

Análise dos recursos dos softwares livres Cacti e Nagios que utilizam o protocolo SNMP para Gerenciamento de Redes

Gustavo Martineli Sanches, André Luiz Ferraz Castro, Elvio Gilberto da Silva, Henrique Pachioni Martins

Centro de Ciências Exatas e Sociais Aplicadas
Universidade Sagrado Coração (USC) – Bauru, SP – Brasil

gustavo.sanches@usc.br, andre.castro@usc.br, egsilva@usc.br,
henrique.martins@usc.br

***Resumo.** A evolução tecnológica provoca um grande impacto na sociedade atualmente. A informação tem-se tornado objeto de significativa vantagem competitiva entre as empresas em seus investimentos; e é com base nisto que as redes de computadores estão em crescimento contínuo. Conseqüentemente é necessária a adoção de ferramentas automatizadas para a sua monitoração e controle. Diante de tais fatos, este trabalho tem como objetivo realizar uma análise de dois softwares livres (Nagios e Cacti) baseados no protocolo SNMP para gerenciamento de redes, identificando os recursos oferecidos por ambos além de proporcionar uma visão mais detalhada e permitir uma base de escolha para administradores de rede.*

***Abstract.** The technological progress causes a large impact on society today. Information has become an object of significant competitive advantage between companies in their investments, and on this basis is that computer networks are constantly growing. Consequently, the adoption of automated tools for its monitoring and control were necessary. Faced with such facts, this research aims to conduct an analysis of two free softwares (Nagios and Cacti) based on SNMP protocol for network management, identifying the features offered by both in addition to providing a more detailed view and allow a base of choice for network administrators.*

1. Introdução

Na visão de Santos (2005), os avanços tecnológicos exercem hoje um grande impacto na sociedade. A informação tem-se tornado cada vez mais uma vantagem competitiva para as empresas e organizações em investimentos futuros. O fato é que, cada vez mais, as empresas, para se tornarem competitivas e sobreviverem no mercado, têm investido em tecnologia de informação, como a única forma de tornar seguro o processo decisório. E é nesse quadro que as redes de computadores se proliferam, encurtando as distâncias e diminuindo o tempo de resposta entre as transações de organizações por todo o mundo.

Santos (2005) ainda afirma que em decorrência das vantagens que as redes de computadores oferecem, o número e a extensão dessas estão em expansão contínua. À medida que as redes crescem em escala e extensão, dois fatores vão ficando mais evidentes: as redes, juntamente com seus recursos e aplicações, tornam-se cada vez mais indispensáveis para as organizações que as utilizam, e uma maior possibilidade de ocorrerem problemas, o que pode levar as redes a um estado de inoperância ou a níveis

inaceitáveis de desempenho.

Para controlar tudo isso, surgiu o conceito de gerencia de redes, que visa maximizar sua eficiência e produtividade. A fim de garantir certa qualidade dos serviços a seus usuários, é que as redes de computadores devem ser gerenciadas. Este gerenciamento envolve o monitoramento e o controle de recursos distribuídos com o objetivo de assegurar que sistemas de informação estejam operacionais e eficazes a todo instante.

Com esta crescente necessidade de gerenciamento, fez-se necessário que padrões para ferramentas fossem estabelecidos e, em resposta a esta necessidade surgiu o padrão SNMP.

Conforme lembra Santos (2005), o gerenciamento da rede realizado pelo protocolo Simple Network Management Protocol (SNMP), permite que uma ou mais máquinas na rede sejam designadas gerentes da rede. Esta máquina recebe informações de todas as outras máquinas, chamadas agentes, e através do processamento destas informações pode gerenciar toda a rede e detectar facilmente problemas ocorridos.

Conseqüentemente o gerenciamento não pode ser realizado somente pelo esforço humano, ou seja, é necessária a adoção de ferramentas automatizadas para a sua monitoração e controle.

Diante de tais fatos, este trabalho tem como objetivo realizar uma análise de dois softwares livres (Nagios e Cacti) baseados no protocolo SNMP para gerenciamento de redes, identificando os recursos oferecidos por ambos além de proporcionar uma visão mais detalhada e permitir que gerentes de redes possam obter uma base de escolha para tais softwares de acordo com suas necessidades.

2. Objetivos

2.1. Objetivo Geral

Analisar os recursos de softwares livres que utilizam o protocolo SNMP no gerenciamento de redes.

2.2. Objetivos Específicos

- Identificar vantagens e desvantagens do uso de ferramentas livres para o gerenciamento de redes.
- Realizar análises dos recursos dos softwares livres a fim de se propor uma base de escolha para aqueles que procuram ferramentas com características voltadas ao protocolo SNMP.

2.3. Justificativa

As organizações públicas ou privadas detêm atualmente de redes de computadores de pequeno a grande porte em suas instalações. Muitas dessas organizações sequer conhecem os mecanismos para realizar um gerenciamento das informações em suas redes, onde dados importantes trafegam por seus mais variados dispositivos.

As atividades de algumas dessas organizações se tornam inviáveis se os serviços prestados pela rede não estiverem disponíveis, ou se forem prestados com tempos de resposta acima de determinados limites. À medida que as redes locais crescem e se

interligam com redes de outras organizações, torna-se necessária a utilização de ferramentas que facilitem sua gerência. (ALBUQUERQUE, 2001).

Hoje, o SNMP (Simple Network Management Protocol) é o protocolo mais utilizado para controlar redes comerciais de diversos tipos. Nesse contexto, existem ferramentas para o gerenciamento de rede baseadas no protocolo SNMP, com a vantagem adicional de serem distribuídas gratuitamente com versões disponíveis para os mais variados sistemas operacionais.

Essa integração de ferramentas livres baseadas no protocolo SNMP para gerência de redes pode se tornar, portanto, um vantajoso meio para as organizações conseguirem realizar um eficiente controle sobre suas redes de computadores utilizando os recursos oferecidos pelas ferramentas livres.

Faz-se inevitável realizar análises referentes aos recursos de cada software a fim de se identificar vantagens, desvantagens e a viabilidade para implementação em organizações que necessitem de uma correta gerência das informações em suas redes de computadores.

3. Revisão de Literatura

De acordo com Black (2008), o gerenciamento de redes é uma atividade importante para manter as mesmas operando corretamente. Para se realizar tais tarefas gerenciais, o uso de softwares específicos (aqui também chamados de ferramentas) tornou-se uma constante, dado o notório aumento do número de dispositivos a ser gerenciado, o que impede um tratamento individualizado de cada um, bem como dado à necessidade de procedimentos automatizados de configuração, monitoração, reportes, entre outros.

A gerência está associada ao controle de atividades e ao monitoramento do uso de recursos da rede. As tarefas básicas de gerência em redes são: obter informações da rede, tratar estas informações possibilitando um diagnóstico e encaminhar as soluções dos problemas (SZTAJNBERG, 1996).

Stange (2008) diz que além dos sistemas de gerenciamento é fundamental que o responsável por uma rede tenha amplos conhecimentos de procedimentos, desempenho e identificação de falhas que possam acontecer. Outra característica essencial ao administrador ou gerente de uma rede é a familiarização com os sistemas por ele utilizados no cotidiano.

Os sistemas usados na gerência de redes procuram prestar os serviços sem sobrecarregar as entidades gerenciadas ou canais de comunicação e de forma objetiva.

3.1 Importância do gerenciamento de redes

Segundo Stallings (1999), 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 especial, grandes redes corporativas estão fadadas ao caos sem estas funções. Além de agirem reativamente, as tarefas gerenciais de rede também são proativas no sentido de prevenir e detectar possíveis problemas.

Segundo Martin-Flatin, Znaty e Hubaux (1999), uma aplicação de gerenciamento é composta por gerentes executando nas estações de gerenciamento e

agentes executando nos elementos gerenciados.

Gerenciar uma rede é uma atividade bastante trabalhosa. Nos últimos anos o tráfego de informações dentro das redes corporativas aumentou exponencialmente devido ao surgimento de inúmeras novas aplicações. Concorrentemente, novas tecnologias e padrões proporcionaram uma grande proliferação de dispositivos heterogêneos conectados à rede.

3.2 Necessidade do gerenciamento de redes

De acordo com Black (2008), o investimento em um software de gerenciamento pode ser justificado pelos 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 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 da rede deve atribuir e controlar recursos para balancear estas várias necessidades.

3.3 Protocolo SNMP (Simple Network Management Protocol)

Como explica Harnedy (1997), o Simple Network Management Protocol (SNMP) é um protocolo da camada de aplicação lançado em 1988 e projetado para facilitar a troca de informação de gerência entre dispositivos da rede. Através do SNMP, são transportados dados informativos (tais como pacotes por taxas de segundo e de erro da rede).

Utiliza os serviços do protocolo de transporte UDP (User Datagram Protocol) para enviar suas mensagens através da rede. Com esse protocolo, os administradores controlam facilmente o desempenho da rede, encontram e resolvem problemas. Sua especificação está contida no RFC-1155 (Structure Of Management Information), RFC-1156 (Management Information Base) e RFC-1157 (Simple Network Management Protocol). Este protocolo é o centro do desenvolvimento do gerenciamento SNMP. (MELO, 2007).

Como o Transmission Control Protocol (TCP), o SNMP é um Internet Protocol. Atualmente, existem três versões do SNMP: versão 1, versão 2 e versão 3. Na versão 2 do SNMP, procurou-se a correção de algumas deficiências da versão 1, melhorando a comunicação através da chamada Manager to Manager MIB. Já a versão 3 do SNMP tem como vantagens aspectos ligados à segurança.

Conforme Melo (2007), hoje, o SNMP é o protocolo mais utilizado para controlar redes comerciais de diversos tipos. O SNMP é um protocolo relativamente simples, contudo seu poder de gerenciamento é bastante poderoso, podendo controlar difíceis problemas apresentados em variados tipos de redes TCP/IP.

O SNMP, segundo Harnedy (1997), parte do esquema de gerenciamento OSI, onde os processos que implementam as funções de gerenciamento de Internet atuam

como agentes ou gerentes. Esses agentes têm por função descobrir falhas ou problemas nos componentes da rede (Hosts, roteadores, gateways, etc.). Dessa forma, podem ser tomadas providências antes mesmo que o problema venha a acontecer, ou até mesmo saber como ou de onde surgiu o problema.

Cada componente gerenciado é visto como uma coleção de variáveis, onde os valores podem ser lidos ou alterados. O gerente, então, envia comandos aos agentes, solicitando uma leitura no valor das variáveis dos componentes gerenciados, ou modificando seu valor. Na troca de informações entre o gerente e o agente, são aplicados mecanismos de autenticação para evitar que usuários não autorizados interfiram no funcionamento da rede. Essa troca de mensagem entre gerente e agente é definida pelo protocolo SNMP, onde ele define o formato e a ordem que deve ser seguida à seqüência das informações de gerenciamento.

Para armazenar tais informações, são utilizados MIB (Management Information Base), onde são armazenadas as informações sobre o funcionamento dos Hosts, Roteadores e dos processos que executem os protocolos de comunicação (TCP, IP, ARP, etc...). Com o SNMP os gerentes de rede têm também a capacidade de modificar valores de uma variável de um objeto na MIB. (MELO, 2007).

A Figura 1 ilustra um sistema envolvendo a troca de informações entre Agente e Gerente:

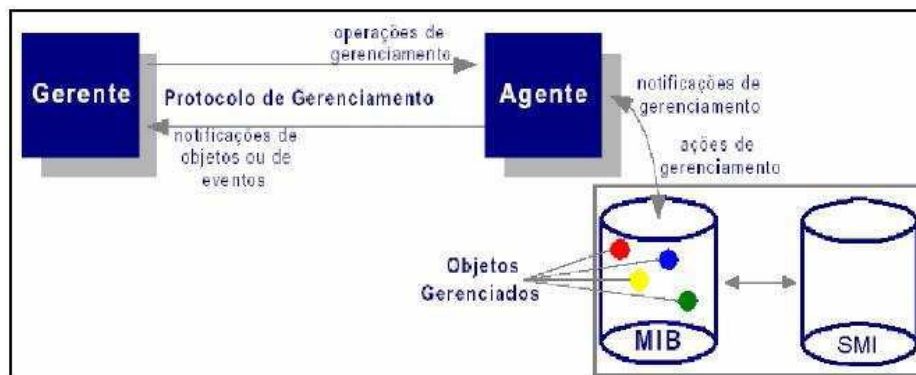


Figura 1 - Componentes do SNMP.

Fonte: Harnedy (1997).

3.4 Software Livre

Segundo Campos (2006), Software Livre, ou Free Software, conforme a definição de software livre criada pela Free Software Foundation é o software que pode ser usado, copiado, estudado, modificado e redistribuído sem restrição. A forma usual de um software ser distribuído livremente é sendo acompanhado por uma licença de software livre (como a GPL ou a BSD), e com a disponibilização do seu código-fonte.

Um programa é software livre se os usuários têm todas essas liberdades. Portanto, o usuário deve ser livre para redistribuir cópias, seja com ou sem modificações, seja de graça ou cobrando uma taxa pela distribuição, para qualquer um em qualquer lugar. Ser livre para fazer essas coisas significa (entre outras coisas) que o usuário não tem que pedir ou pagar pela permissão, uma vez que esteja de posse do programa. (COSTA, 2010).

Deve-se também ter a liberdade de fazer modificações e usá-las privativamente no trabalho ou lazer, sem nem mesmo mencionar que elas existem. Se modificações forem publicadas, o usuário não deve ser obrigado a avisar a ninguém em particular, ou de nenhum modo em especial. (COSTA, 2010).

Por fim, Campos (2006) lembra que, para que essas liberdades sejam reais, elas tem que ser irrevogáveis desde que o usuário não faça nada errado; caso o desenvolvedor do software tenha o poder de revogar a licença, mesmo que o usuário não tenha dado motivo, o software não é livre.

3.5 Cacti

De acordo com Black (2008), Cacti é uma ferramenta freeware que recolhe e exhibe informações sobre o estado de uma rede de computadores através de gráficos.

Com o Cacti é possível gerar gráficos referentes a uso de memória física, memória virtual, quantidade de processos, processamento, tráfego de rede, quantidade de espaço em disco, etc. Através do SNMP, permite ter acesso a gráfico não só de sistemas operacionais Linux, mas também de Windows e de dispositivos de rede como roteadores e switches, bem como qualquer dispositivo que suporte SNMP. Todas as três versões do SNMP são suportadas atualmente pelo Cacti. (BLACK, 2008).

Sua arquitetura prevê a possibilidade de expansão através de inúmeros plugins desenvolvidos por sua comunidade que adicionam novas funcionalidades.

O Cacti permite que os gráficos gerados sejam organizados de diversos modos: configurando-os em forma de árvores ou agrupando todos os gráficos de um mesmo tipo sob um gráfico maior, podendo-se ter um gráfico em duas ou mais árvores também. Estas árvores de gráficos possuem diversas maneiras de serem organizadas, de acordo com a necessidade do administrador, podendo-se gerar gráficos de praticamente qualquer dispositivo que se deseje. A variedade de modelos que vêm com a instalação padrão é suficiente para cuidar de redes simples, e você pode criar seus próprios tipos de dados e modelos mais complexos para redes, apesar do Cacti não conseguir exibir e tabular dados numéricos. (BLACK, 2008).

3.6 Nagios

De acordo com Lopes (2010), o Nagios é um aplicativo de monitoramento de sistemas e de redes, podendo ser estendido amplamente a um gerenciador de redes graças aos diversos plug-ins disponíveis em sua comunidade. Ele verifica clientes e serviços especificados, gerando alertas quando algo está fora dos padrões pré-definidos.

Originalmente desenvolvido para rodar em Linux, há pacotes personalizados para distribuições comuns como Fedora, Ubuntu, SUSE e Debian.

Algumas das várias ferramentas do Nagios TM incluem:

- Monitoramento de rede e serviços;
- Monitoramento dos recursos de clientes (carga de processador, uso de disco, etc.);
- Organização simples de plugins que permite aos usuários facilmente desenvolverem seus próprios serviços de checagem;

-Checagem paralela de serviços;

-Notificação de contatos quando problemas em serviços e clientes ocorrerem ou forem resolvidos (via e-mail, pager, ou métodos definidos pelo usuário);

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

-Interface web opcional para visualização do status atual da rede, histórico de notificações e problemas, arquivos de log, etc;

Uma vez instalado, existem muitos arquivos de configurações que serão necessários criar ou editar antes de iniciar o monitoramento da rede.

4. Metodologia

O trabalho envolveu uma pesquisa exploratória, pois de acordo com Gil (2008), o objetivo desta é familiarizar-se com um assunto ainda pouco conhecido, pouco explorado. Ao final de uma pesquisa exploratória, se conhecerá mais sobre aquele assunto, estando apto a construir hipóteses. Como qualquer exploração, a pesquisa exploratória depende da intuição do explorador (neste caso, da intuição do pesquisador).

Por ser um tipo de pesquisa muito específica, quase sempre ela assume a forma de um estudo de caso. Como qualquer pesquisa, ela depende também de uma pesquisa bibliográfica, pois mesmo que existam poucas referências sobre o assunto pesquisado, nenhuma pesquisa hoje começa totalmente do zero. Haverá sempre alguma obra, ou entrevista com pessoas que tiveram experiências práticas com problemas semelhantes ou análise de exemplos análogos que podem estimular a compreensão.

O desenvolvimento se deu em um microcomputador pessoal (notebook) com o sistema operacional Windows XP, equipado com um processador Intel Dual Core de 1.8 GHz, 2 Gb de memória RAM, 160 Gb de Disco Rígido, sendo ele emulado em uma máquina virtual com o sistema operacional Linux Ubuntu 10 Server, pois os programas que foram utilizados são compatíveis com tal sistema.

Os instrumentos que foram utilizados, ou seja, as ferramentas foram os softwares livres de monitoramento de redes chamados Cacti e Nagios, já apresentados e definidos nos capítulos anteriores.

A escolha das ferramentas foi feita analisando a funcionalidade e facilidade de uso, e também de serem licenciadas pela GPL (GNU General Public License), ou seja, são softwares livres, o que garante um constante desenvolvimento por parte dos criadores, além de não perder em nada para as soluções comerciais existente, que são extremamente caras.

De início, foram feitos alguns estudos sobre as características, bem como um aprofundamento no conhecimento dos softwares livres Cacti e Nagios através de livros e material disponível na Internet.

Após o estudo das ferramentas, deu-se o início da parte prática do trabalho onde o primeiro passo envolveu a criação da máquina virtual através do programa Sun Virtualbox no computador pessoal. O sistema operacional usado na máquina virtual foi o Linux Ubuntu versão 10.

Em seguida, foi feita a instalação do protocolo SNMP no ambiente Linux pelo fato deste ser o protocolo mais utilizado para o gerenciamento de redes IP e internet.

Após realizado todos os processos descritos acima, foram feitas as instalações e configurações dos softwares Cacti e Nagios pelo terminal do Linux que realizou o download automático através de comandos digitados no mesmo, instalação essa que utilizou o Arquivo Fonte (source) de cada uma.

Foram instalados também algumas dependências dos softwares para seu correto funcionamento como o banco de dados MySQL para servir de base na criação e armazenamento dos gráficos e informações geradas pelos softwares, garantindo um longo armazenamento dos dados; além do servidor Apache 2 e o Php 5 devido aos softwares utilizarem códigos de programação da linguagem Php.

Terminado o processo de instalação e configuração das ferramentas, se iniciou a fase de análise e obtenção dos dados que cada ferramenta gerou de acordo com suas características. Os dados obtidos pelas ferramentas foram guardados e analisados de acordo com o propósito do trabalho.

Por fim, todos os resultados e conclusões foram escritos e documentados para divulgação, atingindo assim a meta principal do projeto.

5. Resultados Obtidos

A análise apresentada a seguir advém dos resultados obtidos ao longo do processo de aplicação dos métodos citados anteriormente envolvendo uma série de visualizações e explicações das funcionalidades testadas do Cacti e Nagios.

Antes de instalar o Cacti é necessário realizar a instalação de suas dependências.

Depois de feito o procedimento de instalação, é digitado no navegador o endereço <http://localhost/cacti/> para realizar o login mediante validação de usuário e senha. Após feito o login, é possível visualizar a tela inicial do Cacti onde pode-se acessar suas abas principais de recursos e adicionar dispositivos para monitoramento, onde, juntamente com esses dispositivos podem ser criados gráficos para visualização de estatísticas sobre o gerenciamento.

Conforme Figura 2, uma das funcionalidades do Cacti, o uso de memória, é mostrado graficamente. Ele possui um sistema de monitoramento com marcações legendadas do dia e das horas monitoradas, além de detalhar a quantidade em kilobytes usada pela memória.

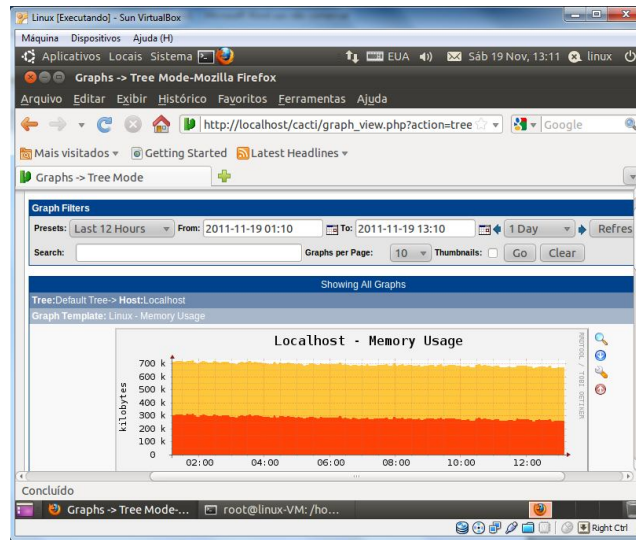


Figura 2 – Gráfico do uso de memória gerado pelo Cacti.

Na Figura 3, outra das funcionalidades do Cacti, a média de carregamento, é mostrada graficamente. Ele possui um sistema de monitoramento com marcações legendadas do dia e das horas monitoradas, além de detalhar a média de tempo em que os serviços são carregados no sistema.

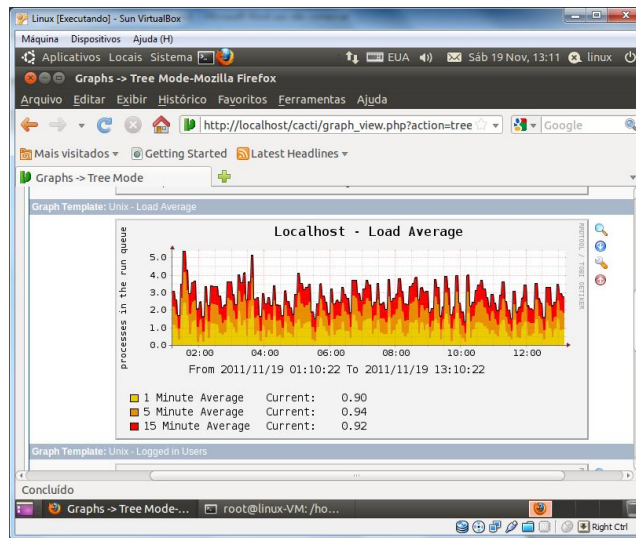


Figura 3 – Gráfico da média de carregamento gerado pelo Cacti.

Outra das funcionalidades do Cacti, usuários logados, podem ser mostrados graficamente. Ele possui um sistema de monitoramento com marcações legendadas do dia e das horas monitoradas, além de detalhar a quantidade de usuários que estão logados no sistema em determinado período de tempo.

Mais uma das funcionalidades do Cacti, processos, podem ser mostrados graficamente. Nele, são mostrados a quantidade de processos sendo executados na rede por um sistema de monitoramento com marcações legendadas do dia e das horas monitoradas.

Todos esses gráficos e dispositivos mostrados acima podem ser configurados de

acordo com os recursos disponíveis para o usuário além de o programa apresentar uma tela onde são adicionados e monitorados os dispositivos desejados pelo administrador.

Há também o serviço para a consulta dos dados e estatísticas processadas pelo Cacti, entre eles, as informações obtidas e geradas através do protocolo SNMP.

E por fim, outro dos recursos disponíveis no Cacti é o relatório com informações dos usuários que estão sendo monitorados pelo programa que vão do administrador até os usuários hospedados pela rede.

A seguir, foi analisado o software Nagios, onde após instaladas as dependências, foi baixado e compilado o programa.

Depois de feito o procedimento de instalação, foi digitado no navegador o endereço <http://localhost/nagios/> para realizar o login mediante validação de usuário e senha.

Após o login, é possível visualizar a tela inicial do Nagios onde pode-se acessar suas abas principais de recursos. Nessa aba, vê-se uma série de opções para o monitoramento.

Observando a Figura 4, é mostrado um resumo geral do monitoramento e sua performance diante da rede analisada com itens bem detalhados, além de fornecer a informação sobre a “saúde” da rede contemplando o host e os serviços. Também é possível checar alguns recursos da monitoração como detecção de flap, notificações, manipuladores de eventos, verificações ativas.

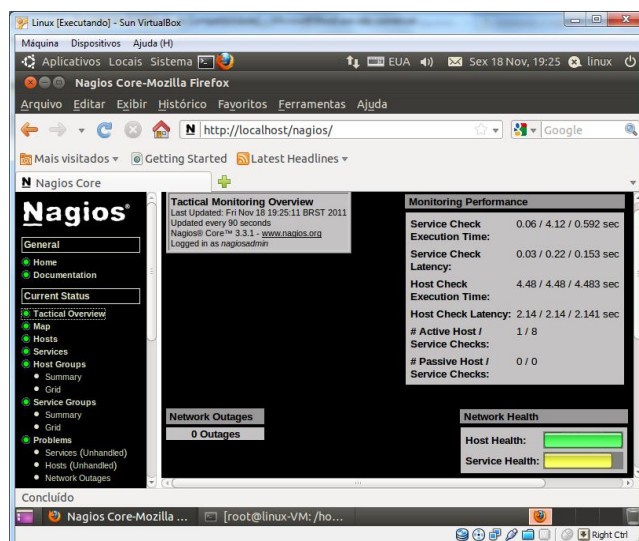


Figura 4 – Resumo geral da performance de monitoramento do Nagios.

O Nagios mostra também o detalhamento dos hosts e dos serviços que eles utilizam, informando e notificando avisos se houver algum problema com ambos, além de mostrar o período de checagem e o status dos mais variados recursos como, por exemplo, a perda de pacotes.

É possível realizar o acesso a relatórios detalhados em relação ao monitoramento da rede. Esse relatório é gerado através de passos onde o administrador escolhe as opções que lhe melhor convêm.

Uma parte importante do programa envolve o gerenciamento de alertas, onde

qualquer erro que ocorra com algum serviço ou alguma falha no sistema, como uma máquina na rede desligada, o Nagios emite um alerta (Host Down) avisando sobre o problema.

Outro recurso importante são os Event Logs, ou seja, um sistema de gerenciamento e correlação de todos os eventos trabalhados pelo programa onde qualquer processo executado é registrado numa lista com informações detalhadas.

Por fim, um recurso extremamente importante para os administradores que utilizam o Nagios, é o sistema de agendamento de serviços a serem executados pelo gerenciador. Nele, o usuário define o tempo em que o programa realizará uma rotina de checagem de determinado processo a fim de se evitar qualquer problema que possa ser ocasionado na rede.

6. Conclusão

Após aplicadas as observações de monitoramento e feitas as análises dos recursos de cada software, as seguintes conclusões foram obtidas:

Em relação ao Cacti, as possibilidades do software são muitas, quando utilizado suas funções básicas é possível visualizar gráficos diários, semanais, mensais e anuais sobre utilização de interfaces de rede, CPU, memória, espaço em disco, entre outros. Mas quando são adicionadas as funcionalidades desenvolvidas pela comunidade do Cacti, como plugins e templates diversos este software se torna excelente para qualquer área funcional do gerenciamento de redes, além de ficar muito mais robusto e funcional.

A implantação no ambiente de testes se mostrou muito efetiva, tornando-se evidentes as vantagens da implantação do software Cacti em qualquer ambiente de rede, devido sua robustez, facilidade de implantação e excelente desempenho, é uma economia para qualquer empresa com suporte de TI, pois, economiza com a aquisição, por ser gratuito, tem aperfeiçoamento constante, com foco na qualidade e diversificação de ferramentas pela comunidade de software livre, além de ser possível fazer uma adaptação aos objetivos específicos de cada pessoa ou empresa.

Como ponto fraco, comparado ao Nagios observou-se um desempenho aquém do esperado para levantar, armazenar e exibir os dados, ainda que não seja nada de alarmante.

O software Cacti, correspondeu de forma positiva nos testes realizados, demonstrando que esta ferramenta é de extrema importância para garantir um alto nível de confiabilidade e qualidade no gerenciamento de redes em empresas.

Em relação ao Nagios, a instalação e configuração foram trabalhosas, porém a quantidade de listas de discussões na internet auxiliou muito seu desenvolvimento. Além disso, o próprio site oficial do Nagios disponibiliza formas de contato bastante ágeis entre os usuários e os desenvolvedores do sistema.

Para o monitoramento de serviços o Nagios se mostrou muito bem aplicável, pois através do uso de seus recursos é possível ter uma visão global da rede. Ele é um software abrangente e experiente que reporta e atualiza corretamente todas as informações relevantes, dando-se ênfase maior em cima do quesito disponibilidade, tendo este produto diversas ferramentas para monitorar os mais variados serviços e plataformas Windows/Linux/Unix.

Alguns itens podem ser implementados para aprimorar o Nagios: desenvolvimento de um front-end de configuração, com o intuito de facilitar e concentrar o meio de configuração dos seus arquivos cfg; ampliação da capacidade de monitoramento do Nagios, para abranger arquivos de servidor web, evitando, assim, a ação de hackers; desenvolvimento de plugins com objetivos específicos, voltados para o monitoramento de algum equipamento em particular, como controladores de temperatura, umidade, volume de água, etc.

Com os recursos humanos tornando-se cada vez mais escassos, nenhum departamento de TI pode se dar ao luxo de ter seus sistemas manualmente verificados. Redes estão se tornando mais complexas e demandam especialmente a necessidade de serem informadas o quanto antes, sobre quedas que aconteceram ou por problemas que estão por acontecer.

O Nagios, uma ferramenta de código aberto para monitoração de sistemas e redes, ajuda o administrador a detectar problemas antes que o pior possa acontecer. Devido à eficiência da monitoração, ele não sobrecarrega o servidor nem os dispositivos de rede; permite que outras aplicações possam compartilhar o dado SNMP; o teste de dispositivos é feito de forma rápida; gera relatórios identificando imprecisão na monitoração existente e possui dados de configuração unificados.

O Nagios provê uma visão do essencial de desempenho e disponibilidade, e é um exemplo de como a Comunidade de Código Aberto pode ajudar no gerenciamento da rede.

Por fim, os dois softwares analisados neste trabalho mostraram possuir muitas opções para um monitoramento de rede eficaz, sendo em sua essência semelhantes entre si, porém cada qual com suas particularidades que fazem deles ótimos produtos de escolha para um gerenciamento satisfatório e funcional, sem contar o fato de serem totalmente gratuitos.

Espera-se assim que o estudo e análise feitos neste trabalho possam contribuir para que administradores de redes conheçam e desenvolvam melhorias para tais softwares a fim de se melhorar cada vez mais um recurso tão importante no que tange a tecnologia, o gerenciamento de uma rede.

Referências

ALBUQUERQUE, Fernando. TCP-IP Internet: protocolos & tecnologias. 3. ed. Rio de Janeiro : Axcel Books do Brasil, 2001. xv, 362 p.

BLACK, Tomas Lovis. Comparação de Ferramentas de Gerenciamento de Redes. Porto Alegre, 2008.

CAMPOS, Augusto. O que é software livre. BR-Linux. Florianópolis, 2006. Disponível em: <<http://br-linux.org/linux/faq-softwarelivre>>. Acesso em: 2 maio 2011.

COSTA, Reinaldo Candido da. Conhecendo o Software Livre. Minas Gerais: Ed. Horizonte, 2010.

GIL, Antonio Carlos. Como elaborar projetos de pesquisa. 5. ed. São Paulo: Atlas, 2008.

HARNEDY, Sean. Total SNMP: Exploring the Simple Network Management Protocol. 2 ed. Prentice Hall PTR, 1997.

- LOPES, Taylor. Redes: Uma introdução ao Nagios. São Gonçalo, 2010.
- MARTIN-FLATIN, J.P.; ZNATY, S.; HUBAUX, J.P. A Survey of Distributed Enterprise Network and System Management Paradigms. Journal of Network and Systems Management, New York, v.7, n.1, p.9-26, Mar. 1999.
- MELO, Tiago Maciel. Monitoramento de Redes de Médio Porte Utilizando Software Livre. Palhoça, 2007.
- SANTOS, Adriano Pereira. Implantação de Software de Gerenciamento de Rede baseado nas plataformas Microsoft e Linux. São Paulo, 2005.
- STALLINGS, W. SNMP, SNMPv2, SNMPv3 and RMON 1 and 2: the practical guide to network management standards. 3rd ed. Reding: Addison-Wesley, 1999.
- STANGE, Rodrigo. Ferramenta para Gerenciamento de Falhas em Rede Ethernet Baseada em Protocolo SNMP. Blumenau, 2008.
- SZTAJNBERG, Alexandre. Gerenciamento de redes – Conceitos básicos sobre os protocolos SNMP e CMIP. 2. ed. Rio de Janeiro. Ed. Conexão 1996.