FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE - FANESE

NÚCLEO DE PÓS-GRADUAÇÃO E EXTENSÃO – NPGE

CURSO DE PÓS-GRADUAÇÃO "LATO SENSU"

GESTÃO DE REDES E SEGURANÇA DA INFORMAÇÃO.

ISRAEL PACHECO SOUZA

Monitorando redes de computadores com NAGIOS.

ARACAJU – SE

2015.1

ISRAEL PACHECO SOUZA

Monitorando redes de computadores com NAGIOS.

Trabalho de Conclusão de Curso apresentado ao Núcleo de Pós-graduação e Extensão da Faculdade de Administração e Negócios de Sergipe como exigência para obtenção do título de Especialização Gestão de Redes de Segurança da Informação.

_____

Marcelo Vieira de Menezes

_____

Luciano Cerqueira Passos

_____

Israel Pacheco Souza

Aprovado (a) com média: _____

ARACAJU (SE), 26 de Maio de 2015.

RESUMO

Este artigo aborda a importância de monitorar uma rede de computadores, através da utilização da ferramenta de monitoramento Nagios. Importante ferramenta que apresenta características de monitoramento de serviços de rede SMTP, POP3, HTTP, NNTP, dentre outros, além do monitoramento de recursos de servidores como CPU, memória, disco e processos. Um ambiente de tecnologia da informação (TI) bem planejado traz melhorias aos processos das organizações, mesmo para as empresas em que o principal foco não seja TI, pois, com a globalização, as empresas dependem cada vez mais da utilização da Internet e dos serviços aos quais ela disponibiliza, como correio eletrônico, VoIP (Voz por IP - telefonia pela internet), www, acesso remoto, compartilhamento de arquivos, dentre outros. O objetivo principal deste artigo é comprovar a importância do monitoramento de redes através de serviços baseados em internet, contribuindo na pro-atividade da solução de eventuais problemas. Entretanto, é importante ressaltar que os equipamentos que serão utilizados no monitoramento, como servidores e ativos de redes, estejam em perfeito estado de uso para não comprometer o processo de monitoração. Uma rede bem monitorada permite que os administradores de TI, possam atuar de forma mais eficaz para manter os equipamentos sempre disponíveis e acessíveis pelas organizações.

Palavras-chave: Ferramenta de Monitoramento, Nagios, Tecnologia da Informação, Monitoramento, Servidores e Ativos de Rede.

SUMÁRIO

1 INTRODUÇÃO

Este artigo teve como motivação uma sequência de erros, de um sistema voltado para o desenvolvimento agropecuário, onde o mesmo necessitava ser monitorado constantemente, fazendo com que os analistas de suporte técnico trabalhassem reativamente na solução dos problemas, quando poderíamos ser pró-ativos, identificando os problemas logo que eles ocorressem ou até mesmo futuros, a fim de oferecer aos clientes uma solução de maior segurança com o monitoramento e mantendo disponibilidade da rede e da aplicação.

O gerenciamento de redes tem a função observar e analisar o estado e o comportamento dos dispositivos gerenciáveis. Ao utilizar um software de gerenciamento, é possível verifica o estado operacional de uma ou mais interfaces de rede, realizando assim uma monitoração.

> Gerenciar um sistema consiste em supervisionar e controlar seu funcionamento para que ele satisfaça aos requisitos tanto do seus usuários quanto do seus proprietários. [Sloman, 1994]

Para gerenciar uma rede e seus ativos, percebemos que era necessário adotar um conjunto de ferramentas de gerenciamento. Atualmente existe uma gama de ferramentas de monitoramento, que permite que seja implementado um sistema composto por diversos aplicativos como o Nagios, *software* que abordaremos neste artigo, que foi escolhido por se tratar de uma ferramenta muito bem aceita no mercado tecnológico, além de não custar ônus inicial a organização, fator fundamental para a implantação do projeto de monitoramento.

2 REDE DE COMPUTADORES

Atualmente muitos dispositivos se comunicam e compartilham recursos físicos e lógicos através das redes de computadores. São utilizadas no dia a dia em serviços bancários, no uso do cartão de crédito, em chamadas telefônicas, entre outros. A facilidade e comodidade que é adquirida utilizando os serviços de rede fazem com que haja a cada dia mais dependência dos mesmos. O compartilhamento de recursos e serviços de rede passaram a ser indispensáveis nas organizações. Uma rede permite que diversos equipamentos e recursos possam ser interligados e compartilhados, dando acesso a protocolos e requisitos de segurança de forma a permitir que o usuário possa se beneficiar com a utilização de serviços de rede, porém, caso estes estejam inativos todos os departamentos, diretamente ou indiretamente, podem ser afetados.

> "Uma rede de computadores pode oferecer um meio de comunicação altamente eficaz para funcionários que trabalham em locais muito distantes um do outro". [Andrew S. Tanenbaum]

As redes apresentam diversas definições, sendo que as mais conhecidas são:

- LANs (*Local Area Network*) - redes locais que compartilham recursos privados;
- MANs (*Metropolitan Area Network*) - redes maiores que abrangem a cidade;
- WANs (*Wide Area Network*) – redes que podem abranger um país ou continente, e tem como principal exemplo a Internet.
- Sem Fio (*wireless*) – esta rede vem se destacando e ganhando cada vez mais adeptos devido aos baixos custos de aparelhos eletrônicos, que fazem o uso deste recurso, e dos equipamentos de rede, que possibilitam aos profissionais de TI uma maior facilidade na implantação e expansão da rede, além de possibilitar maior flexibilidade dos usuários.

3 ATIVOS E SERVIÇOS DE REDE

Antigamente, uma rede de computadores tinha como principal objetivo compartilhar documentos e dispositivos da rede, como por exemplo, impressoras e discos. Porém com o passar do tempo e a queda nos preços dos equipamentos, cada vez mais as organizações e demais usuários caíram no gosto por adquirir novos equipamentos, motivando assim o crescimento dos ativos e serviços de rede.

Monitoramento engloba *hardware* e *software* dentro de um ambiente corporativo. Local com poucos ativos conectados pode ser monitorado tranquilamente por apenas uma pessoa. Em contra partida, ambientes maiores onde a rede está distribuída em vários locais, o monitoramento é mais complexo e indispensável, devido ao grande número de equipamentos.

O monitoramento dos ativos de redes é uma avaliação contínua, e tem como objetivo detectar possíveis falhas, garantindo assim a disponibilidade dos serviços e maior confiabilidade das redes de computadores monitoradas.

> Para interligar os computadores na rede é necessária a utilização de alguns dispositivos como o roteador e *switch*. Esse último responsável por criar um barramento de comunicação entre os diversos dispositivos de rede que podem estar presentes na estrutura. O roteador é um dispositivo que tem como característica selecionar a rota mais apropriada para transferir e receber protocolos na rede. É utilizado para fazer a comunicação entre diferentes redes de computadores provendo a comunicação entre computadores distantes entre si. Já o *switch* é um dispositivo utilizado em redes de computadores para reencaminhar quadros entre os diversos nós. Possuem diversas portas, assim como os *hubs*, e operam na camada acima dos *hubs*. A diferença é que ele segmenta a rede internamente, sendo que cada porta corresponde a um segmento diferente, o que significa que não haverá colisões entre os computadores de segmentos diferentes. (REVISTA INFRA MAGAZINE 1, 2011 , p. 5).

4 A IMPORTÂNCIA DE MONITORAMENTO DA REDE

O monitoramente auxilia diretamente os sistemas de gerenciamento de rede (*Network Management System* – NMS), onde profissionais de TI podem obter informações da rede e ativos de rede, diagnosticando e tratando possíveis problemas e encaminhando as soluções destes problemas.

Os profissionais de TI sabem que até mesmo os equipamentos de última geração e os *softwares* mais atualizados não garantem sistemas imunes a erros. Por isso, qualquer sistema crítico para um negócio deve ser monitorado constantemente para evitar interrupções.

Servidores são uma das ferramentas que exigem monitoramento constante para prevenir problemas e garantir a disponibilidade do serviço para as organizações. Com uma infraestrutura monitorada, um profissional de TI poderá solucionar o problema imediatamente, de forma remota, antes mesmo que os funcionários comecem a trabalhar no dia seguinte.

Monitorar uma rede é verificar o funcionamento de cada serviço e equipamento disponível. Para isso é necessário utilizar ferramentas que verificam o funcionamento adequado dos equipamentos e serviços, enviando relatórios e alertas aos administradores, prevenindo falhas, e até mesmo fazendo com que sejam corrigidas antes que sejam notadas pelos usuários.

Com uma rede bem monitorada é possível que os gestores de TI possam programar manutenções periódicas ou investimentos em novos equipamentos para prevenir problemas em *hubs*, *switchs*, roteadores, modems, ou outros pontos da infraestrutura. Isso evita que a rede opere no limite de sua capacidade por muito tempo, permitindo que a empresa planeje os investimentos com mais tranqüilidade e sem grandes impactos no orçamento.

5 FERRAMENTAS DE MONITORAÇÃO DE REDE

Uma melhor gerência de redes requer controle de todos os ativos nela disponíveis, incluindo dispositivos de redes e serviços providos por ela. Administrar tudo isso, demanda uso de boas ferramentas de trabalho. Para tais fins, existem as ferramentas de monitoramento, *softwares* que se encarregam em auxiliar a gerenciar alguns desses ativos.

Atualmente existem diversas ferramentas capazes de fazer estes monitoramentos, entretanto, para que seja feita sua implantação, é necessário realizar um levantamento das necessidades e verificar qual delas se adéqua melhor a estrutura de uma determinada rede dentro das organizações.

5.1. Que Ferramenta Utilizar

As ferramentas podem ser do tipo comercial ou livre, apesar de que podem requerer complementos pagos. Enxiste uma série de ferramentas de monitoramento como Zabbix, Argus, Collectd, Zenoss, ObserverNMS, dentre outros, e cada um com sua peculiaridade. Destacaremos a utilização do Nagios, que é capaz de monitorar serviços de rede, recursos de computadores e equipamentos de rede, além de possuir uma interface fácil de utilizar além de plugins que os possibilitam trabalhar em conjunto com outras ferramentas.

6 NAGIOS

O Nagios é, considerado por muitos, um poderoso programa de monitoramento de rede, e ativos de redes que verifica constantemente a disponibilidade dos serviços, seja local ou remoto, sendo capaz de avisar por meio de envio de email ou mensagens de celular sobre o problema ocorrido. Através dele é possível obter relatórios de disponibilidade e formar gráficos que possibilitem configurar ações corretivas para os problemas ocorridos na rede, proporcionando assim um acompanhamento em tempo real dos acontecimentos.

Em termos gerais sua função principal é realizar verificações configuráveis de hosts e serviços, locais ou remotos, e quando houver algo de errado nestes, permitir a notificação aos administradores de sistema.

Originalmente batizado de Netsaint, o Nagios a partir de agosto de 2009 passou a ser Nagios Core e sua versão atual estável é a 3.2.3, a razão para ele ganhar um nome mais longo deve-se á vinda da versão comercial Nagios XI. Escrito e atualmente mantido por Ethan Galstad, junto a uma equipe de desenvolvedores que mantém *plugins* oficiais e não-oficiais. Nagios primeiramente foi escrito para o sistema operacional Linux, mas pode rodar em outros Unix-like.

6.1. Visão Geral

- Monitora serviços de rede (SMTP, POP3, HTTP, NNTP, ICMP, SNMP);
- Monitora recursos de computadores ou equipamentos de rede (carga do processador, uso de disco, logs do sistema);
- Monitoração remota suportada através de túneis criptografados SSH ou SSL;

- Desenvolvimento simples de *plugins* que permite aos usuários facilmente criar seus próprios modos de monitoração, usando a ferramenta de desenvolvimento da sua escolha (Bash, C, Perl, Python, PHP, C#, etc.)
- Capacidade de definir a rede hierarquicamente definindo equipamentos "pai", permitindo distinção dos equipamentos que estão indisponíveis daqueles que estão inalcançáveis.
- Capacidade de notificar quando um serviço ou equipamento apresenta problemas e quando o problema é resolvido (via email, pager, SMS, ou qualquer outro meio definido pelo usuário por plugin).
- Capacidade de definir tratadores de eventos que executam tarefas em situações pré-determinadas ou para a resolução pró-ativas de problemas.
- Rotação automática de log.
- Suporte para implementação de monitoração redundante.
- Excelente interface web para visualização do atual status da rede, notificações, histórico de problemas, arquivos de log, etc.
- Sua versão estável é a 3.2.3, além do atual Nagios Core, que assim foi batizado, devido á vinda da versão comercial Nagios XI.

6.2. Estrutura

O Nagios foi construído em uma arquitetura servidor/agentes e, usualmente em uma rede, executa em um servidor específico com seus *plugins* distribuídos nos servidores remotos que precisam ser monitorados. Estes *plugins* enviam informações para o servidor onde se encontra o Nagios que por sua vez exibe tudo na interface gráfica do usuário - GUI (*Graphical User Interface*). Sua composição consiste de 3 partes:

- O S*chedule* ou agendamento de tarefa, é um agente que ele verifica, em intervalos regulares, os *plugins* e de acordo com seus resultados executa ações;
- O GUI que é exibido em páginas web geradas pelo CGI (*Common Gateway Interface*) que podem ser vistos por botões de estado (verde para normal, amarelo para situação de alerta e vermelho para erro), sons, gráficos MRTG, etc;
- E *Plugins* que devidamente configurados são capazes de conferir um serviço e retornar um resultado para o Nagios.

Quando um *plugin* retorna um alerta ou um erro é alcançado o estado de *soft*. Neste momento na interface gráfica, um botão verde torna-se vermelho e um som é emitido. Quando este estado é alcançado muitas vezes, o alerta torna-se *hard*, e o servidor Nagios envia as notificações pertinentes.

6.2.1. Plugins

Um *plugin* nada mais é do que um pequeno software criado com o objetivo de realizar uma tarefa muito específica, normalmente apenas um *shell script* (*Bash, Perl*, etc), que através de um *ping* são capazes de fornecer uma das quatro possíveis condições: ok, *warning, critical, unknown*. Da mesma forma que um *plugin* pode monitorar equipamentos por *pings* é possível utilizar *plugins* para monitorar serviços de rede como HTTP, POP3, SMTP, SNMP, SSH e assim por diante. Não existem limites, considerando que se possa encontrar um meio de prover dados ou eventos como informação para ser avaliada por computador.

Os *plugins* do Nagios podem ser escritos em qualquer linguagem de programação e qualquer pessoa pode escrever um *plugin* simples em questão de minutos, a imaginação é o limite para a criação de *plugins* de notificações.

6.2.2. Agentes

Agentes são *softwares* instalados nos dispositivos para medir dados de desempenho que estão sendo monitorados como, por exemplo, utilização de CPU, uso de memória, ocupação de disco, dentre outros, que irão atender as requisições de *plugins* específicos.

Uma vez que o dispositivo que estiver sendo monitorado possua um agente de monitoração instalado, será possível coletar qualquer informação deste equipamento.

6.2.3. Banco de dados

O local onde serão armazenadas as informações pode ser um banco de dados ou arquivos de textos em formato de *logs*.

Por padrão o local de armazenamento de dados de um sistema Nagios são arquivos de *log*. Esse é o método convencional por ser o mais simples, entretanto utilizar o Nagios com o armazenamento de dados em arquivos texto causa desvantagens como, lentidão no acesso aos dados para geração de relatórios e dificuldade de extração de dados personalizados.

É óbvio que para coletar uma série de informações em um banco de dados relacional é muito mais rápido e simples do que utilizar ferramentas de pesquisas em arquivos texto, afinal toda estrutura proporcionada por um Sistema de Gerenciamento de Banco de Dados - SGBD, tem como proposta principal entregar informações de forma rápida.

6.2.4. Nagwin

Nagwin é um pacote de sistema de monitoração que possui a versão do Nagios para o sistema operacional Windows.

6.3. Objetivo

O principal objetivo do Nagios é informar aos administradores, no menor tempo possível, sobre condições questionáveis (*warning*) ou críticas (*critical*). Estas questões são definidas pelos administradores na configuração. Diferente das ferramentas de rede que mostram o tempo decorrido graficamente ou que registrem e meçam tráfego, o Nagios se utiliza de cores, como em um semáforo.

6.4. Peculiaridade

O Nagios executa verificações diferentes entre servidores e serviços. No servidor testa se um computador está alcançável, utilizando apenas um *ping*, quando necessário. Seletivamente testa serviços de rede individuais tais como HTTP, SMTP, DNS, etc; Já os processos executando, carga de CPU ou arquivos de *log*. O teste mais simples para serviços de rede consiste em ver se a porta de destino está escutando, e se o serviço está ativo.

Um aspecto especialmente interessante do Nagios é o fato de poder considerar dependências na topologia de rede. Se o sistema de destino só pode ser alcançado por um roteador específico que acabou de cair, então o Nagios reporta que o sistema está inatingível, e não irá mais enviar novas verificações.

6.5. Vantagens e Desvantagens

Uma vantagem do Nagios é possuir uma estrutura modular, possibilitando que ele utilize programas externos, conhecidos como *plugins*, para verificações de serviços e servidores. O pacote básico já contém uma quantidade padrão de *plugins* para as aplicações mais conhecidas. O uso de programas externos serve para notificações livremente configuráveis, para que se possa integrar qualquer sistema que se deseje: e-mail, SMS, servidor de recados que o administrador chama pelo telefone e recebe uma mensagem de voz referente ao erro. O contrário também é possível onde, através de uma interface separada, programas independentes podem enviar informação de estado e comandos para o Nagios.

A desvantagem em Nagios é a complexidade na instalação e uso, já que para trabalhar com esse sistema de monitoração o administrador precisa de um elevado conhecimento.

7 CONCLUSÃO

O presente estudo destaca a importância de monitorar uma rede de computadores fazendo o uso do *software* Nagios, escolhido por ser uma ferramenta de código aberto e que possui uma boa credibilidade tecnológica, que auxilia os administradores de TI quanto a problemas que estão ocorrendo na rede, bem como alertas a eventuais problemas, de modo que profissionais não se dêem ao luxo de realizar verificações manualmente.

Redes estão se tornando mais complexas e demandam mais cuidados, pois a cada novo *host* na rede, provavelmente um novo problema irá surgir. Saber como está a "saúde" de *hosts* e serviços da rede faz bem para a saúde do administrador de TI e é algo fundamental também para a saúde da empresa como um todo.

O Nagios amplia a capacidade de monitoramento, através de *plugins* com objetivos específicos, de algum equipamento em particular, como controladores de temperatura, umidade, memória, etc., e alertando aos administradores sobre problemas futuros ou que estão ocorrendo.

Por fim, gostaria de frisar a satisfação profissional por obter um grande sucesso na implantação do ambiente de monitoração fazendo o uso do Nagios, que a princípio foi apenas para a aplicação de desenvolvimento agropecuário, e que infelizmente por questões de contrato de suporte não fui autorizado a citar o nome. Com o passar do tempo passamos a monitorar outras aplicações e ativos de rede e servidores em diversos estados, chegando ao ponto de ultrapassar a utilização dos recursos livres que o Nagios dispõe, adquirindo *plugins* que nos permitiu trabalhar em conjunto com outras ferramentas de monitoração de modo que podemos assegurar e dar mais garantias de disponibilidade das aplicações junto aos clientes.

REFERÊNCIAS:

APARECIDA, Renata e SANTOS, Marcelo. Devmidia - **Monitoramento de Redes de Computadores** - Artigo Revista Infra Magazine 1, em < http://www.devmedia.com.br/monitoramento-de-redes-de-computadores-artigo-revista-infra-magazine-1/20815>. Acessado em 27 out. 2014.

OLIVEIRA, Ricardo. Artigo: Gerenciamento em Redes Utilizando a Ferramenta Nagios, em <https://pt.scribd.com/doc/181892143/GERENCIAMENTO-EM-REDES-UTILIZANDO-FERRAMENTA-NAGIOS-pdf>. Acessado em 27 out. 2014.

WIKIPEDIA. **Nagios**, em <http://pt.wikipedia.org/wiki/Nagios>. >. Acessado em 27 out. 2014.

NAGIOS. **Nagios Official Website**, em <http://www.nagios.org>. Acessado diversas vezes durante a pesquisa.

NETSAINT. **Netsaint Official Website**, em <http://www.netsaint.org>. Acessado em 30 out. 2014.

NAGIOS PLUGINS. **Plugins**, em <http://www.nagiosplug.sourgeforge.net>. Acessado em 30 out. 2014.

CENTRO UNIVERSITARIO DO NORTE – UNINORTE. Artigo: **Ferramenta de Gerenciamento de Redes – NAGIOS**, em <https://pt.scribd.com/doc/54401069/Nagios-TRABALHO>. Acessado para download em 31 out. 2014.

LUIZ, Sérgio.Artigo: **Nagios - O seu gerenciador de redes**, em <http://www.vivaolinux.com.br/artigo/Nagios-O-seu-gerenciador-de-redes>. Acessado em 31 out. 2014.

ABSTRACT

This article discusses the importance of monitoring a computer network, by using the Nagios monitoring tool. Important tool that provides monitoring characteristics of network services SMTP, POP3, HTTP, NNTP, among others, as well as monitoring of server resources such as CPU, memory, disk and processes. An information technology (IT) environment brings well-planned improvements to the processes of organizations, even for companies in which the primary focus is not IT, as with globalization, companies increasingly rely on the use of the Internet and services to which it offers, such as email, internet telephony, www, remote access, file sharing, among others. The main purpose of this article is to prove through the results, the importance of monitoring the network, and was based on learnings acquired on research done on the internet, through websites and articles dealing with the subject, and shows that you can monitor the network making use of internet-based services, and how they can contribute to the identification of possible problems more efficiently when they are properly configured. It is also important to note that servers which are centralized computing systems, and active networks such as hubs, switches and routers, among others, are working properly. A well-monitored network allows IT administrators can act more effectively to keep the equipment always available and accessible by organizations.

Keywords: Monitoring Tool, Nagios, Information Technology, Monitoring, Server and Network Assets.