ANÁLISE DE FERRAMENTAS PARA MONITORAMENTO DE REDES: ASPECTOS DE SEGURANÇA E VISUALIZAÇÃO DA INFORMAÇÃO

Luiz Felipe de Camargo, Kelton Augusto Pontara da Costa e José Remo Ferreira Brega
Faculdade de Ciências - Universidade Estadual Paulista "Júlio de Mesquita Filho" - UNESP, Bauru, Brasil

RESUMO

Com o uso cada vez mais intenso das redes de computadores, a necessidade de monitoramento destas se faz cada vez mais presente, de modo a garantir a gerência e segurança das destas, principalmente no aspecto da disponibilidade. Este trabalho tem como objetivo analisar diversas ferramentas para monitoramento disponíveis no mercado, considerando os aspectos de segurança da informação e visualização de dados, selecionando entre elas a melhor opção, de acordo com as funcionalidades, custo benefício e flexibilidade presentes nos serviços oferecidos. Os dados utilizados para embasar a escolha foram coletados das documentações das aplicações e através de testes realizados em máquinas virtuais monitorando a estrutura real de uma unidade universitária. Para uma visão mais ampla dos dados coletados, estes foram dispostos em um quadro. Para concluir o trabalho elegeu-se através da ponderação de pontos positivos e negativos a melhor opção.

PALAVRAS-CHAVE

Monitoramento, Redes, Computadores, Segurança, Visualização

1. INTRODUÇÃO

As redes de computadores evoluíram de tal forma que nos dias atuais é quase impossível estar off-line, essa evolução foi exponencial e junto dela, houve também o aumento dos incidentes e problemas, da necessidade de gerência e segurança, principalmente do aspecto da disponibilidade. A necessidade de controlar, monitorar e coordenar os dispositivos de hardware e software se tornou evidente. (Kurose James F.; Ross, 2010). O administrador de redes deve garantir a segurança de sua rede e principalmente sua disponibilidade, através de dados, sejam eles em tempo real ou históricos, de todos os equipamentos e serviços que fazem parte dela. As opções de softwares para obtenção destes dados são inúmeras, sendo assim este trabalho busca estudar algumas delas, de modo a selecionar a melhor opção frente as necessidades apresentadas, considerando aspectos de segurança e da construção visual dos softwares.

Em 2012, Shiravi realizou um levantamento de todas as ferramentas desenvolvidas nos anos anteriores, para monitoramento de diversos aspectos de segurança de rede considerando a visualização da informação. (Shiravi, Shiravi and Ghorbani, 2012) No ano de 2013, Wu realizou um estudo monitorando tráfego de rede com o apoio de GPU em redes com grande tráfego. (Wu and Demar, 2013). Já em 2015, Aouini procedeu com um estudo sobre monitoramento de redes no âmbito residencial, avaliando as ferramentas existentes de código aberto no mercado da época. (Aouini, Kortebi and Ghamri-Doudane, 2015).

A seção 2 deste trabalho trata da fundamentação teórica, seguida da seção 3 que descreve a metodologia e o cenário utilizado, os resultados e discussões serão apresentados na seção 4 e por fim teremos a conclusão seguida das referências utilizadas.

2. FUNDAMENTAÇÃO TEÓRICA

A seguir serão apresentados conceitos básicos relacionados às temáticas utilizadas no decorrer deste trabalho:

Segurança da informação: definida como a proteção contra as diversas ameaças que tem como objetivo comprometer os negócios de uma organização através das informações, a segurança da informação garante a

continuidade destes negócios, garantindo e maximizando o retorno sobre os investimentos e as oportunidades de negócio e minimizando os riscos. (ABNT, 2005)

Disponibilidade, definida como a capacidade de algo estar acessível e utilizável sob demanda, ou seja, quando necessário e solicitado por usuário devidamente autorizado. (ISO/IEC, 2004)

Gerenciamento de redes: a definição de gerenciamento de redes é muito bem resumida por Saydam: "Gerenciamento de rede inclui o desenvolvimento, a integração e coordenação de todo o hardware, software e elementos humanos para monitorar, testar, consultar, configurar, analisar, avaliar, e controlar os recursos da rede e seus elementos para atender em tempo real os requisitos de desempenho operacional e de qualidade de serviço a um custo razoável." (Saydam and Magedanz, 1996)

Visualização da Informação: sistemas computacionais baseados em visualização representam conjuntos de dados como imagens, para auxiliar na compreensão, de forma a realizar as tarefas de interpretação de dados de maneira mais eficiente. Uma ferramenta de visualização pode ser criada respondendo três perguntas: por que a tarefa está sendo executada, quais dados são exibidos nas visualizações, e como a linguagem de expressão é construído como opções de design. (Munzner, 2014)

3. METODOLOGIA

Para realização deste trabalho foi realizada uma breve pesquisa bibliográfica de modo a definir os conceitos utilizados. Em seguida foi definido o cenário utilizado nos estudos de monitoramento, citando as demandas de monitoramento. Através de consultas a profissionais da área e informações disponíveis na internet, foram selecionadas 9 ferramentas de monitoramento, estas foram instalados em servidores virtualizados e utilizadas para o monitoramento real da estrutura principal de uma rede. Foram levantados os aspectos de construção dos softwares e funcionalidade através das instalações realizadas e da documentação disponível. Foi construído um quadro comparativo entre os softwares com as principais características de cada ferramenta, com os dados coletados, para melhor comparação.

Por fim, foram comparados os resultados, contabilizando pontos positivos e negativos, indicando dentro dos aspectos analisados a melhor opção a ser utilizada dentre as ferramentas avaliadas e seguida foram realizadas as considerações finais. Para realização dos testes práticos foi utilizada a infraestrutura de rede da Faculdade de Medicina de Botucatu (FMB), pertencente a Unesp. O monitoramento foi realizado em 23 equipamentos de comutação de dados (switches), sendo estes os que recebem as conexões de entrada de cada área que compõe a FMB e suas unidades.

4. ANÁLISE E DISCUSSÃO DOS RESULTADOS

4.1 Análise Visual

Cacti: permite criação de gráficos de séries temporais para qualquer dispositivo ou porta, possui modelos pré-configurados e permite customização. Mostra nos gráficos valores atuais, média e pico máximo.

Icinga: possui identificação visual do status da rede na tela inicial, através de cores. Tem toda sua construção baseada na cor verde indicando situação normal e na cor vermelha indicando problemas, pode mostrar gráficos de séries temporais para tendências, gráficos de barras com a "saúde" da rede e possui funcionalidade para criação automática de mapas da rede, itens todos herdados do Nagios, software no qual é baseado.

MRTG: possui o visual mais simples das ferramentas selecionadas, constituído por uma página com todos os gráficos de séries temporais dispostos sequencialmente. Através dos arquivos de configuração é possível fazer pequenas customizações nos gráficos.

Nagios: mostra na interface detalhes em verde e vermelho para identificação de situações normais e problemas respectivamente, pode mostrar gráficos de séries temporais para tendências e gráficos de barras com a "saúde" da rede. Possui funcionalidade para criação automática de mapas da rede.

NetXMS: não possui recursos visuais disponíveis por padrão na interface, possibilita a criação de mapas e painéis de controle (dashboards) customizados manualmente.

Observium: possui identificação de status por cores: verde, azul e vermelho, gráficos de barras para exibição de uso de recursos dos equipamentos, integração com mapas da plataforma CARTO, gráficos de séries temporais diversos, com prévias através de sparklines (pequenos gráficos integrados ao texto).

PRTG: gráficos de pizza para exibição de problemas, escala de cores para níveis de gravidade dos problemas em diversos itens, gráficos de séries temporais para dados históricos, possibilidade de criação de mapas de topologia integrados com visão de satélite, criação de painéis de controle (dashboards) customizados.

The Dude: indicação por cor para status dos equipamentos, verde para online, amarelo para parcialmente online e vermelho para off-line, possibilidade de construção manual de mapas de redes, ícones personalizáveis e gráficos de séries temporais para dados históricos.

Zabbix: Cores de itens variando de acordo com problemas e notificações, possibilidade de criação de mapas e gráficos de séries temporais.

4.2 Comparação

Aspectos	CACTI	ICINGA	MRTG	NAGIOS CORE	NETXMS	OBSERVIUM	PRTG	THE DUDE	ZABBIX
Requisitos de hardware	Não informados	Proc. de 1 Ghz 1 GB de mem. RAM 8 GB de HD (mesmos do Nagios)	Não informados	Proc. de 1 Ghz 1 GB de mem. RAM 8 GB de HD	Pentium III 500 MHz 256MB de mem. RAM 100MB de HD + espaço para BD	256MB de mem. RAM para uma pequena instalação	3GB de mem. RAM 250GB de HD	Não especificado, citado computador com especificações baixas.	128 MB de mem. RAM 256 MB de HD mais espaço para BD
Interface WEB	Sim	Sim	Sim, estática, exibindo os gráficos	Sim	Adaptada da aplicação desktop	Sim	Sim	Sim	Sim
Licenciamento e Custos	GPL, gratuito, possibilidade de doações	GPL, gratuito	GPL, gratuito	GPL, gratuito, versão comercial a partir de US$ 1.995,00	GPL, gratuito	Licença própria, gratuito, versão comercial por £200/ano	Licença própria, gratuito, versão comercial a partir de US$ 1.600,00	Licença própria, preço sob consulta	GPL, gratuito
Limitações da Versão Gratuita	-	-	-	Recursos exclusivos na versão comercial	-	Recursos exclusivos na versão comercial, atualizações limitadas	Limitação no número de equipamentos monitorados	Somente para testes	-
Suporte Comercial	Não	Não	Não	Somente na versão comercial	Pode ser contratado	Somente na versão comercial	Somente na versão comercial	Somente na versão comercial	Pode ser contratado
Compat. Ipv6	Sim	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim
Notificações	E-mail	E-mail e SMS	Não suporta	E-mail	E-mail e SMS	E-mail, SMS, XMPP e etc	E-mail, SMS, Push	E-mail	E-mail, SMS e XMPP
Versão Inst.	0.8.8	1.13.4	2.17.4	3.5.1	2.0.8	0.16.10.8128	17.2.31.2018	6.57.5	3.2.6
Fonte de inst.	Repositório S.O.	Repositório S.O.	Repositório S.O.	Repositório S.O.	TAR Fabricante	TAR Fabricante	EXE Fabricante	Fabricante	Appliance
Sist. Op.	Ubuntu 17.04 Srv	Ubuntu 17.04 Srv	Ubuntu 17.04 Srv	Ubuntu 17.04 Srv	Ubuntu 17.04 Srv	Ubuntu 17.04 Srv	Windows 7	RouterOS 6.37.5	Ubuntu 14.04.3
Configuração	Visual - Web	Arquivos	Comandos	Arquivos	Visual - Desktop	Visual - Web	Visual - Web	Visual - Desktop	Visual - Web
Mem. (Sem monitorar)	231 MB	109 MB	98 MB	123 MB	1.100 MB	300 MB	832 MB	48 MB	404 MB
Mem. (Monitorando)	287 MB	121 MB	104 MB	146 MB	1.100 MB	359 MB	1.040 MB	48 MB	1.192 MB

Figura 1. Principais características de cada software obtidas na avaliação

Os dados sintetizados na figura 1 foram retirados das documentações ou obtidos nas instalações realizadas.

Com os dados citados, pode-se avaliar o comportamento e consumo de hardware das ferramentas. Mesmo com o caráter estimativo destes dados, uma vez que diferentes cenários e demandas influenciam no comportamento do software, pode-se indicar os grandes consumidores de recursos (NetXMS, PRTG, Zabbix).

Com o crescimento exponencial das redes, o protocolo principal de comunicação, IPv4, deixou de atender todas as demandas e surgiu a necessidade de um substituto, o IPv6. Desta forma as ferramentas de monitoramento devem estar preparadas para esta gradual substituição, ferramentas que ainda não oferecem suporte ao novo protocolo se tornam cada vez mais irrelevantes com o passar do tempo (NetXMS, Dude).

Com o atual foco em programação para web, uma ferramenta que não possua monitoramento e gerência através da web possui desvantagens, pode-se citar como ponto negativo também a interface web adaptada precariamente da aplicação para área de trabalho (NetXMS) e interfaces não interativas (MRTG), em contraponto de opções que possuem até mesmo sua interface de configuração totalmente baseada em web (Cacti, Observium, PRTG, Zabbix). A disponibilidade de informação fica prejudicada pela falta de acesso através da web, em qualquer navegador, dificultando a gerência.

Com relação a custos, limitações, atualizações e suporte comercial, foram consideradas com pontos positivos as opções gratuitas (Cacti, Icinga, MRTG, NetXMS, Zabbix), com versões comerciais gratuitas sem grandes limitações (Nagios, Observium), ferramentas com possibilidade de aquisição posterior de versão comercial (Nagios, Observium, PRTG, Dude) ou com possibilidade de contratação de suporte comercial para versão gratuita (NetXMS, Zabbix). Foram consideradas com pontos negativos as ferramentas com versões gratuitas com grandes limitações e uso somente para testes (PRTG, Dude) e com suporte unicamente gratuito e

oferecido pela comunidade (Cacti, Icinga, MRTG), correndo o risco de ter seu desenvolvimento suspenso, colocando em risco o projeto de monitoramento.

Foram consideradas as formas de notificação oferecidas pelas ferramentas, com destaque para opções como SMS e mensageiros instantâneos (Icinga, NetXMS, Observium, PRTG, Zabbix), problemas podem ser encontrados na utilização de ferramentas que só oferecem notificações por e-mail (Cacti, Nagios Core, Dude) ou não oferecem opção de notificações (MRTG), o que foi considerado como negativo.

No que diz respeito aos aspectos visuais, diversas técnicas de visualização foram utilizadas, pode-se destacar positivamente a grande gama de recursos disponíveis em algumas ferramentas (Observium e PRTG) e negativamente ferramentas que só possuem o recurso visual de gráficos de séries temporais (Cacti e MRTG).

Foram tabulados os pontos indicados com positivos e negativos, sendo que na avaliação, um ponto considerado positivo anula um ponto considerado negativo, também sendo válido o inverso. Com 5 pontos destacados positivamente e nenhum ponto negativo averiguado, mediante as métricas anteriormente definidas, foi selecionado o software Observium como opção mais recomendada entre as ferramentas avaliadas, totalizando 5 pontos, como pode-se observar na tabela 1.

Tabela 1. Pontos de positivos e negativos reconhecidos em cada ferramenta e sua pontuação total

	CACTI	ICINGA	MRTG	NAGIOS	NETXMS	OBSERVIUM	PRTG	DUDE	ZABBIX
Positivos	2	2	1	2	3	5	3	1	4
Negativos	3	1	4	1	3	0	3	3	1
Total	-1	1	-3	1	0	5	1	-2	3

5. CONCLUSÃO

Conclui-se, de acordo com os aspectos avaliados, dentre as ferramentas selecionadas, que é possível recomendar como melhor opção o Observium, pois, possui comportamento regular com consumo moderado de recursos, interface web para acesso e configurações, suporte ao protocolo IPv6, versão comercial de acesso gratuito sem limitações prejudiciais ao uso, versão comercial com suporte mais robusto, maior flexibilidade nas opções de notificações e melhor exploração de recursos visuais, auxiliando o processo de gerenciamento.

O principal ponto positivo levantado com este trabalho é que existe uma variedade grande de ferramentas disponíveis para o monitoramento de redes, permitindo a escolha da que melhor atenda as necessidades, gerando assim proteção para as redes, melhorando a gerência delas, evitando prejuízos, utilizando os princípios da segurança de informação.

REFERÊNCIAS

ABNT (2005) *NBR ISO/IEC 27002:2005 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação*. Rio de Janeiro.

Aouini, Z., Kortebi, A. and Ghamri-Doudane, Y. (2015) 'Traffic monitoring in home networks: Enhancing diagnosis and performance tracking', *IWCMC 2015 - 11th International Wireless Communications and Mobile Computing Conference*, pp. 545–550. doi: 10.1109/IWCMC.2015.7289142.

ISO/IEC, J. 1/SCISO/IEC J. 1/SC 27 (2004) *ISO/IEC 13335-1:2004 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management*. Suiça.

Kurose James F.; Ross, K. W. (2010) *Computer networking : a top-down approach*. Edited by Addison-Wesley Reading. Addison-Wesley Reading.

Munzner, T. (2014) 'Chapter 01. What?s Vis, and Why Do It?', in *Visualization Analysis and Design*. A K Peters/CRC Press (AK Peters Visualization Series), pp. 1–19. doi: doi:10.1201/b17511-2.

Saydam, T. and Magedanz, T. (1996) 'From Networks and Network Management into Service and Service Management', *Journal of Networks and System Management*, 4(4), pp. 345–348.

Shiravi, H., Shiravi, A. and Ghorbani, A. A. (2012) 'A survey of visualization systems for network security', *IEEE Transactions on Visualization and Computer Graphics*, 18(8), pp. 1313–1329. doi: 10.1109/TVCG.2011.144.

Wu, W. and Demar, P. (2013) 'A GPU-accelerated network traffic monitoring and analysis system', *2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 77–78. doi: 10.1109/INFCOMW.2013.6970747.