Um Estudo Comparativo de Ferramentas Baseadas em Código Livre para o Controle e Monitoramento de Redes

Adriano M. Meier[1], Douglas D. J. de Macedo[1,2], Rafael R. Righi[1], Diego L. Kreutz[3], M. A.R. Dantas[2]

[1]Faculdade de Tecnologia SENAI Florianópolis – SENAI-SC
Centro de Tecnologia em Automação e Informática – CTAI

[2]Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento – PPGEGC
Universidade Federal de Santa Catarina (UFSC) – Florianópolis, SC – Brasil

[3]Centro de Tecnologia de Alegrete – CTA
Universidade Federal do Pampa (UNIPAMPA) – Alegrete, RS – Brasil

{adriano,righi}@ctai.senai.br,{douglas,kreutz}@computer.org, mario@inf.ufsc.br

Resumo. *O crescimento acentuado de aplicações associadas à utilização das redes de computadores, torna cada dia mais complexa a tarefa de monitoramento desses ambientes. Com o intuito de reduzir a complexidade administrativa relativa a esse esforço, usualmente são empregadas ferramentas que auxiliam no controle e monitoramento de serviços e nodos das redes. No entanto, a variedade de soluções é tão grande que torna-se difícil a opção por uma determinada ferramenta, sem que um estudo mais criterioso seja realizado. Neste sentido, este trabalho apresenta uma análise empírica entre algumas soluções de gerenciamento de redes, cujo objetivo é auxiliar na escolha de uma determinada ferramenta, considerando-se um ambiente específico de rede. Os resultados experimentais são baseados e analisados, levando-se em conta cinco ferramentas de gerenciamento baseadas em código livre, que foram escolhidas devido as facilidades que essas podem prover no dia-a-dia para os administradores de sistemas.*

1. Introdução

O número e o tamanho das redes de computadores crescem à medida que a quantidade de informação e de usuários que precisam dessas informações aumentam. Entretanto, este crescimento e as diferentes tecnologias utilizadas acabam dificultando as tarefas de gerenciamento dessas redes.

Devido ao cenário apresentado, diversas ferramentas de monitoramento de dispositivos e sistemas em rede têm sido desenvolvidas. O principal propósito das soluções de gerenciamento é facilitar o trabalho de administradores de rede e gerentes de tecnologia da informação. Os critérios que levam a escolha das ferramentas podem incluir custo, plataforma utilizada, forma de distribuição da licença, segurança no processo de gerência, abrangência do monitoramento, facilidade de instalação, configuração, utilização, confiabilidade e documentação. Atualmente a tendência é que as soluções não sejam baseadas em apenas uma ferramenta, mas sim, desenvolvidas através da integração de várias ferramentas, protocolos e tecnologias.

Os motivos que levam administradores de sistemas a dar atenção especial ao gerenciamento efetivo das redes podem ser variados. Entre eles podem ser citados: melhorar o desempenho das comunicações, garantir um maior nível de segurança, maximizar a disponibilidade de serviços e recursos, registrar e armazenar a ocorrência de eventos e contabilizar o uso de recursos. Todas essas questões dizem respeito às cinco áreas funcionais da gerência de redes: falhas, configuração, contabilização, desempenho e segurança.

Este artigo tem como objetivo apresentar os resultados da análise de cinco ferramentas de controle e monitoramento de redes, sendo elas: MRTG (*Multi Router Traffic Grapher*), NTOP (*Network Traffic Probe*), Cacti, Zabbix e Nagios. A análise é baseada na comparação de algumas funcionalidades importantes em gerenciamento de redes, como suporte a SNMP (*Simple Network Management Protocol*), agentes e funcionamento em modo promíscuo (como *sniffer*), além de características das interfaces de controle e tipos de dados monitorados.

A estrutura do artigo é composta por cinco seções, sendo a presente seção a primeira delas. Na seqüência, a seção 2 sintetiza alguns aspectos relacionados ao SNMP. A seção 3 apresenta as ferramentas utilizadas na análise. Os resultados da avaliação comparativa são pormenorizados na seção 4. O documento encerra com a conclusão, além de apresentar possíveis complementos à pesquisa, a título de trabalhos futuros.

2. O Protocolo SNMP

A gerência de redes está em constante transformação, sendo lançadas novas ferramentas e soluções constantemente. No entanto, novos protocolos para a gerência de redes não surgem com a mesma velocidade. O protocolo padrão (*de facto*) para a gerência de redes TCP/IP é o SNMP, que evoluiu desde 1988 – ano em que as bases para este protocolo foram lançadas [Stallings, 1998].

O SNMP é um dos componentes que formam uma arquitetura de gerência de redes. Ele representa o protocolo utilizado para o tráfego de informações entre o agente (recurso gerenciado) e o gerente da rede, que centraliza, processa e apresenta informações ao profissional de rede. Os demais componentes são a MIB (Base de Informações de Gerenciamento) e a SMI (Estrutura da Informação de Gerenciamento) [Stallings, 1998].

Grande parte dos dispositivos de rede vem com suporte a SNMP. Além disso, as principais ferramentas de gerenciamento de redes também apresentam recursos que permitem o uso desse protocolo na administração de recursos disponíveis em rede.

3. Apresentação das Ferramentas

A escolha das ferramentas levou em consideração aspectos como o fato de ela estar disponível livremente e estar entre as soluções utilizadas com maior freqüência na prática do dia-a-dia de administradores de sistemas. Com isso, foram escolhidas as seguintes ferramentas [Freshmeat, 2007]: MRTG, NTOP, Cacti, Zabbix e Nagios.

Nas subseções seguintes as ferramentas serão apresentadas e as suas principais funcionalidades expostas. Foram levadas em consideração as características técnicas de cada ferramenta, visando a sua utilização para o auxílio ao gerenciamento das redes.

3.1 MRTG

O MRTG é uma ferramenta de monitoramento, desenvolvida na linguagem de programação *Perl* por Tobias Oetiker e Dave Rand, muito utilizada na gerência de redes [Oetiker, 2007]. Um de seus maiores usos é no monitoramento do tráfego de rede. Contudo, suas funcionalidades vão além, incluindo suporte ao monitoramento de dispositivos como servidores, roteadores e *switches*. A coleta dos dados é realizada através do protocolo SNMP ou por meio de *scripts* [Oetiker, 2001].

Apesar das funcionalidades de monitoramento de dispositivos conectados em rede, algumas deficiências foram detectadas. Exemplos incluem: 1) o baixo refinamento do intervalo de monitoramento, sendo que o menor intervalo é de cinco minutos, o que pode ser um problema em determinadas situações; 2) a falta de uma interface (*frontend*) de configuração; 3) a probabilidade de perdas em desempenho no monitoramento de cenários maiores, pois a ferramenta é responsável, além da coleta dos dados, por gerar gráficos e páginas HTML.

3.2 NTOP

O NTOP foi desenvolvido em 1998 por Luca Deri. Ele possui um servidor HTTP(S) nativo e gera uma série de gráficos e estatísticas de todo o tráfego na rede em tempo real, detalhando a utilização por equipamento, protocolo e serviços, e possui também um modo interativo [Deri, 2007].

Os principais focos do NTOP estão no monitoramento e medida do tráfego, no planejamento e otimização da rede e na detecção de violações na segurança. Com ele pode-se controlar a utilização da rede, descobrindo os diferentes tipos de tráfegos, protocolos mais utilizados, origem e destino dos pacotes, assim como de onde vem o tráfego mais “pesado” e quais os destinos mais acessados [Deri, 2000].

Outros tipos de dados que podem ser verificados com o NTOP são o valor atual, valor médio e o valor de pico do uso da largura de banda, tráfego total de *multicast* recebido pelos *hosts*, conexões TCP ativas e tráfego UDP total. Todas as informações são disponibilizadas na forma de gráficos e tabelas, o que facilita a interpretação dos dados para eventuais análises.

Essas informações podem ser úteis no planejamento e otimização de uma rede, pois provêem uma visão mais precisa de gargalos e áreas que necessitam de maior atenção. Complementarmente, o NTOP é capaz de fornecer informações sobre serviços de rede ativos, como HTTP (*HyperText Transfer Protocol*), SMTP (*Simple Mail Transfer Protocol*), DNS (*Domain Name System*) e DHCP (*Dynamic Host Configuration Protocol*)[Deri, 2001].

3.3 Cacti

O Cacti é uma ferramenta de monitoramento criada por Ian Berry e é distribuída sob os termos da GPL. Ela surgiu como uma opção de *frontend* para o RRDTool (*Round-Robin Database Tool*), que é o responsável por armazenar os dados coletados de dispositivos e sistemas da rede, através do SNMP ou de *scripts*, e posteriormente gerar os gráficos de utilização dos recursos [Berry, 2007].

O Cacti disponibiliza um ambiente de operação agradável e acessível com con-

trole de acesso por nível de usuário. Tanto as informações de controle quanto os dados coletados são armazenados em um banco de dados MySQL.

A arquitetura da ferramenta é modular, de forma que prevê a possibilidade de expansão. Esta pode dar-se através de *plugins* (ou *add-ons*) desenvolvidos por usuários da ferramenta e disponibilizados na Internet. Os *plugins* adicionam novas funcionalidades, complementando os casos de utilização do Cacti.

3.4 Zabbix

O Zabbix é uma ferramenta de monitoramento livre distribuída sob a licença GPL. Ela foi desenvolvida por Alexei Vladishev. Ela permite que praticamente toda a intraestrutura de uma rede, como servidores, aplicações e dispositivos, seja monitorada. A ferramenta pode ser instalada em diferentes plataformas, como: Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD e Mac OS/X [Vladishev, 2007].

Serviços de rede como HTTP, POP3, IMAP e SSH podem ser monitorados, sem o uso de agentes, por esta ferramenta. Além disso, ela provê suporte nativo ao protocolo SNMP, um dos únicos padrões de gerenciamento amplamente difundidos.

Os dados de monitoramento coletados são armazenados em um banco de dados MySQL ou PostgreSQL. Os gráficos estatísticos, a partir dos dados coletados, são gerados em tempo real. A visualização deles é dada através de uma interface de gerenciamento *web* amigável, o que facilita o entendimento e a operação.

Outras características da ferramenta incluem o suporte a SLA (Acordos de Nível de Serviço), configurações para envio de notificações por e-mail ao administrador do domínio caso eventos relevantes ocorram [Vladishev, 2007].

3.5 Nagios

O Nagios é um monitor de rede desenvolvido por Ethan Galstad. Ele opera em plataformas GNU/Linux e outras variantes Unix, sendo distribuído gratuitamente sob a licenas GPL. O nome original da ferramenta era Netsaint. Sua estrutura é modular, o que permite que novas funcionalidades sejam adicionadas na forma simples de *plugins*.

O Nagios é capaz de monitorar e fornecer informações sobre serviços de rede como HTTP, POP3, IMAP, SMTP e FTP. Esta ferramenta possibilita também suporte para o monitoramento de equipamentos como servidores, roteadores e *switches*. Os dados monitorados incluem carga de processamento, uso da memória e uso de discos. Estes dados podem ser coletados tanto local quanto remotamente [Galstad, 2007].

As opções de configuração da ferramenta permitem, por exemplo, programá-la para enviar notificações aos administradores da rede quando problemas ocorrem. Uma notificação, através do Nagios, pode ser enviada por e-mail, *pager* ou SMS. Adicionalmente, elas podem ser direcionadas a um grupo de pessoas de acordo com o tipo de problema detectado.

Os resultados das atividades de monitoramento do Nagios são exibidos no formato *web* padrão, sendo possível visualizá-las através de um navegador qualquer. As informações coletadas podem ser armazenadas para que sejam utilizadas posteriormente para gerar e visualizar históricos do estado de serviços e dispositivos da rede. O arma-

zenamento pode ser feito em um banco de dados (MySQL ou PostgreSQL) ou ainda em arquivos de texto.

4. Análise das Ferramentas

As cinco ferramentas, NTOP, MRTG, Cacti, Zabbix e Nagios, foram instaladas, configuradas e testadas na prática, monitorando uma rede de computadores. O cenário foi composto por um servidor Linux, onde foram instaladas todas as ferramentas, por um roteador ADSL com suporte a SNMP e como cliente foram usados cinco computadores com o Microsoft Windows XP Professional®. Nos próximos parágrafos são apresentadas algumas inferências tomadas durantes os experimentos das ferramentas.

O NTOP se mostrou uma ferramenta muito útil no monitoramento de redes locais, uma vez que pode fornecer informações sobre o que os usuários da rede estão acessando. Ele informa também a quantidade de tráfego, os sites acessados e protocolos utilizados. Consegue ainda detectar a presença de diferentes serviços como servidores *web*, servidores de nomes e *gateways* na rede. Esses dados podem ser utilizados para tomadas de decisão quanto aos pontos a serem melhorados ou corrigidos na rede, como um controle mais rígido o tipo de conteúdo acessível por determinados conjuntos de usuários.

Um de seus pontos fracos, embora não determinante, é referente ao seu funcionamento como *sniffer* da rede, que exige que ele seja instalado no *gateway* da rede ou que a porta do *switch* em que o computador estiver conectado seja configurada para receber todos os quadros que estão trafegando. Além disso, sua atuação como ferramenta de monitoramento restringe-se a redes locais.

O MRTG, apesar de ser um dos mais conhecidos e utilizados, não possui um conjunto extenso de recursos. Para que seja possível a coleta de dados sem a utilização do SNMP é necessário ter algum conhecimento em linguagem de programação para que sejam desenvolvidos algoritmos específicos para essa função, além da criação do arquivo de configuração para o MRTG. Isso não inviabiliza sua aplicação, apenas exige maiores conhecimentos do responsável.

Por outro lado, o Cacti pode gerar gráficos idênticos aos gerados pelo MRTG, além de contar com uma maior variedade de aplicações. Como o Cacti utiliza o RRDTool e, devido ao modo de que RRD armazena as informações, seu desempenho é melhor [Berry, 2007], se comparado ao atingido com o MRTG, sendo possível definir tempos menores que cinco minutos para o processo de *polling* (o MRTG só permite esta particularidade quando integrado ao RRDTool). É possível ainda definir diferentes permissões de acesso para os seus usuários e sua operação é totalmente realizada via interface *web*.

Entre as funcionalidades do Zabbix, além de monitorar basicamente todos os itens da rede, está aquela que gera informações de inventário e de SLA (Acordo de Nível de Serviço) – sendo estes seus principais diferenciais. Ele permite configurar níveis de acesso do tipo *somente leitura* e também é configurado através do navegador. A sua pró-atividade, em caso de falhas, se mostrou um ponto forte durante os testes práticos.

No caso de monitoramento de serviços, o Nagios se mostrou a melhor opção; principalmente em ambientes onde se deseja uma visão global da rede. Outro marco positivo desta solução é seu grau de extensão através da utilização de *plugins*. No entanto,

ele não gera gráficos estatísticos e seu método de configuração é complexo; realizado quase que totalmente via edição manual de arquivos, o que o torna pouco amigável.

As Tabelas 1 a 5 comparam os itens pertinentes relacionados às cinco ferramentas de monitoramento de rede analisadas. Aspectos não oficiais das soluções, como melhoramentos de outros desenvolvedores, foram ignorados na pesquisa. O foco da análise centrou-se apenas nas funcionalidades nativas das ferramentas.

Tabela 1 – Método de coleta de dados das ferramentas.

	Método de coleta de dados		
	SNMP	**AGENTE**	***Sniffer***
MRTG	Sim	Não	Não
NTOP	Não	Não	Sim
CACTI	Sim	Sim	Não
ZABBIX	Sim	Sim	Não
NAGIOS	Sim	Sim	Não

Como pode ser observado na Tabela 1, apenas o MRTG possui uma única forma de coleta de dados. As demais ferramentas possuem pelo menos dois mecanismos distintos para monitorar serviços e dispositivos de rede. Para esta pesquisa o conceito "agente" possui dois significados, dependendo da sua semântica. No primeiro, destaca-se o agente SNMP pertencente à arquitetura de gerenciamento e na segunda, chama-se de agente o método de coleta de informações onde existe um software cliente no dispositivo monitorado, o qual envia sistematicamente dados a uma central (gerente).

A Tabela 2 mostra que apenas o MRTG não é configurável via interface web, não possui controle de acesso e não possui suporte para o envio de alertas através de e-mail. Considerando-se essas três características, as ferramentas mais completas são o Cacti, o NTOP e o Zabbix.

Tabela 2 – Algumas funcionalidades das ferramentas.

	Funcionalidades		
	Configuração via interface web.	**Controle de acesso**	**Envio de alertas por e-mail**
MRTG	Não	Não	Não
NTOP	Sim	Sim	Não
CACTI	Sim	Sim	Sim
ZABBIX	Sim	Sim	Sim
NAGIOS	Não	Sim	Sim

As quatro características relativas ao tipo de monitoramento, carga dos enlaces, disponibilidade dos serviços da rede, recursos de hardware e tráfego da LAN são as métricas utilizadas na Tabela 3. Pode ser observado, nesse caso, que a ferramenta Zabbix fornece a maior diversidade de funcionalidades de monitoramento, sendo este um dos seus pontos fortes.

Tabela 3 – Tipo de monitoramento realizado pelas ferramentas.

Tipo de monitoramento				
	Carga dos links	**Disponibilidade dos Serviços**	**Recursos de Hardware**	**Tráfego da LAN**
MRTG	Sim	Não	Não	Não
NTOP	Não	Não	Não	Sim
CACTI	Sim	Não	Sim	Não
ZABBIX	Sim	Sim	Sim	Não
NAGIOS	Não	Sim	Sim	Não

Na métrica relativa ao suporte à bancos de dados, ilustrado na Tabela 4, as ferramentas Nagios e Zabbix têm um desempenho diferencial, pois apresentam suporte a MySQL e PostgreSQL. Por outro lado, as demais ferramentas apresentam apenas suporte a arquivos ou a um desses dois bancos de dados.

Tabela 4 – Integração com banco de dados.

Integração com banco de dados		
	MySQL	**PostgreSQL**
MRTG	Não	Não
NTOP	Não	Não
CACTI	Sim	Não
ZABBIX	Sim	Sim
NAGIOS	Sim	Sim

A Tabela 5 apresenta comparações relativas a características como: documentação integrada a ferramenta, suporte a geração de gráficos, suporte ao protocolo SNMPv3 e suporte a *plugins*. Os resultados demonstram que cada ferramenta possui as suas particularidades. Dependendo do peso que o administrador da rede alocar a cada um dos itens avaliados, uma ferramenta poderá ser mais interessante que outra. A classificação entre melhor e pior dependerá do cenário de uso e perfil do administrador.

Tabela 5 – Outras características das ferramentas.

Outras características				
	Documentação integrada	**Geração de gráficos**	**Suporte ao SNMPv3**	**Suporte a plugins**
MRTG	Não	Sim	Sim	Não
NTOP	Sim	Sim	Não	Sim
CACTI	Não	Sim	Sim	Sim
ZABBIX	Não	Sim	Sim	Não
NAGIOS	Sim	Não	Sim	Sim

5. Conclusão

O estudo realizado neste trabalho procurou abordar as principais características disponíveis nas versões nativas das cinco ferramentas de monitoramento de redes, MRTG, NTOP, Cacti, Zabbix e Nagios. As funcionalidades e recursos variam entre as ferramentas, sendo que a importância de cada item dependerá substancialmente do cenário de uso e do perfil do administrador da rede.

Ferramentas como o Nagios podem ser utilizadas para monitoramento de servidores de rede. Por outro lado, ferramentas como o NTOP são uma boa opção para monitoramento do tráfego de redes locais. Já para o monitoramento de enlaces WAN seriam necessárias soluções como o Cacti ou o Zabbix, principalmente devido às várias funcionalidades disponíveis, como envio de alertas, armazenamento das informações de monitoramento em banco de dados, monitoramento pró-ativo e melhor maneira de visualização dos dados na forma de gráficos.

Por fim, dependendo do cenário e das necessidades administrativas, o uso conjunto das diferentes ferramentas de monitoramento de redes pode trazer resultados frutíferos à administração das mesmas. Os resultados produzidos por este trabalho podem servir de apoio no processo de escolha entre uma ou mais ferramentas que podem ser mais convenientes e úteis no gerenciamento de um ambiente em particular. Cabe ao administrador deste ponderar entre as diferentes características e pontos fortes das ferramentas aqui apresentadas. Apresenta-se como um potencial trabalho futuro a comparação das ferramentas destacadas nesta pesquisa com aquelas de mesmo objetivo, porém de natureza comercial, como o HP OpenView, o IBM Tivoli NetView e o CiscoWorks.

Referências

Berry, I.. CACTI. Disponível em: <http://www.cacti.net>. Acesso em: 23/07/2007.

Deri, L.. Suin, S. “Effective Traffic Measurement using ntop”. *IEEE Communications Magazine*, vol. 38, n. 5, pp. 138-143, Maio, 2000.

Deri, L.; Carbone, R.; Suin, S., "Monitoring networks using ntop". *Proceedings of the IEEE/IFIP International Symposium on Integrated Network Management*, 2001.

Deri, L.. NTOP. Disponível em: <http://www.ntop.org>. Acesso em: 15/07/2007.

Freshmeat. Disponível em: <http://freshmeat.net>. Acesso em: 10/07/2007.

Galstad, E.. NAGIOS. Disponível em: <http://www.nagios.org>. Acesso em: 11/07/2007.

Oetiker, T.. MRTG. Disponível em: <http://www.mrtg.org>. Acesso em: 28/07/2007.

Oetiker, T.. "Monitoring Your IT Gear: The MRTG Story". *IT Professional*, vol. 03, n. 6, pp. 44-48, Nov/Dec, 2001.

Stallings, W.. SNMP, SNMPv2, SNMPv3, and RMON 1 and 2. Ed. Adisson Wesley, 3ª edição, USA, p. 71-121, 1998.

Vladishev, A.. ZABBIX. Disponível em: <http://www.zabbix.com>. Acesso em: 12/07/2007.