Comparação das Ferramentas de Gerenciamento de Redes de Computadores CACTI, NAGIOS e ZABBIX

Maicon Rafael Hammes[1], Rogério Evandro Hunhoff[1], Claudio Schepke[2]

[1]Curso de Tecnologia em Redes de Computadores
Sociedade Educacional Três de Maio (SETREM)
Av. Santa Rosa, 2405 Três de Maio - RS - CEP 98910-000.

[2]Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS)
Caixa Postal 15.064 – 91.501-970 – Porto Alegre – RS – Brazil

{maiconhammes,schepke}@gmail.com, rogerioh@luanett.com.br

Resumo. *Redes de computadores são cruciais para o desenvolvimento de qualquer atividade atualmente. No entanto, configurar e manter estas redes em perfeito funcionamento não é uma tarefa simples. Por causa disso é possível encontrar diversas ferramentas desenvolvidas para o gerenciamento de redes de computadores. Cada ferramenta, entretanto, possui características peculiares que precisam ser conhecidas pelo gerente da rede. Neste sentido este artigo apresenta uma comparação e análise do funcionamento de três ferramentas de gerenciamento de redes de computadores. Os resultados obtidos mostram que existem diferenças que podem ser impactantes para a escolha de uma em detrimento de outra.*

1. Introdução

O gerenciamento de redes traz diversos benefícios para as empresas pois auxilia no processo de detecção de falhas, bem como na prevenção das mesmas, fazendo com que não ocorra indisponibilidade dos serviços principais das organizações.

As ferramentas de gerenciamento existentes são muitas, entretanto poucas delas são eficientes, pois gerenciar não é só monitorar, e sim utilizar os gráficos gerados pelo monitoramento para corrigir as falhas. Este processo pode ser automático se for utilizado um software que possui gatilhos de segurança que disparam alertas via e-mail ou torpedo SMS.

Neste contexto, este trabalho apresenta a avaliação de 3 ferramentas de gerenciamento de redes de computadores, comparando suas principais características, bem como o seu funcionamento prático em testes de instalação e monitoramento de pequenas redes.

Este artigo está dividido em 5 seções. A próxima seção apresenta diversos conceitos ligados ao gerenciamento de redes de computadores. A Seção 3 descreve as 3 ferramentas avaliadas, bem como as observações práticas feitas na instalação e uso das mesmas. As principais características de cada uma dessas ferramentas encontra-se sumarizada em uma tabela na Seção 4. Por fim, na última seção, são apresentadas as conclusões e trabalhos futuros.

2. Gerenciamento de Redes de Computadores

Segundo Tanenbaum (2003), o gerenciamento de rede pode ser considerado como um controle de qualquer objeto possível de ser monitorado numa estrutura de recursos físicos e lógicos de uma rede, sendo eles em ambientes próximos ou distintos. Realizar o gerenciamento de uma rede de computadores torna-se um fator importante para garantir o bom funcionamento e da boa qualidade dos serviços oferecidos na mesma.

2.1. Tipos de Gerência de Redes

A seguir tem-se os tipos de gerência de redes:

- Centralizada: Um único gerente controla o processo. Quanto maior a rede mais problemas ela apresenta.

- Descentralizada: Existem diversos responsáveis pelo gerenciamento. Permite que o trabalho seja feito de forma hierárquica.

- Reativa: Neste modelo os administradores de rede eram alertados de problemas ocorridos na infra-estrutura e passavam a atuar em sua solução.

- Pró-Ativa: Gerencia eficaz com objetivo de prevenir os problemas interrompendo os serviços o mínimo possível. O presente projeto trata principalmente de Gerência Pró-ativa.

2.2. Etapas da Gerência da Rede

O processo de gerenciamento de uma rede de computadores passa pelos seguintes processos:

- Coleta de dados: É a monitoração dos recursos gerenciados e que também são armazenados em arquivos de logs.

- Diagnóstico: Esta etapa consiste no tratamento e análise realizados a partir dos dados coletados, para detecção da causa do problema no recurso gerenciado. São executados uma série de procedimentos manuais ou automáticos para determinar a causa do problema representado no recurso gerenciado.

- Ação: Atuar para resolver o problema diagnosticado em determinado recurso da rede.

2.3. Elementos da Gerencia de Redes

Segundo Dias e Jr. (2010), o gerenciamento das redes é composto pelo software gerente e pelo software agente.

O software gerente do protocolo SNMP é um programa executado em uma máquina servidora, que possibilita enviar e receber informações de gerenciamento, junto aos dispositivos gerenciados mediante a comunicação com um ou mais agentes. O gerente fica responsável pelo monitoramento, relatórios e decisões na ocorrência de problemas, ou seja, é a interface para o gerente humano num sistema de gerenciamento de rede.

O software agente é um processo executado na máquina a ser gerenciada, responsável pela coleta, envio e manutenção das informações de gerência da máquina. As funções principais de um agente são atender as requisições enviadas pelo gerente e enviar automaticamente informações de gerenciamento ao gerente, quando previamente

programado.

Os agentes coletam junto aos objetos gerenciados as informações com um objetivo de analisar e detectar a presença de falhas no funcionamento dos componentes do gerenciamento. Após analise, será possível tomar providências no sentido de prevenir os problemas que ocorrem como conseqüência das falhas. Neste sentido o agente responde as solicitações de informações e de ações da estação de gerenciamento e deve também prover assincronamente informações importantes que não foram solicitadas por esta estação.

2.4. *Management Information Base*

Segundo Tanenbaum(2003) *Management Information Base* (MIB) é o conjunto dos objetos gerenciados, que procura abranger todas as informações necessárias para o gerenciamento da rede. Em 1990 foi realizada uma revisão de MIB, que passou a ser conhecida como MIB II. Nesta versão MIB é responsável por fornecer informações gerais de um equipamento gerenciado. Com ela é possível obter informações como, por exemplo, número de pacotes transmitidos, estado da interface, entre outras.

Segundo Specialski (2006), MIB contém informações de gerenciamento que refletem a configuração e o comportamento do objeto gerenciado, bem como parâmetros que podem ser usados para controlar a operação do objeto. O funcionamento da MIB ocorre da seguinte forma: o Gerente realiza uma solicitação sobre o tráfego de rede ao agente, por exemplo, onde o agente consulta a SMI que é responsável por descrever como os objetos estão contidos dentro da MIB. Na MIB, ficam armazenadas as informações sobre o objeto gerenciado. Após coletar os dados solicitados, o agente envia através do protocolo SNMP às informações para o gerente, no qual o programa de gerenciamento de SNMP vai realizar a tomada de decisão que a ele foi definida.

2.5. Áreas Funcionais de Gerenciamento

Segundo Specialski (2006), o gerenciamento foi dividido em áreas funcionais para descrever melhor as necessidades de cada área. São elas:

- Gerenciamento de Falhas: segundo Shammas(2004), gerenciamento de falhas possui a capacidade de monitorar os estados dos recursos, da manutenção de cada um dos objetos gerenciados, e pelas decisões tomadas de decisão para restabelecer as unidades do sistema que venham a dar possíveis problemas. A ocorrência de uma falha é uma condição anormal, onde a solução deve partir de uma ação do gerenciamento. Geralmente acontece por uma operação incorreta.

Para garantir o perfeito funcionamento do sistema, é necessário realizar o controle de cada componente, monitorando individualmente. Ao ocorrer uma falha, é de suma importância que seja possível identificar o componente onde ocorreu a mesma. Em seguida, tentar isolar a outra parte da rede para que a mesma continue funcionando e configurar a rede para que o impacto da falha afete o mínimo de processos e componentes.

- **Gerenciamento de Contabilização:** Segundo Shammas (2004), o gerenciamento de contabilização fornece meios para medir e coletar informações dos recursos e serviços disponibilizados na rede, para saber a taxa de uso dos mesmos, garantido assim que eles estejam sempre disponíveis. Segundo Specialski (2006), mesmo que nenhuma cobrança interna seja feita pela utilização dos recursos da rede, o

administrador da rede deve estar habilitado para controlar o uso dos recursos por usuário ou grupo de usuários, com o objetivo de: evitar que um usuário ou grupo de usuários abuse de seus privilégios de acesso e monopolize a rede, em detrimento de outros usuários; e evitar que usuários façam uso ineficiente da rede, assistindo-os na troca de procedimentos e garantindo a desempenho da rede; conhecer as atividades dos usuários com detalhes suficientes para planejar o crescimento da rede.

Quando é realizada a implementação, a função do gerenciamento de contabilização deve levar em consideração alguns aspectos: controlar o registro e a emissão dos dados relacionados à contabilização através dos objetos de controle de medida de contabilização; Coletar os dados de contabilização, usando os objetos de dados de medida de contabilização para representar os recursos contabilizados; E armazenar os resultados da contabilização para criar históricos de contabilização dos recursos através do uso de registros de contabilização.

- **Gerenciamento de Configuração:** Segundo Specialski (2006), o gerenciamento de configuração está relacionado com a inicialização da rede e com uma eventual desabilitação de parte ou de toda a rede. Também está relacionado com as tarefas de manutenção, adição e atualização de relacionamentos entre os componentes e do status dos componentes durante a operação da rede.

Alguns benefícios estratégicos, são por exemplo, auxiliar no planejamento estratégico da área de TI, garantir a confiabilidade das informações, demonstrar a eficiência e controle, entre outros. Já os benefícios operacionais auxiliam a esclarecer funções de cada ferramenta, auxiliar na identificação de problemas, identificação dos dispositivos da rede representando em real-time.

O gerente da rede deve ser capaz de, inicialmente, identificar os componentes da rede e definir a conectividade entre eles. Também deve ser capaz de modificar a configuração em resposta às avaliações de desempenho, recuperação de falhas, problemas de segurança, atualização da rede ou a fim de atender às necessidades dos usuários. Relatórios de configuração podem ser gerados periodicamente.

- Gerenciamento de Desempenho: Segundo Shammas (2004), o gerenciamento de desempenho é um conjunto de funções responsáveis pela manutenção e exame dos registros que contém o histórico dos estados do sistema. O objetivo do histórico é usar na análise das tendências do uso dos componentes, e para definir um planejamento do sistema através do dimensionamento dos recursos que devem ser alocados para o sistema, com o objetivo de atender aos requisitos dos usuários deste sistema para que não ocorram insuficiências de recursos quando sua utilização se aproximar da capacidade total do sistema.

O serviço de gerência de configuração contempla a realização de uma série de atividades dentro desta área funcional, desenvolvendo ações para materialização de resultados de curto prazo. Algumas atividades que podem auxiliar no gerenciamento:

• Gerência de Disponibilidade: Desenvolvimento de processos de verificação de disponibilidade do dispositivo ou sistema ao longo de um determinado período, com a finalidade de exibir relatórios de análises de tendências e índices de disponibilidade.

• Planejamento de Capacidade: Auxiliar na interpretação das bases de dados comportamentais sobre o estado em que as redes se encontram, desenvolvendo a análise de tendência de longo prazo.

• Análise de Tráfego: Desenvolver processos de coleta para interpretação e direcionamento de ações de tráfego e otimização de recursos, verificando a quantidade de tráfego, gargalos na rede, qual o tempo de resposta e também a vazão.

Para tratar das questões acima, o gerente deve focalizar um conjunto inicial de recursos a serem monitorados, a fim de estabelecer níveis de desempenho. Estatísticas de desempenho podem ajudar no planejamento, administração e manutenção de grandes redes. Ações de correção como trocar tabelas de roteamento para balancear ou redistribuir a carga de tráfego durante horários de pico, ou ainda, a longo prazo, indicar a necessidade de expansão de linhas para uma determinada área.

- Gerenciamento de Segurança: Segundo Shammas (2004), o gerenciamento de segurança fornece facilidades para proteger recursos da rede e informações dos usuários de possíveis intrusos. Estas facilidades devem estar disponíveis apenas para os administradores e operadores de redes. É necessário que a política de segurança seja robusta e efetiva, providenciando se necessário um alarme ao gerente da rede sempre que detectarem questões relacionadas a segurança do sistema.

O gerenciamento de segurança trata de questões como: geração, distribuição e armazenamento de chaves de criptografia; Manutenção e distribuição de senhas e informações de controle de acesso; Monitoração e controle de acesso à rede ou parte da rede e às informações obtidas dos nodos da rede; Coleta, armazenamento e exame de registros de auditoria e logs de segurança, bem como ativação e desativação destas atividades; Integridade dos dados; E confidencialidade dos dados.

2.6. SNMP

SNMP é o protocolo padrão das redes TCP/IP. Por ser de baixo nível fornece duas operações básicas, atribuir ou buscar o valor de uma variável.

SNMP versão 1 foi definido em maio de 1990, através da RFC 1157 e da RFC 1155, que trata das informações de gerenciamento. SNMP disponibilizava uma forma simples e sistemática de gerenciar uma rede.

Segundo Shammas (2004), SNMP define propriamente, o formato das mensagens que trafegam entre o computador do administrador e o agente a ser gerenciado. Segundo Tanenbaum (2003), o modelo SNMP de uma rede gerenciada consiste em quatro componentes, sendo eles, nós gerenciados, estações de gerenciamento, informações de gerenciamento e protocolo de gerenciamento.

3. Estudo de caso

Neste trabalho foram estudadas e avaliadas as ferramentas de gerenciamento CACTI, ZABBIX e NAGIOS. Abaixo segue uma descrição comparativa de cada uma das três ferramentas de monitoramento de ativos em uma rede.

3.1. CACTI

Segundo Black (2008), CACTI é uma ferramenta muito abrangente, uma vez que destaca graficamente diversas informações e possui boa usabilidade, não deixando de funcionar mesmo em condições adversas tais como ocorrem quando diversas máquinas da rede precisam ser desligadas ou religadas. Possibilita o controle de broadcasts e “pings da morte”, bem como a execução de testes de exaustão no servidor onde ele está instalado.

Muitas funcionalidades podem ser adicionais a CACTI através plugins de terceiros ou até mesmo pelo próprio administrador da rede, suprimindo algumas falhas encontradas na instalação padrão. Um ponto fraco observado em testes práticos com CACTI foi o armazenamento e a exibição dos dados e dos gráficos. Em redes de pequeno porte esse ponto não é tão preocupante, porém pode ser comprometedor em redes maiores.

3.2. NAGIOS

Segundo Black (2008), NAGIOS é um sistema abrangente com peculiaridades em relação à segurança, suportando diversas tecnologias existentes no mercado, como por exemplo, SSL e kerberos, e ainda diversas configurações para o seu código. Possui ênfase na capacidade de monitorar os dispositivos, com opções disponíveis para plugins desenvolvidos por terceiros.

Todos os recursos documentados de NAGIOS mostraram-se coerentes e funcionais em testes práticos. No entanto, a exibição dos gráficos não é tão esplêndida quanto aos demais softwares avaliados. Porém as informações mais relevantes são mantidas corretamente e sempre atualizadas pelo software. Trata com ênfase a linha de disponibilidade, tendo este produto diversas ferramentas para monitorar os mais variados serviços e plataformas diferentes.

Um ponto fraco observado na ferramenta é a lentidão para finalizar a varredura e reunir os dados, bem como um excessivo número de características que apenas estão disponíveis através de plugins externos, ou seja, de terceiros, aumentando a dificuldade de configuração para o administrador.

3.3. ZABBIX

Segundo Black (2008), ZABBIX é a ferramenta mais completa dentre as ferramentas disponibilizadas pela licença GPL, ou seja, de licença pública para programas da Free Software Fundation. A ferramenta reúne uma gama completa de opções em uma única plataforma robusta e bem amigável.

Em testes práticos, os gráficos e mapas das informações são facilmente gerados e acessados. Os agentes remotos proporcionam um levantamento detalhado do ambiente, porém não possuem uma boa qualidade visual. Isso é uma característica comum de todos os produtos da licença GPL.

ZABBIX possui uma documentação excelente. Isso facilita bastante a administração da rede. O software também é constantemente atualizado, com comunidade ativa e participante. Como ponto forte, a ferramenta tem por destaque a gama de bancos de dados compatíveis com o sistema, além de não apresentar um ponto fraco marcante.

4. Resultados

O Quadro 1 apresenta a avaliação das 3 ferramentas estudadas de acordo com 16 quesitos analisados. O primeiro campo SLA Reports é um documento formal para a contratação de um serviço de gerenciamento. O agente significa se o software possui ou não um agente para ser instalado nos dispositivos gerenciados. O terceiro campo mostra se o software possui suporte ao protocolo SNMP. O Syslog é um padrão para transmissão de logs.

Os demais campos da tabela são peculiaridades como linguagem desenvolvida, forma de armazenamento de arquivos, utilização de scripts externos para enriquecer ainda mais o gerenciamento.

Quadro 1. Comparação de Ferramentas de Gerenciamento de Redes

Quesito/Ferramenta	Cacti	Nagios	Zabbix
SLA Reports	Não	Através de Plugin	Sim
Auto Discovery	Através de Plugin	Através de Plugin	Sim
Agente	Não	Sim	Sim
SNMP	Sim	Através de Plugin	Sim
Syslog	Não	Através de Plugin	Sim
Permite Scripts Externos	Sim	Sim	Sim
Plugins	Sim	Sim	Sim
Linguagem Desenvolvida	PHP	Perl	C e PHP
Gatilhos/Alertas	Sim	Sim	Sim
Front-End Web	Controle Completo	Controle Parcial	Controle Completo
Monitoramento Distribuído	Sim	Sim	Sim
Inventário	Através de Plugin	Através de Plugin	Sim
Método de Armazenamento de Dados	RRDTool, MySQL, PostgreSQL em Desenvolvimento	MySQL e MSSQL	Oracle, MySQL, PostgreSQL e SQLite
Licenciamento	GPL	GPL	SIM
Geração Gráfico/Mapas	Através de Plugin	SIM	SIM
Eventos	Através de Plugin	SIM	SIM

Através deste quadro confirma-se que o software de gerenciamento mais completo é ZABBIX devido as características citadas anteriormente, e que proporciona ao gerente de rede melhores condições de manter a sua rede estável.

As ferramentas de gerenciamento foram testadas desde junho de 2009, quando foi instalado o Nagios para fazer o controle de um provedor de internet na cidade de Boa Vista do Buricá – RS, onde comprovou-se as imensas dificuldades em instalar e configurar a ferramenta bem como problemas com os plugins da mesma.

Em março de 2010 foi instalado o software Cacti para gerenciar a prefeitura municipal de Horizontina, sendo que como concluiu-se que o mesmo era muito fraco pois não possui gatilhos para que fossem tomadas medidas de correção as falhas que o software detectasse. Entretanto, a configuração e administração foi muito mais simples do que a do nagios.

A partir de julho de 2010, ate o presente momento, trabalha-se com o zabbix, que dentre os 3 programas estudados, mostrou ser o que possui a melhor relação custo/beneficio já que a dificuldade de instalação e administração compensa com os benefícios que o uso do software traz.

5. Conclusão

Este trabalho apresentou o resultado comparativo da análise de 3 ferramentas de gerenciamento de redes de computadores. Os resultados obtidos mostram que o ZABBIX é o software mais completo na comparação com os outros dois programas. Ele possui ainda uma interface mais amigável ao gerente da rede, instalação e administração mais fácil do que NAGIOS e CACTI.

O gerenciamento praticamente anula o risco de vulnerabilidades nas redes, e deveria ser implementado em redes de qualquer porte, pois tanto empresas grandes como pequenas necessitam da disponibilidade dos seus recursos. Como trabalhos futuros pretende-se avaliar o comportamento e a eficiência destas 3 ferramentas de gerenciamento de forma prática em uma rede de computadores de grande porte para comprovar o estudo do presente artigo.

Referências

BLACK, Thomas Lovis. **Comparação de ferramentas de gerenciamento de redes.** Disponível em: <http://www.lume.ufrgs.br/bitstream/handle/10183/15986/000695315.pdf?sequence=1>. Acesso em 21 de Abr. de 2010.

DIAS, Beethovem Zanella; JR. Nilton Alves. **Protocolo de Gerenciamento SNMP**. Disponível em: <http://www.rederio.br/downloads/pdf/nt00601.pdf>. Acesso em 7 Abr. 2010.

FINLAY, John. **Cacti**. Disponível em: <http://www.scribd.com/doc/7234195/Cacti>. Acesso em 21 de Abr. de 2010.

SHAMMAS, Gabriel. **Gerenciamento de redes.** Disponível em: <http://www.shammas.eng.br/acad/sitesalunos0106/012006gr/falhas.htm>. Acesso em 21 de Abr. de 2010.

SPECIALSKI, Elizabeth Sueli. **Gerencia de redes de computadores e de telecomunicações**. Disponível em: <http://www.malima.com.br/article_read.asp?id=279>. Acesso em 12 de Abr. de 2010.

TANENBAUM, Andrew S. **Redes de Computadores**. Rio de Janeiro: Elsevier Editora, 2003.