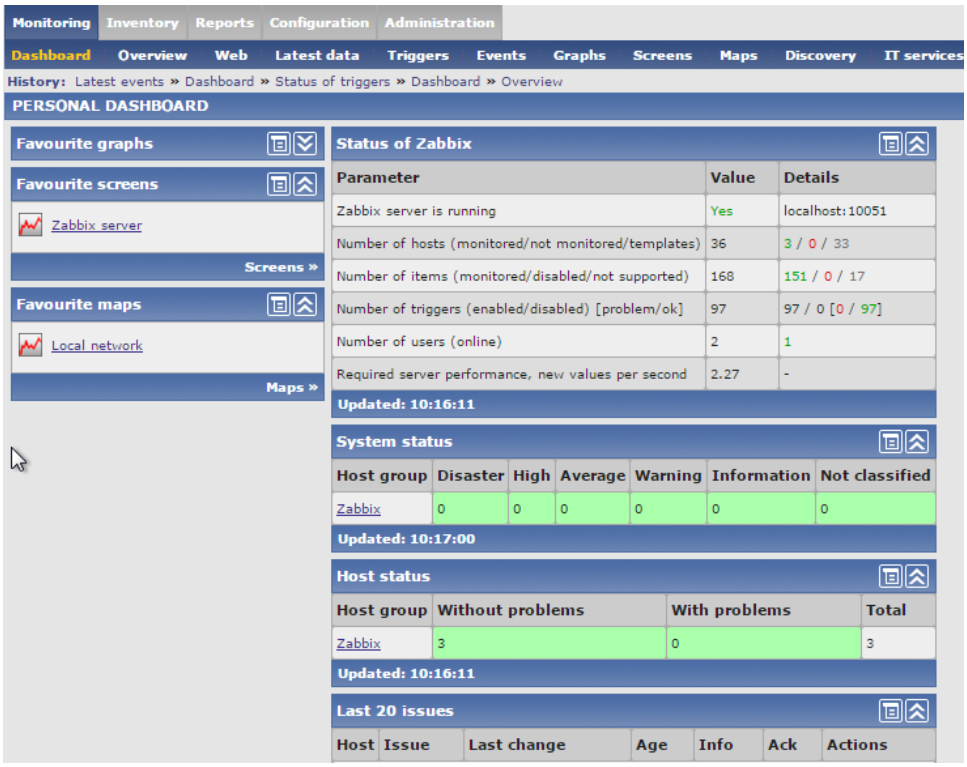

Figura 4. Tela monitoramento geral

Fonte: Elaborado pelo próprio autor, 2015

De acordo com a Figura 5 é possível criar e configurar os dispositivos que se pretende gerenciar como host, aplicações, item, triggers, gráficos, descoberta, Web, interface e templates, status e disponibilidade.

Figura 5. Configuração de host

Fonte: Elaborado pelo próprio autor, 2015

Uma das opções de gerenciamento da ferramenta Zabbix é a opção *Monitoring graphs* onde é possível escolher a informação que se pretende monitorar, de acordo com a Figura 6 é possível observar uma das opções existentes que no caso é a utilização da CPU (Server_AD - CPU *utilization*), ainda na Figura 6 é possível observar diversas informações que auxiliam no monitoramento como por exemplo: idle time (tempo ocioso), user time (tempo do usuário), system time (tempo do sistema), oiwiat time (tempo de entrada e saída), nice time (tempo livre), Interrupt (tempo de interrupção), softirq time (tempo dos softwares de interrupções), steal time (tempo perdido). Este gráfico foi monitorado por uma hora e com o ultimo valores, mínimo, media e máximo.

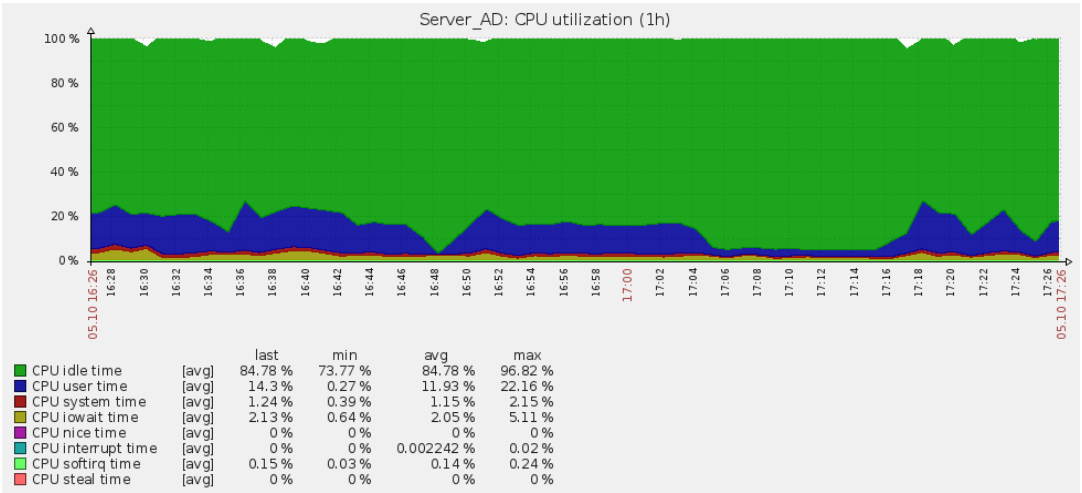

Figura 6. Gráfico do Server_AD - CPU Utilization

Fonte: Elaborado pelo próprio autor, 2015

De acordo com a Figura 7 é possível observar a utilização de jumps da CPU (Server_AG1 CPU jumps) e as informações que são disponíveis para análise do gráfico que são context wiches per second (alternâncias de contexto por segundo) e intrrupts per second (interrupção por segundo). Este gráfico foi coleta informações de uma hora e

monitorado num tempo aproximado de quarenta minutos e com o ultimo valores, mínimo, media e máximo.

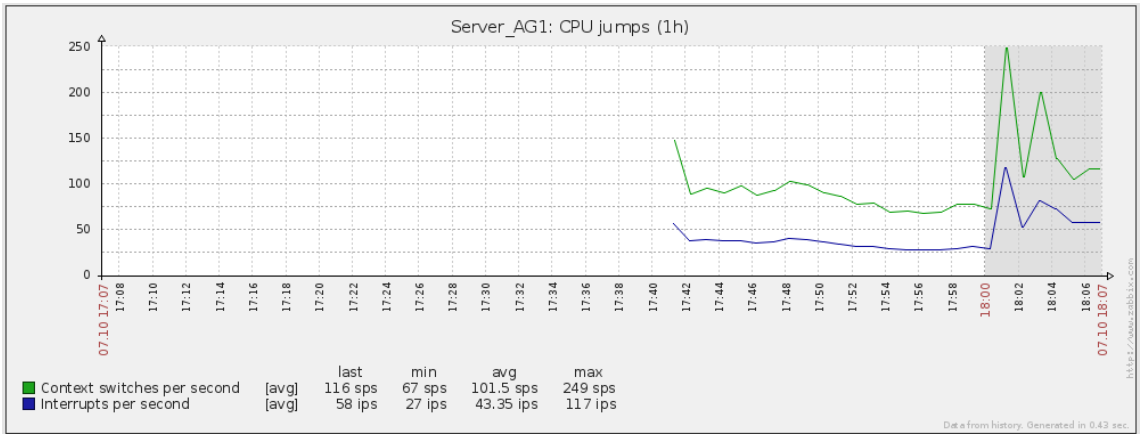

Figura 7. Gráfico do Server_AG1 CPU jumps

Fonte: Elaborado pelo próprio autor, 2015

Já na Figura 8 é possível observar o tráfico de Rede (Wind7AG2 Network traffic), no caso está sendo monitorada a placa de rede eth2 do servidor. As informações que são disponibilizadas para análise são incoming network traffic (entrada do trafego da rede) e outgoing (saída do trafego da rede). Este gráfico coleta informações de uma hora e foi monitorado num tempo aproximado de quarenta minutos e com o ultimo valores, mínimo, media e máximo.

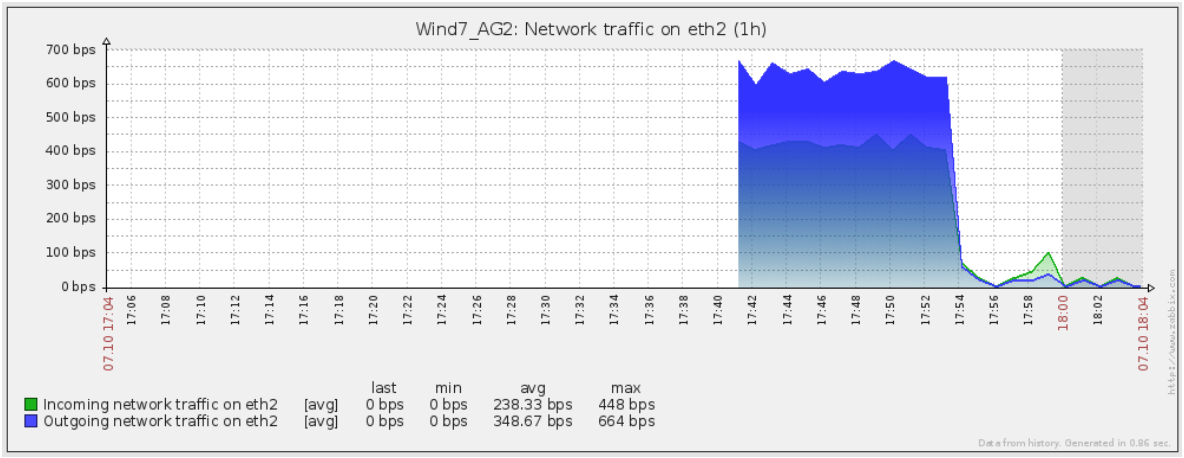

Figura 8. Gráfico do Wind7_AG2 Network traffic on eth2

Fonte: Elaborado pelo próprio autor, 2015

5.2 Cacti

O Cacti precisa ser executado por um navegador e em seguida digitar o caminho para acessar a pagina (http://192.168.0.1/cacti/), após ser instalado e autenticado o usuário e senha é possível entrar na tela inicial onde é possível realizar a navegação por toda a ferramenta a partir dela. No console é criado os dispositivos, gráficos e verifica novos gráficos; Gerencia gráfico, arvore de gráficos, fontes de dados e dispositivos. Método de

recolha onde consulta os dados e métodos de entrada de dados. Templates de gráficos, templates de acolhimento, templates de dados. Configuração configura o caminho, gráfico de exportação e autenticação. Utilitário, temos o suporte técnico, permissão para o usuário, SNMP para uma versão mais atual e reconstrói o original conforme a Figura 9.

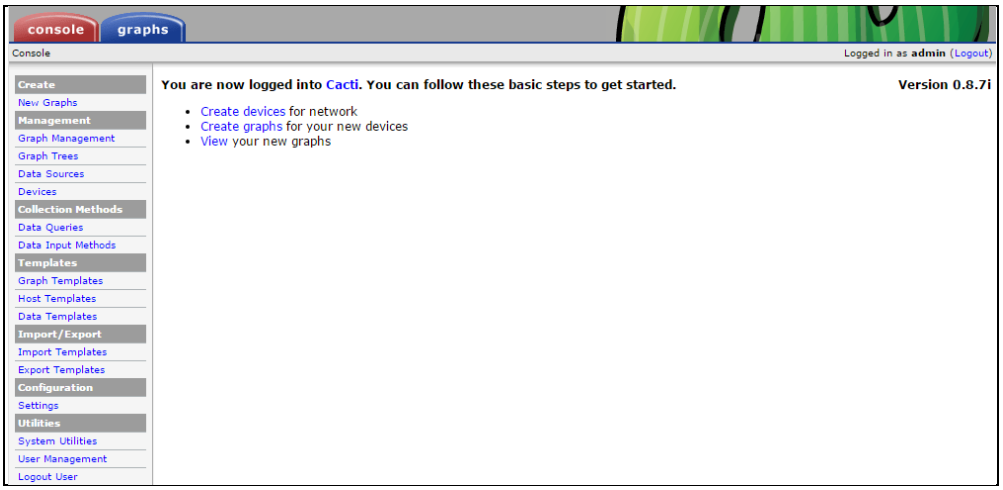

Figura 9. Disponibilidades e funcionalidade

Fonte: Elaborado pelo próprio autor, 2015

Na opção *Console Devices* é possível realizar as configurações dos computadores que se pretende monitorar pela ferramenta, e é possível observar alguns dados iniciais como: fontes de dados, estado da maquina, estado, ip, atuais (ms), media (ms) e disponibilidade Figura 10.

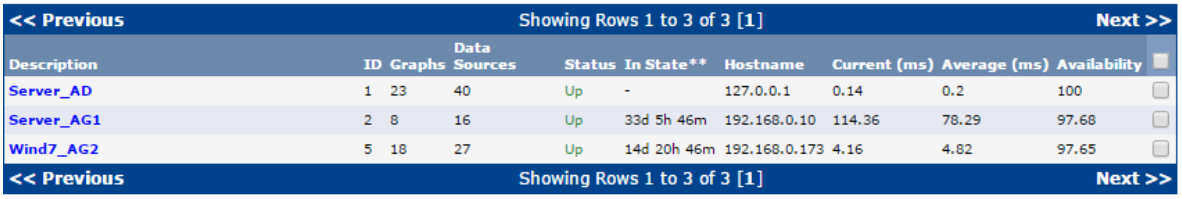

Figura 10. Dispositivos da rede entre Server_AD, Server_AG1 e Wind7_AG2.

Fonte: Elaborado pelo próprio autor, 2015

Na opção *Graphic Preview Mode* é possível verificar os gráficos de monitoramento dos computadores. Conforme a Figura 11 é possível observar o Load Average do computador que está sendo monitorado. Uma media de 1, 5 e 15 minutos com um valor atual. Este gráfico coleta informações num período de 24 horas e é atualizado a cada 5 minutos e foi monitorado mais ou menos um período de 1 hora e vinte minutos.

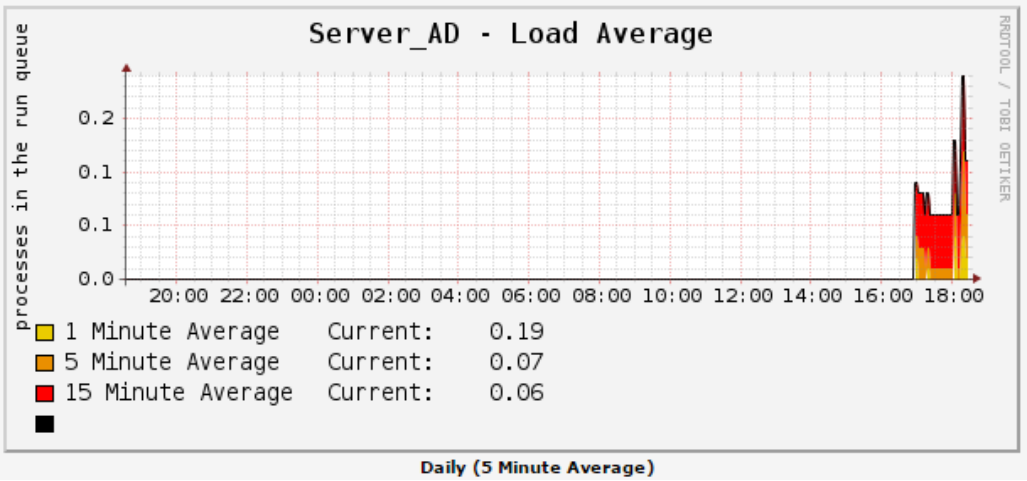

Figura 11. Gráfico do Server_AD - Load Average

Fonte: Elaborado pelo próprio autor, 2015

Já na Figura 12 é possível monitorar os processos que estão rodando no servidor monitorado. Este gráfico coleta informações num período de 24 horas e é atualizado a cada 5 minutos, também foi monitorado mais ou menos um período de 2 horas e quarenta minutos e com um valor atual, media e máximo.

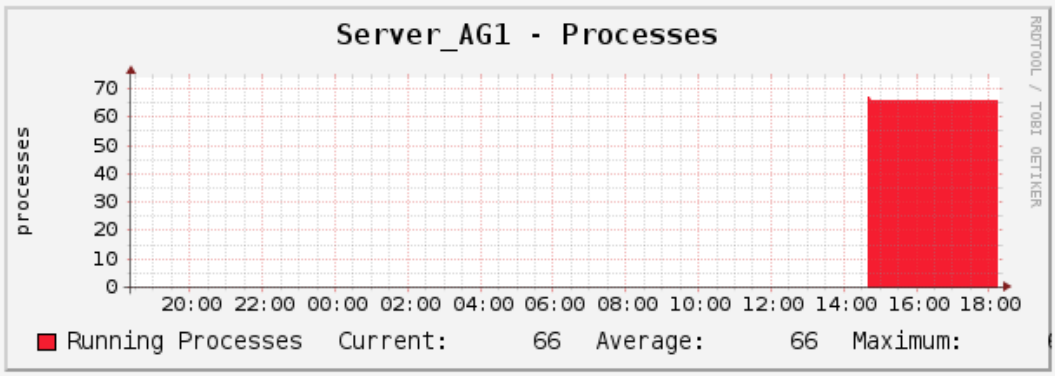

Figura 12. Gráfico do Server_AG1 - Processes

Fonte: Elaborado pelo próprio autor, 2015

Na Figura 13 é possível observar a latência de Ping de uma máquina que está sendo monitorada. Neste gráfico foi coleta informações num período de 24 horas e é atualizado a cada 5 minutos, também foi monitorado mais ou menos um período de 1 hora e trinta minutos e com um valor atual, média e máximo.

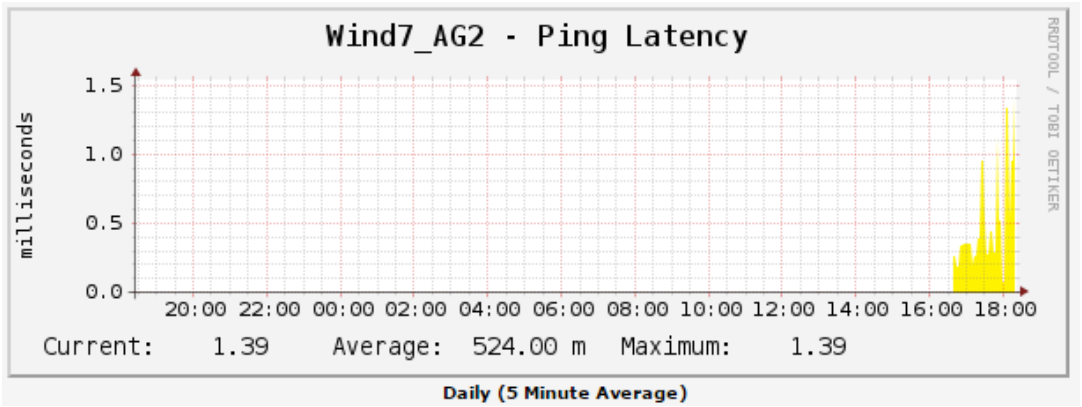

Figura 13. Gráfico do Wind7_AG2 Ping Latency

Fonte: Elaborado pelo próprio autor, 2015

Na Tabela 1 podem-se observar os recursos de funcionalidades das ferramentas de todas as seis maquinas utilizada na pesquisa. As ferramentas cacti continham 49 gráficos, mas somente 14 gráficos continham informações adequadas para o analise. O zabbix continham 26 gráficos e foram analisados 26 gráficos.

Tabela 1. Comparativo de funcionalidades.

Cacti	Zabbix
CPU usage (AD)	CPU jumps (AD/AG1)
CPU utilization (AD)	CPU load (AD/AG1/AG2)
Load usage (AG1)	CPU utilization (AD/AG1)
Load averge (AD/AG1)	Disk space usage (AD/AG1/AG2)
Logged in users (AD/AG2/AG2)	Memory usage (AD/AG1/AG2)
Memory usage (AD/AG2)	Network traffic on eth0 (AD/AG1/AG2)
Ping Latency (AD/AG1/AG2)	Network traffic on eth2 (AD/AG1/AG2)
Traffic (bits/sec) (AG2)	Swap usage (AD/AG1)
	Value cache effectiveness (AD)
	Zabbix cache usage, % free (AD)
	Zabbix data gathering process busy % (AD)
	Zabbix internal process busy % (AD)
	Zabbix server performance (AD)

Fonte: Elaborado pelo próprio autor, 2015

Na Tabela 2, apresenta uma comparação dos recursos disponíveis em cada ferramenta, coletado durante os testes nas ferramentas Cacti e Zabbix.

Tabela 2. Comparativo de funcionalidades.

Funcionalidade	Cacti	Zabbix
CPU jumps	Não	Sim
CPU load	Sim	Não
CPU usage	Sim	Não
CPU utilization	Sim	Sim
Disk space usage	Não	Sim
Load averge	Sim	Não
Load usage	Sim	Não
Logged in users	Sim	Não
Memory usage	Sim	Sim
Network traffic on eth0	Não	Sim
Network traffic on eth2	Não	Sim
Ping Latency	Sim	Não
Swap usage	Não	Sim
Traffic (bits/sec)	Sim	Não
Value cache effectiveness	Não	Sim
Zabbix cache usage, % free	Não	Sim
Zabbix data gathering process busy %	Não	Sim
Zabbix internal process busy %	Não	Sim
Zabbix server performance	Não	Sim

Fonte: Elaborado pelo próprio autor, 2015

6. Conclusão

As ferramentas implantadas e configuradas comprova ser eficiente e eficaz aos objetivos apresentado no trabalho. Analise e testes podem ser utilizados por administradores de empresas, universitários e aos interessados na área de redes de computadores, as informações ajudam na verificação ativas dos dispositivos e componentes, estados das maquinas, configuração do equipamento. Com os resultados obtidos através de análises e testes, pode-se concluir que as informações contidas nas ferramentas ajudam a obter uma boa visualização e um melhor desempenho da rede analisada.

No mercado existem inúmeras ferramentas de gerenciamento e monitoramento de redes de computadores que proporciona aos administradores de redes verificação ativas dos dispositivos e componentes, analisar e testar relatórios, gráficos e comando que ajudam a garantir o funcionamento de rede de computadores.

Para auxiliar as atividades do profissional na área de tecnologia de redes de computadores tais como administradores docentes e universitários, foram instaladas e configuradas as ferramentas Zabbix e Cacti sendo que as ferramentas são *open-source* e sem custo. Após as analise e testes executados pode-se concluir que o Zabbix tem uma boa visualização e mostras às falhas com mais precisão, mais opções de gráficos em funcionamento e com mais recursos de utilização. O Cacti tem uma visualização

simples, menos gráficos que auxiliam no monitoramento e com menos recursos. Como trabalhos futuros, pode-se acrescentar mais algumas funções e ferramentas como a utilização e configurações web, assim como criar mais gráficos, templates bem como a implementação de mais agentes.

Referências

Adilson G. Filho, Jhonatan Geremias (2010) "Avaliação da Ferramenta Zabbix". Curitiba: Pontifícia Universidade Católica do Paraná.

Costa, F. (2008) "Ambiente de Redes e Monitoramento com Nagios e Cacti". Rio de Janeiro: Ciência Moderna LTDA.

Eduardo P. Pereira, Rodrigo C. Moura (2009) "Estudos da ferramenta cacti, para análise de desempenho de rede". Pelotas: Centro Politécnico - Universidade Católica de Pelotas (UCPel).

Forouzan, B. A. (2009) "Protocolo TCP/IP". São Paulo: McGaw-Hill, 3 edição.

Kurose, J. F. e Ross. K. W. (2006) "Redes de Computadores e a Internet". São Paulo: Pearson Adilson Wesley, 5º edição.

Maia, L. P. (2009) "Arquitetura de Redes de Computadores"**.** Rio de Janeiro: LTC - Livro Técnico e Científica Editora SA.

Tanenbaum, A. S. (2007) "Redes de Computadores". Holanda: Campus, 4 edição.

Torres, G. (2013) "Redes de Computadores". Rio de Janeiro: Novaterra Editora e Distribuidora LTDA.

Zabbix "The Enterprise-class Monitoring Solution for Everyne" http://www.zabbix.com, Out.