

## **DIREÇÕES NO MONITORAMENTO EM REDES DE LARGA ESCALA: UMA VISÃO GERAL, FERRAMENTAS E TENDÊNCIAS**

Rafael Couto Barros, Marcelo Anderson Batista Santos

Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano-campus  
Salgueiro; rafaelcoutobarros10@gmail.com, marcelo.santos@ifsertao-pe.edu.br

**RESUMO:** Ferramentas de monitoramento em redes de computadores são essenciais para determinar se a rede está em seu perfeito funcionamento, detectar falhas e avaliar seu desempenho. Redes de largas escala trazem um desafio maior para seu monitoramento por haver uma grande quantidade de geração de dados em intervalos de tempo curtos, necessitando geralmente de uma infraestrutura de monitoramento distribuída e processamento dos dados de forma eficiente. Na literatura diversas ferramentas que possuem características diferentes, coletam métricas diferentes e executam em diferentes tipos de plataforma. Dessa forma, temos como objetivo realizar uma análise das ferramentas disponíveis, seus pontos fortes e fracos e suas características, facilitando a escolha da ferramenta que se adequa a determinada necessidade.

**Palavras-chave:** Monitoramento, Redes de Larga Escala e Gerenciamento de Rede

**ABSTRACT:** Monitoring tools in computer networks are essential to determine if the network is working correctly, detect faults and evaluate its performance. Large-scale networks bring new challenges due to the high amount of generation of data in short time intervals, usually requiring a distributed infrastructure monitoring and data processing efficiently. In the literature, there are several tools, each one with specific characteristics, collecting different metrics, and working on different platforms. Thus, we aim to carry out an analysis of the available tools, their strengths and weaknesses and their characteristics, facilitating the choice of the adequate tool to appropriate needs.

**KEYWORDS:** Monitoring, Large-Scale Networks, and Network Management.

### **INTRODUÇÃO**

A expansão da internet possibilitou a interligação de um número inimaginável de usuários, passando de algumas centenas de dispositivos conectados a mais de três bilhões em um curto intervalo de tempo . Juntamente com o crescimento do número de usuários, a estrutura da Internet tornou-se complexa sendo composta pela interligação de diferentes redes e milhares de dispositivos heterogêneos. Nesse contexto, é fundamental haver o monitoramento da rede para que através da avaliação do seu funcionamento seja possível mensurar seu desempenho, identificar erros e melhorar a qualidade do serviço oferecido. Assim, um dos principais mecanismos responsáveis por auxiliar os administradores da rede são as ferramentas de monitoramento, pois elas são

indispensáveis para que o pleno funcionamento da rede seja alcançado. O feedback dado por essas ferramentas é responsável por dar uma visão geral da rede, alertando os administradores sobre possíveis pontos de limitação, falha de servidores e mau funcionamento da rede, possibilitando que medidas específicas sejam adotadas para resolver um dado problema, evitando assim, por exemplo, possíveis quebras de acordos de serviços (SLAs) e conseqüentemente melhorando a qualidade de serviço oferecida.

Há, atualmente, uma variedade de ferramentas de monitoramento disponíveis no mercado fazendo com que haja dúvida em relação quais as mais apropriadas e melhores ferramentas para monitorar determinado serviço ou rede. Nesse contexto, redes de larga escala trazem consigo desafios adicionais pela quantidade de informações geradas em um curto espaço de tempo, acarretando problemas de armazenamento, processamento das informações coletadas em tempo hábil para uma tomada de decisão e até mesmo dificuldades para gerar uma visualização agregada dos dados coletados de forma eficiente.

Assim, esse artigo tem como objetivo levantar o estado da arte dos principais softwares de monitoramento em redes de larga-escala, suas características, pontos fracos e fortes, para que administradores de rede e pesquisadores tenham uma visão clara do seu funcionamento e conseqüentemente consigam optar por uma ferramenta que atenda às suas necessidades.

## **MONITORAMENTO DE REDES: DESAFIOS E PERSPECTIVAS**

A Internet é formada por diversos dispositivos conectados entre si, como roteadores, switches, estações de rede sem fio, computadores etc. Esses dispositivos são interligados através de enlaces de comunicação (com fio ou sem fio) formando uma rede complexa e heterogênea. Com a popularização da Internet e uma dependência crescente dos usuários estarem conectados, é essencial que exista um mapeamento do funcionamento da rede para que se tenha uma visão clara de sua performance e conseqüentemente sua eficiência.

A área de monitoramento em redes computadores é um campo de estudo importante que levanta discussões atuais como, por exemplo, dentro do maior fórum de discussões sobre padrões para a Internet conhecido como IETF (Internet Engineering Task Force) que possui um grupo de discussão voltado apenas para avaliação e medição (BMWG – Benchmarking Methodology Work Group).

Nesse contexto, com a disponibilização de diferentes serviços, interconexão de diferentes tipos de redes e dispositivos, torna-se primordial monitorar o funcionamento dos serviços e redes corrigindo eventuais erros o mais rapidamente possível. Conseqüentemente, diversas ferramentas surgiram no mercado com diversas características e atendendo a demandas diferentes. Assim, na próxima seção realizamos um levantamento das principais ferramentas de monitoramento e suas principais características, servindo como material de referência para determinar qual a ferramenta de monitoramento é adequada de acordo com uma necessidade específica.

## **FERRAMANTAS DE MONITORAMENTO: UMA VISÃO GERAL**

Nesse tópico, foi feito o levantamento de algumas ferramentas de monitoramento, com o objetivo de demonstrar as suas respectivas funções, assim como suas características, pontos fracos e fortes. As ferramentas analisadas são: Zabbix (ARCENIO, 2010), Nagios (OLIVEIRA, 2007), Collectl (BLACK, 2008), OpenNMS, Munin (PRADO, 2015), Monit(LESSA, 2000), Cacti, Icinga e Pandora FMS.

**Zabbix:** É uma ferramenta bastante utilizada para monitorar vários parâmetros da rede, pensada para monitorar a disponibilidade, experiência de usuário e a qualidade de serviços, com um sistema de alerta bem flexível que permite alertas por e-mail, possibilitando que medidas de correção dos erros no sistema sejam adotadas com rapidez e de forma eficaz. O Zabbix tem uma estrutura de código aberto, pois está escrito e distribuído sob a GNL (*General Public license*), tendo sua estrutura dividida em vários componentes, os principais e mais conhecidos são: zabbix sever, zabbix proxy e zabbix agent, destes apenas o zabbix sever é instalado em um servidor dedicado gerenciado pelo administrador da rede.

Abaixo temos as principais vantagens e desvantagens em se utilizar o sistema de monitoramento Zabbix:

### Pontos Positivos:

- Solução open source;
- Suporte para SNMP;
- Monitoramento distribuído com administração centralizada na web;
- Agentes de alto desempenho;
- Interface web.

### Pontos Negativos:

- Não realiza o monitoramento de outros serviços, apenas monitoramento de desempenho e disponibilidade dos ativos;
- O Unix é o único sistema operacional que pode consistentemente responder ao desempenho necessário para instalação do zabbix;

**Nagios:** O Nagios é a ferramenta mais conhecida e mais utilizada no contexto de monitoramento de rede de pequena e de larga escala. É utilizado em empresas de pequeno, médio e grande porte, sendo um dos programas mais completos de gerenciamento e monitoramento de redes, oferece uma estrutura open source (código aberto) sob a licença (GPL), ou seja, é um software de licenciamento livre. Oferece o monitoramento de toda estrutura da rede de serviços e hosts, alertando quando um problema é detectado e quando ele é resolvido, esse alerta pode ser feito através de efeitos sonoros, e-mail e até mesmo nos celulares dos administradores. A seguir há uma lista com as principais vantagens em utilizar Nagios assim como suas desvantagens:

#### Pontos Positivos:

- Manutenção preventiva: O programa alerta possível falhas no sistema, possibilitando assim que medidas sejam adotadas para resolver essas anormalidades, evitando assim possíveis transtornos aos usuários.
- Monitora toda sua infraestrutura de rede: a ferramenta pode monitorar vários servidores, possibilitando assim que todos os parâmetros monitorados sejam agregados em uma única interface.
- Aumento da produtividade dos administradores e analistas da rede: tendo em vista que monitora os ativos de forma automática, isso possibilita que novos plug-ins (componentes que adicionam mais opções ao sistema operacional, navegadores, games etc.) sejam instalados na máquina.
- Integração com plug-ins: o próprio usuário pode escrever as linhas de comandos para automatizar e facilitar ainda mais o monitoramento da rede, o código pode ser escrito em diferentes linguagens de programação.
- Age prontamente e executa ações de resolução de problemas: ou seja, o programa alerta o administrador quando é detectado algum problema no sistema e quanto o problema é resolvido reduzindo assim o tempo de resposta em casos de problemas.

#### Pontos Negativos:

- Falta de recursos gráficos de configuração: exige do usuário certo conhecimento na área de redes, para que assim ele possa configurar o sistema.
- Atraso de configuração do sistema: Ocorrerá pelo menos até o administrador adquirir intimidade com a ferramenta em questão.
- Indisponibilidade de ferramentas de configuração na interface web: Dessa forma toda a configuração tem que ser executada manualmente.
- Apresenta certa limitação para se adaptar á rápida evolução das redes atuais: Provenientes de bugs não corrigidos.

**Collectl:** É uma ferramenta de monitoramento básica que tem a capacidade de capturar diversas métricas de uma única máquina. Diferentemente de outros softwares de monitoramento ele não possui uma estrutura cliente-servidor. Coleta métricas tais como: CPU, disco, memória, rede, soquetes abertos etc. Abaixo há uma lista com as principais características da ferramenta.

Pontos positivos:

- Executado de forma interativa;
- Capacidade de monitorar boa parte do subsistema;
- Capacidade de gravar e reproduzir os dados armazenados;
- Exportação de dados em vários formatos;
- Monitoramento de máquinas remotas assim como um cluster de servidor inteiro;
- Exibição de dados no terminal;

Pontos negativos:

- Incapacidade de gerar gráficos;
- Ferramenta não distribuída;

**OpenNMS:** OpenNMS é um software livre que não possui taxa de licença, criado para o monitoramento de empresas, atua principalmente na camada de aplicação. É responsável por monitorar e fazer a coleta dos dados transformando as informações em gráficos estatísticos e base de dados para inventários. Abaixo há uma lista com as principais vantagens, assim como as desvantagens do OpenNMS:

Pontos Positivos:

- Ferramenta Open Source;
- Flexibilidade nas configurações;

- Armazenamento das informações em base de dados;
- Permite a configuração de comandos;

Pontos Negativos:

- Documentação precária;
- Ausência de interface para configuração;

**Munin:** É um software livre, sob a licença GPL, pode ser instalado em qualquer plataforma Unix. Caracterizado por possuir uma ênfase plug and play (ligar e usar), apresenta resultados em forma de gráfico a partir de uma interface web. Os gráficos provenientes dos dados extraídos da ferramenta são formados sobre variados temas como: uso de memória, CPU, carga dos discos, desempenho do MYSQL, tráfego na placa de rede e etc. A seguir uma lista com as principais características da ferramenta:

Pontos Positivos:

- Arquitetura simples;
- Monitoramento de vários parâmetros;
- Determina com antecedência quando um recurso é usado em demasia;

Pontos Negativos:

- Apenas alertas parciais;
- Seus gráficos perdem precisam com o tempo;

**Monit:** É um software que consome poucos recursos, responsável por monitorar de forma automática estruturas da rede, criado principalmente, para monitorar e ajustar a estrutura de processos *daemon* tais como: Sendmail, Apache e MySQL. A seguir há uma lista com suas principais características do software:

Pontos positivos:

- Monitora conexões de rede com vários servidores tanto em localhost ou em máquinas remotas;
- Sistema autônomo: não depende de plug-ins ou outra biblioteca qualquer para ser executado;
- Open Source;

Pontos negativos:

- Configuração Complexa;
- Ferramenta não distribuída;

**Cacti:** É uma ferramenta que foi desenvolvida para ser flexível, armazena dados recolhidos, e faz um levantamento dessas informações em forma de gráficos. É especializado na monitoração de desempenho, uma das mais completas ferramentas para monitoramento de dispositivos remotos, funciona por meio da tecnologia PHP5 ou superior para consultar uma base de dados MySQL, a qual também administra. A seguir há uma lista com suas principais vantagens e desvantagens:

Pontos Positivos:

- Fácil manipulação;
- Gráficos customizáveis;
- Manipulação de dados usando funções matemáticas usando o RRDTool;
- Criação de fonte de dados utilizando o MySQL;
- Coleta de dados por meio de scrips personalizados definidos pelo usuário;
- Recuperação de dados através do SNMP (Simple Network Management Protocol);
- Criação de hierarquias gráficas;
- Controle de permissões;
- Interface intuitiva e agradável;

Pontos Negativos:

- É apenas uma interface de gerenciamento, para que seja possível o monitoramento e levantamento de dados em gráficos. Necessita de softwares complementares como: RRDTool, MRTG ou Nagios.

**Icinga:** É uma ferramenta de código aberto, originalmente foi um fork do Nagios, feito principalmente, para o monitoramento de grandes instituições com vários serviços e hosts, com uma arquitetura modular autônoma. A seguir há uma lista com as principais vantagens assim como as desvantagens em se utilizar Icinga:

Pontos Positivos:

- Suporte MySQL, PostgreSQL e Oracle;
- Compatibilidade com recursos do Nagios;
- API robusta para integração com outras aplicações;
- Interface web bastante simples e fácil de usar;
- Sistemas de monitoração redundante através da criação de cluster;

Pontos Negativos:

- Necessidade de softwares complementares;

**Pandora FMS:** É software que permite a monitoração de hardware, software, aplicações e sistemas operacionais, funciona com o banco de dados MySQL. É uma estrutura que funciona tanto em ambiente ativo como em passivo, pode ser utilizado em um ambiente de cluster. Abaixo há uma lista com as principais vantagens e desvantagens da ferramenta:

Pontos Positivos:

- Capacidade de distribuição;
- Agentes enviam os dados coletados para os servidores de forma automática;
- Interface simples e fácil de utilizar;

Pontos Negativos:

- Documentação pobre;
- Instalação Complexa;

**Tabela 1.** Tabela comparativa demonstrando características das ferramentas de monitoramento.

TABELA COMPARATIVA								
	Plataforma	Distribuído	Sem Agentes	SNMP	Gráficos	Alerta	Licença	Controle Acesso
ZABBIX	C, PHP	Sim	Suportado	Sim	Sim	Sim	GPL	Sim
NAGIOS	C	Sim	Suportado	ViaPlug-in	Sim	Sim	GPL	Sim
COLLECTL	Perl	Não	Não encontrado	Sim	Não	Sim	Desconhecido	Não encontrado
OpenNMS	Java	Sim	Suportado	Sim	Sim	Sim	AGPLv3	Sim
MUNIN	Perl	Via nodes	Não	Sim	Sim	Parcial	GPL	Não encontrado
MONIT	C	Não encontrado	Não encontrado	Sim	Sim	Sim	AGPLv3	Não encontrado
CACTOS	C++,Java	Sim	Não	Sim	Sim	Sim	GPL	Sim
ICINGA	C	Sim	Suportado	Via Plug-in	Sim	Sim	GPL	Sim
Pandora FMS	Perl,PHP C++,Java-script	Sim	Suportado	Sim	Sim	Sim	GPLv2,	Sim



## CONCLUSÃO

Com o crescimento das Redes de Computadores é fundamental a existência de ferramentas de monitoramento para que possa ser possível avaliar o seu desempenho, disponibilidade dos recursos, manter a segurança da rede e proporcionar o menor tempo possível para uma recuperação de falha.

Dado a heterogeneidade da rede e diversidade de serviços oferecidos, existem demandas e métricas específicas que fazem com que determinada ferramenta de monitoramento seja mais adequada para um administrador de rede. Cenários de rede de alta velocidade, por exemplo, criam ainda mais desafios por haver a geração de uma grande quantidade de dados em curto intervalo de tempo, necessitando de grande poder de processamento para análises em tempo real. Assim, nesse contexto de monitoramento de redes de computadores, realizamos uma análise das ferramentas de monitoramento em redes de computadores e sua importância e suas principais características, pontos fortes e fracos. Verificamos que há uma grande quantidade de ferramentas disponíveis de forma gratuita e que oferecem uma ampla quantidade de serviços, no entanto a sua aplicabilidade dependerá da demanda do usuário, sendo este artigo uma referência para a tomada de decisão de qual ferramenta se adequa melhor a uma dada demanda.

Como trabalhos futuros pretendemos analisar ferramentas de monitoramento em novos paradigmas de redes como SDN (*Software Defined Network*) e NFV (*Network Functions Virtualization*).

## REFERÊNCIAS

ARCENIO, S. F. L. **Monitoramento de Dispositivos de Redes com Zabbix**. Universidade Federal da Grande Dourado, MS, Brasil 2010.

BLACK, L. T. **Comparação de Ferramentas de Gerenciamento de Redes**. Universidade federal do rio Grande do Sul, Porto Alegre, Dez.2008.

BENINI, A. R; SANTOS, M. **Monitoramento de Redes de Computadores**. Artigo revista Infra Magazine, Abr.2011.



MENEZES, S. E; SILVA, L. L. P. **Gerenciamento de Redes: Estudos de Protocolos.** Universidade Federal de Pernambuco, Recife, Set.1998.

Oliveira, Ricardo Luiz. "GERENCIAMENTO EM REDES UTILIZANDO A FERRAMENTA NAGIOS." (2007).

Prado, Rodrigo Braga. "Implantação de estrutura cliente/servidor na empresa Data Press." (2015).

