

## Ferramentas Livres para Monitoração de Servidores

Arlindo Follador Neto<sup>1</sup>, Joaquim Quinteiro Uchôa<sup>2</sup>

<sup>1</sup>Centro de Pesquisa e Desenvolvimento em Engenharia Elétrica  
Universidade Federal de Minas Gerais (UFMG)  
Av. Antônio Carlos 6627 – 31270-010 – Belo Horizonte – MG – Brasil

<sup>2</sup>Curso de Pós-Graduação Lato Sensu Administração em Redes Linux  
Universidade Federal de Lavras (UFLA)  
Caixa Postal 3037 – 37200-000 – Lavras – MG – Brasil

arlindo@lopan.eti.br, joukim@ginux.ufla.br

**Resumo.** *Este artigo apresenta uma análise de ferramentas de monitoração de servidores, serviços e ativos de rede. O objetivo principal do trabalho realizado foi o de comparar ferramentas distribuídas livremente que atendam os quesitos de monitoração cumulativa, geração de gráficos e alertas ao administrador. O artigo apresenta os resultados dos testes efetuados, indicando a melhor ferramenta para esse tipo de tarefa.*

**Abstract.** *This paper presents an analysis of monitoring tools for servers, network services, and equipments. The main objective was to establish a comparison among freely distributed applications that provide cumulative monitoring, graph generation and administrator notification. The article presents the results of the conducted tests, pointing out the best tool for these tasks.*

### 1. Comentários Iniciais

O gerenciamento de máquinas servidoras infelizmente ainda não é uma tarefa simples. Muitas são as dificuldades e em alguns problemas é necessário um acompanhamento de determinados processos para poder avaliar a melhor solução, como por exemplo a avaliação de gargalos de aplicações distribuídas. Dessa maneira, é extremamente necessário ter uma fonte de dados disponível para consulta imediata no caso de quedas, congestionamento, mal funcionamento ou qualquer anormalidade que afete servidores ou redes de computadores. Em casos mais críticos, a presença dessas informações permitirá que o administrador tenha bases para estudar o comportamento do ambiente até o acontecimento de uma fatalidade ou mesmo detectar e evitar sua ocorrência.

Como comentado em [Comer 2001], o uso de um software *de gerência de rede* é o mecanismo para que o administrador descubra problemas e isole sua causa. Esse tipo de *software* compreende ferramentas de monitoração de serviços e equipamentos de redes, baseados principalmente no protocolo SNMP (*Simple Network Management Protocol*), [Mauro and Schmidt 2001], sendo que alguns desses aplicativos podem ainda agregar *scripts* e agentes remotos para coletar dados. Posteriormente essas informações são utilizadas para extrair históricos, análises gráficas e consultas diversas, auxiliando assim no acompanhamento detalhado de um ambiente computacional.

O objetivo deste trabalho é apresentar algumas ferramentas relativamente bem conhecidas pela comunidade *software* livre para monitoração de serviços e equipamentos

de redes. Para isso, ele encontra-se organizado da seguinte maneira: na Seção 2 são apresentadas as ferramentas MRTG, Nagios, Cacti, Zabbix, utilizadas neste trabalho; a análise crítica dessas ferramentas, bem como a recomendação de uso, são feitas na Seção 3; por fim, na Seção 4 são apresentados os resultados principais deste trabalho.

## 2. Ferramentas de Monitorização de Servidores

O MRTG<sup>1</sup> é uma das ferramentas mais conhecidas para monitoração de servidores. Desenvolvido por Tobias Oetiker e programado em Perl, o MRTG está na sua versão 2.13 [Oetiker 2006]. A instalação do MRTG é uma das mais simples, seu pacote e o de suas dependências estão disponíveis para a maioria das distribuições Linux. O MRTG é muito utilizado em servidores locais, para extrair e exibir informações do uso de processador, memória, tráfego nas interfaces de rede, uso de discos, etc. Seus gráficos tem uma resolução agradável e a forma histórica de apresentação é usada por quase todas as aplicações do gênero como pode ser visto na Figura 1. O mesmo *script* que cria os gráficos também cria arquivos em HTML para facilitar a visualização, que pode ser feita mesmo na ausência de um servidor *web*.

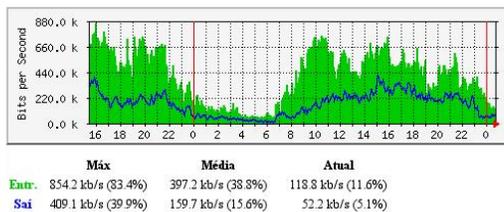


Figura 1. Gráfico MRTG

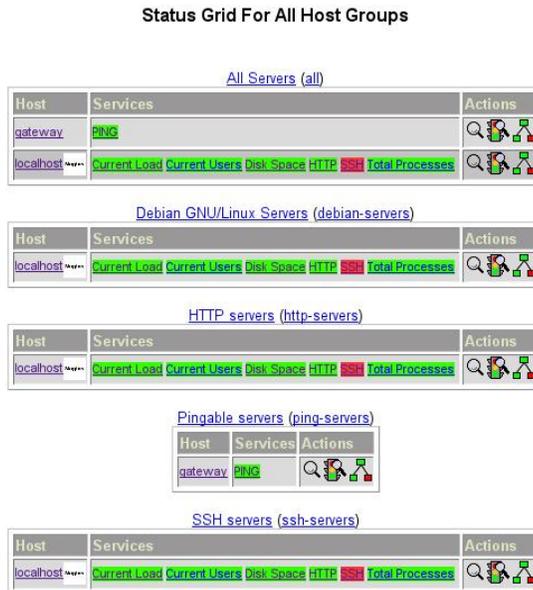
O Nagios<sup>2</sup> é uma aplicação para monitoramento de servidores e serviços de rede com o intuito de alertar clientes ou administradores sobre possíveis problemas. O Nagios utiliza-se de *plugins* locais e remotos para colher informações necessárias em suas avaliações. A aplicação permite o envio de alertas por *e-mail*, sistemas de mensagens instantâneas, SMS, dentre outros. Entre seus recursos, encontra-se monitoração de serviços de SMTP, POP3, SSH, HTTP, discos, temperatura, etc., utilizando-se de aplicações CGI para coletar dados e constituir sua interface *web* [Galstad 2006]. O Nagios se encontra na versão 2.0 e seu desenvolvimento é liderado pelo americano Ethan Galstad.

A instalação do Nagios é relativamente simples, dependendo do Apache<sup>3</sup> devidamente configurado e funcionando com suporte a execução de aplicações CGI. Após sua instalação, já é possível acompanhar os resultados de seus testes padrões para a máquina onde se encontra instalado. Dentre as opções que inicialmente ele disponibiliza estão: a utilização do processador, disco, usuários conectados, o estado de serviços que estão rodando localmente (SSH por exemplo), total de processos em execução assim como o *ping* para o *gateway* da máquina de instalação e seus agentes (uma vez configurados), como visto na Figura 2. A configuração para obter informações de diversas máquinas na rede é mais complexa e depende da instalação de agentes remotos para a coleta de dados.

<sup>1</sup>O MRTG pode ser obtido em: <http://people.ee.ethz.ch/~oetiker/webtools/mrtg/>

<sup>2</sup>O Nagios pode ser obtido em: <http://www.nagios.org>

<sup>3</sup>Servidor HTTP <http://www.apache.org>



**Figura 2. Monitoração de *Hosts* no Nagios**

O Cacti<sup>4</sup> é um *frontend* para o RRDTool desenvolvido em PHP com utilização de base de dados MySQL ele utiliza o RRDTool para a confecção de arquivos de dados e geração de gráficos informativos. O Cacti foi desenvolvido inicialmente por Ian Berry, está atualmente na versão 0.8.6h [Berry et al. 2005]. A aplicação utiliza-se de *scripts* em Bash, Perl, XML, dentre outros para colher dados localmente, ou remotamente utilizando SNMP. O RRDTool<sup>5</sup>, por sua vez, foi desenvolvido por Tobias Oetiker e constitui um pacote de ferramentas para gerar e interpretar informações em arquivos de dados, assim como a geração de gráficos estatísticos com base nesses arquivos [Oetiker 2005].

Para a instalação do Cacti é necessário ter previamente instalado o RRDTool, Apache com suporte a PHP e banco de dados MySQL. Em uma rede com suporte a SNMP instalado e ativo, o Cacti utiliza-se dos dados de servidores, roteadores, equipamentos *wireless* ou qualquer outro com suporte a SNMP, para gerar gráficos de alta qualidade e precisão, que podem ser acompanhados por interface *web*, com opções para configurar, criar e visualizar diversas opções de gráficos de monitoração de recursos (Figura 3). Os principais *scripts* do Cacti medem a latência entre os *hosts na rede*, uso de interfaces de rede, uso de CPU, memória, disco, usuários conectados, etc. A construção dos gráficos é feita por rotinas em PHP, inicialmente elas recebem os dados coletados por *scripts*, criam arquivos RRDs (forma de dados do RRDTool) e posteriormente os converte em gráficos.

<sup>4</sup>O Cacti pode ser obtido em: <http://www.cacti.net>

<sup>5</sup>Mais informações sobre o RRDTool (Round Robin Database Tool) podem ser obtidas no endereço: [http://freshmeat.net/redirect/rrdtool/9129/url\\_homepage/rrdtool](http://freshmeat.net/redirect/rrdtool/9129/url_homepage/rrdtool)

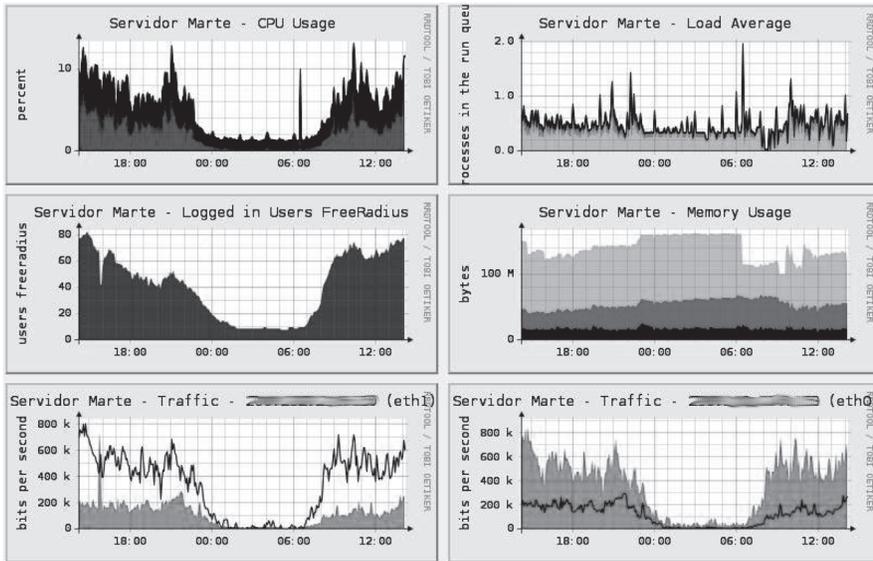


Figura 3. Gráficos de Dados SNMP no Cacti

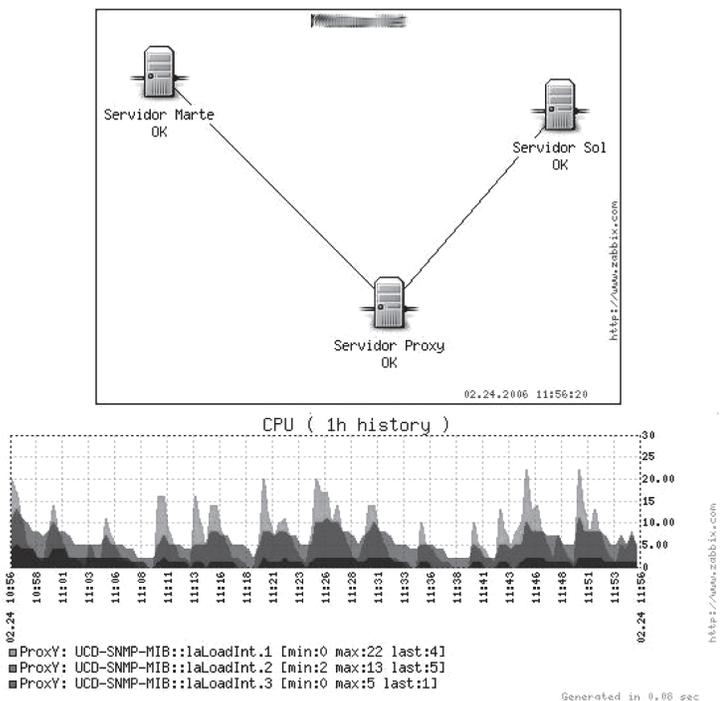
O Zabbix<sup>6</sup> é uma aplicação para monitorar aplicações, redes e servidores, com grande flexibilidade para para coleta de dados e geração de gráficos, mapas e alertas. Criado por Alexei Vladishev, em C e PHP, utiliza banco de dados compatíveis com MySQL e PostgreSQL, sendo que sua versão estável é a 1.0 [Vladishev 2000]. A personalização na coleta de dados no Zabbix é um ponto muito forte desta ferramenta. As informações são coletadas por itens cadastrados em cada *host* ou em um grupo de *hosts*. Um item constitui uma chave SNMP para a extração de um resultado ou uma informação passada remotamente ou localmente por um agente Zabbix. Um exemplo de gráfico no Zabbix pode ser visto na Figura 4, onde foram inseridas as chaves SNMP referentes ao processamento médio da máquina remota.

As informações gráficas do Zabbix não se resumem em gráficos estatísticos. O Zabbix oferece a possibilidade de se criar mapas de toda a rede, ligando servidores a *switches*, roteadores, dentre outros, monitorando se estes estão ou não ativos como visto na Figura 4. A simples detecção de falha nas ligações entre os itens cadastrados nos mapas é bastante para o disparo de *triggers* que executarão comandos em *scripts* ou ações internas do próprio Zabbix, de acordo com a necessidade do administrador.

### 3. Resultados e Discussão

As ferramentas apresentadas neste trabalho foram instaladas e testadas e um AMD Athlon XP 2200+, com 256MB de RAM, HD de 40GB e o sistema operacional GNU/Linux Debian 3.1. A instalação das ferramentas não causou dificuldades, MRTG, Nagios, Cacti e Zabbix tem pacotes disponíveis para a maioria das distribuições, bem como suas dependências. De todas as ferramentas o MRTG tem a instalação mais simples, suas dependências são poucas e ele não necessita de configurações em outros serviços. A

<sup>6</sup>O Zabbix pode ser obtido em: <http://www.zabbix.com>



**Figura 4. Gráfico e Mapa do Zabbix**

instalação do Nagios também é simples e no Debian seu pacote auto-configura o Apache para a execução de aplicações CGI; após sua instalação já é possível conferir os primeiros resultados sobre a máquina local. Na instalação dos pacotes Cacti e Zabbix, é iniciado automaticamente um instalador que guia passo-a-passo o usuário na criação da base de dados e configuração do Apache; seguindo os passos corretamente é possível utilizar Cacti e Zabbix logo após a instalação dos pacotes.

Para obter os primeiros resultados, sem dúvida o MRTG é o mais desgastante: ele não possui uma interface para configuração e exige do usuário o conhecimento das chaves SNMP ou a criação de *scripts* para obtenção dos dados e posteriormente a geração dos gráficos. O Nagios já detecta os principais serviços que estão em funcionamento na máquina de instalação (conexão com o *gateway*, etc.) e os monitora. O ponto forte do Nagios é o esquema de alerta sobre anormalidades que pode ser configurado por sua interface *web*, mas o fato de não usar gráficos para o acompanhamento de resultados torna mais complexa a análise e acompanhamento dos mesmos.

Como o MRTG, Cacti e Zabbix não trazem nenhuma informação para acompanhamento logo após sua instalação, mas contam com uma interface *web* que simplifica a configuração para a geração de gráficos. A configuração do Cacti é extremamente simplificada, principalmente quando as informações devem ser obtidas na maquina local ou em máquinas remotas através de SNMP; o fato do Cacti contar com perfis de coleta de dados básicos (uso de CPU, memória, rede, etc) e geração de gráficos agiliza a configuração da ferramenta. A principal dificuldade do Cacti é a inclusão de novas chaves SNMP ou novos *scripts* para coleta de dados que não se encontram disponíveis nos perfis padrões, além de não possuir nenhum mecanismo de alerta.

O Zabbix agrega funcionalidades do MRTG, Cacti e Nagios, possui mecanismo de coleta de dados local, remota através do Agente Zabbix e SNMP que possibilitam monitorar o *status* de servidores, serviços, ativos de rede, banco de dados e alertas em caso de problemas. A customização na coleta de dados pelo Zabbix é feita através de sua interface *web*, permitindo incluir qualquer chave SNMP ou Agente Zabbix para coleta de dados em um grupo ou *host* isolado. A interface *web* também é usada para criar os gráficos a partir de dados coletados, mapas, eventos e alertas ao administrador.

Com base nos testes realizados nas ferramentas apresentadas, a indicação para uso em ambientes de médio e grande porte é o Zabbix. Em ambientes pequenos ou onde apenas é necessário gerar gráficos estatísticos com dados locais ou remotos usando SNMP, sem a necessidade de nenhum outro recurso, o Cacti pode ser usado devido a sua praticidade. O Zabbix é equivalente ou melhor que o uso conjunto de todas as outras ferramentas apresentadas, permitindo ao administrador obter informações extremamente minuciosas sobre as mais diversas chaves SNMP, servidores, serviços, emissão de alertas, etc. Além disso, possui uma instalação rápida e simplificada para o Servidor e Agente Zabbix e uma interface *web* simplificada para sua configuração. Uma sugestão de melhoria para esse aplicativo é o aperfeiçoamento do cadastro de itens para coleta de dados em um ou mais *hosts*. Esse cadastro pode se tornar repetitivo dependendo do tamanho da rede e quantidade de *hosts* existentes, assim como a quantidade de itens a serem monitorados. É interessante, por exemplo, uma opção que replicasse os itens de um *host* para outro.

#### 4. Comentários Finais

Ter à disposição informações sobre o comportamento de servidores, ativos de rede e qualquer outro dispositivo que possa ser monitorado, ajuda a manter a estabilidade, performance e disponibilidade do ambiente computacional. Isso ocorre graças à possibilidade de acompanhar os horários de pico, detecção de problemas e avaliação de cada ponto em busca de melhorias.

As ferramentas de *software* livre expostas no artigo são capazes de mostrar ao administrador de forma eficiente e confiável, informações históricas sobre toda a rede, alertá-lo sobre falhas ou qualquer outro mal funcionamento a fim de evitar problemas ou tornar seu reparo o mais rápido possível. Implementando um sistema de monitoramento, preferencialmente o Zabbix é possível obter informações detalhadas sobre servidores, equipamentos de rede, recebimento de alertas, mapas da rede, etc., ajudando a acompanhar o funcionamento da rede e dos serviços como um todo.

#### Referências

- Berry, I., Roman, T., and Adams, L. (2005). *The Cacti Manual*. The Cacti Group.
- Comer, D. E. (2001). *Redes de Computadores e Internet*. Bookman, Porto Alegre, 2 edition.
- Galstad, E. (2006). *Nagios Version 2.0 Documentation*.
- Mauro, D. and Schmidt, K. (2001). *Essential SNMP*. O'Reilly, Sebastopol.
- Oetiker, T. (2005). *RRDtool Documentation*. Olten.
- Oetiker, T. (2006). *MRTG Documentation*. Olten.
- Vladishev, A. (2000). *Zabbix Manual*. ZABBIX SIA.