# Monitoramento SNMP com Nagios

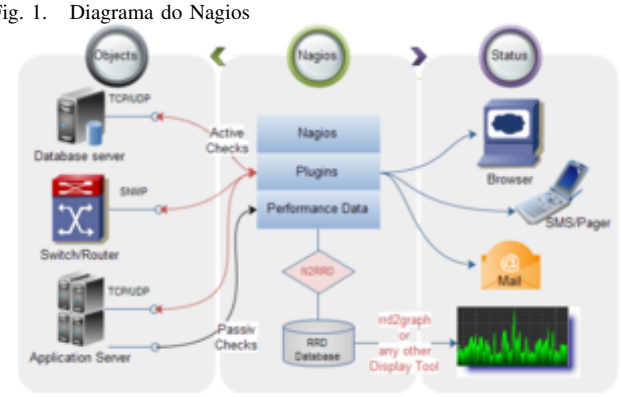
Guilherme Utech, Matheus Rambo da Roza, *Udesc*

## I. Introdução

Neste trabalho iremos a instalação, configuração e utilização de uma plataforma de gerenciamento de redes de computadores que utilize o protocolo SNMP em seu funcionamento. A plataforma a ser utilizada será o Nagios.

O Nagios é um software open-source que realiza monitoramento de redes e dá suporte ao monitoramento tanto de hosts quanto de serviços, alertando quando problemas ocorrem ou quando os problemas são solucionados. O Nagios foi criado e até hoje é mantido por Ethan Galstad, um norte-americado formado em Ciência da Computação pela Universidade Minnesota. No início o Nagios era chamado de NetSaint que é uma referência a cidade natal do autor, Saint Paul porém a partir de Outubro de 2007 passou a ser chamado de Nagios.

Fig. 1. Diagrama do Nagios




### A. *Funcionalidades do Nagios*

Diversos protocolos são suportados pelo Nagios, são eles:

- STMP
- POP3
- HTTP
- NNTP
- ICMP
- SNMP
- Entre outros

O Nagios monitora diversos equipamentos da rede, o estado da rede e seus recursos. O Nagios pode através de seus plugins realizar este monitoramento. Alguns recursos que podem são monitorados são:

- Carga de processador
- Uso de memória
- Serviços carregados
- Uso de disco

**Monitoramento local**

Um outro recursos do Nagios é realizar o monitoramento local. Realiza essa tarefa através da definição de Hosts locais como servidores que estão localizados na mesma rede da máquina Nagios (Caso não exista nenhum firewall ou roteador entre eles). Estes equipamentos podem ser monitorados através do algoritimo de verificação simples. Para tanto, é usado o comando ping para a verificação.

**Monitoramento remoto**

Outro recurso do Nagios é a realização de monitoramentos remotos. Este são os servidores que não estão no mesmo segmento de rede da máquina com o Nagios. É necessário, para o Nagios monitorar o servidor, descrever quais são os hosts que estão no caminho.

O monitoramento de servidores remotos é uma tarefa muito mais complexa que o monitoramento local pois à construção de todo um trajeto de rede para os hosts situados em outros segmentos. Existe uma forte necessidade de se diferir hosts que estão acessíveis ou não. De tal forma, sempre que é recebido como resposta de um comando de verificação, uma mensagem que dá ao host como inoperante, o Nagios percorre toda a hierarquia no sentido ascendente até encontrar um host ativo. Caso isso se verifique no nível imediatamente acima do host monitorado então conclui-se que o referido host esteja abaixo. Caso contrário, deduz-se que sejam os acessos ao host que estejam em baixo e que estão tornando o host inacessível. [VITOLO, 2002].

**Criação de plugins**

Um outro recurso muito interessante que o Nagios possibilita é a criação de plugins próprios para realizar o monitoramento de objetos que o Nagios não oferece suporte por padrão. Pode-se utilizar uma infinidade de linguagens para desenvolver tais plugins, como por exemplo:

- Bash
- PHP
- C
- C++
- C#

Entre outras linguagens.

**Checagem paralela**

Outro recurso que o Nagios permite é a realização de checagem de serviços de forma paralela e com isso, evita que serviços não sejam checados por falta de recursos.

**Hierarquia de rede**

Através do Nagios é possível definir uma hierarquia nos monitoramentos da rede, por exemplo: os computadores virtuais dependem dos equipamentos físicos para o

funcionamento. O computador físico é hierarquicamente superior ao equipamento virtualizado. Se o equipamento físico apresenta problemas, automaticamente o equipamento virtual apresentará também.

**Notificações de problemas** O Nagios realiza a notificação em tempo real através de alertas enviados ao gerenciador de rede caso ocorra alguma problema na rede, problemas estes podem ser por exemplo:

- Mudança do estado de soft para hard.
- Caso um serviços esteja com estado hard por mais tempo do que foi programado.

Existem diversos outros casos que podem ser checados na documentação.

**Tratamento de eventos e rotação automática dos logs**
O Nagios permite deixar um sistema que realiza rotinas pré-definidas em certos casos. Como por exemplo realizar uma rotina que faz o restart do sistema. Quanto a rotação automática dos logs, tais logs são rotacionados automaticamente e assim diminui o espaço em disco gasto com logs.

**Interface WEB**
O Nagios oferece uma interface WEB para facilitar o gerenciamento das redes.

**Detecção e tratamento de flapping**
O Nagios possui uma funcionalidade que podem detectar serviços que que efetuem trocas constantes. Tais trocas podem ser ocasionadas por lentidões, ou configurações mal realizadas.

**Falhas de redes**
O Nagios permite que se definam através das hierarquias já apresentadas nesta seção, definir redes que são independentes nesta estrutura. Como por exemplo: Segmentos de redes separados por switchs monitorados. Em caso de queda neste equipamento, todo o restante da rede abaixo dele estarão inacessíveis.

## II. Instalação do Nagios

A instalação do Nagios foi dividida em alguns passos diferentes que serão abordados no segmento desta seção.

### *A. Primeiro passo: Criação das Máquinas Virtuais*

Aqui criaremos duas máquinas virtuais que serão utilizadas para a instalação do Nagios, as máquinas virtuais utilizaram o sistema operacional Ubuntu na versão 18.04 que é indicado caso queira instalar o Nagios. A primeira máquina virtual vai conter a instalação do Nagios e esta será responsável por fazer o monitoramento da segunda máquina virtual chamada **VM_TESTE**, esta será a máquina que realizaremos o monitoramento através da utilização do protocolo SNMP.
A primeira máquina virtual que irá conter o Nagios, seguimos o seguinte passo a passo para sua instalação:

**Instalar Security-Enhance:**
$ sudo dpkg -l selinux*

**Instalar os pré-requisitos:**
$ sudo apt-get install -y autoconf gcc libc6 make wget unzip apache2 php libapache2-mod-php7.2 libgd-dev

**Download do código fonte:**
$ wget -O nagioscore.tar.gz https://github.com/NagiosEnterprises/nagioscore/archive/nagios-4 tar xzf nagioscore.tar.gz

**Compilar:**
$ cd /tmp/nagioscore-nagios-4.4.5/ e após isso, $ sudo ./configure –with-httpd-conf=/etc/apache2/sites-enabled seguido por $ sudo make all

**Criar usuário e grupo:**
$ sudo make install-groups-users $ sudo usermod -a -G nagios www-data

**Instalar os binários:**
$ sudo make install

**Instalar o serviço:**
$ sudo make install-daemoninit

**Instalar modo de comando:**
$ sudo make install-commandmode

**Instalar arquivos de configuração:**
$ sudo make install-config

**Instalar os arquivos de configuração do Apache:**
$ sudo make install-webconf $ sudo a2enmod rewrite $ sudo a2enmod cgi

**Configurando o Firewall:**
$ sudo ufw allow Apache $ sudo ufw reload

**Criação do conta de administrador nagiosadmin:**
$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

**Iniciando o Apache:**
$ sudo systemctl start nagios.service

Agora vamos as instalações do plugin.

**Instalar os Pré-requisitos:**
$ sudo apt-get install -y autoconf gcc libc6 libmcrypt-dev make libssl-dev wget bc gawk dc build-essential snmp libnet-snmp-perl gettext

**Download dos plugins:**
$ wget –no-check-certificate -O nagios-

plugins.tar.gz https://github.com/nagios-plugins/nagios-plugins/archive/release-2.2.1.tar.gz tar zxf nagios-plugins.tar.gz

**Compilar e instalar:**
$ cd /tmp/nagios-plugins-release-2.2.1/ $ sudo ./tools/setup $ sudo ./configure $ sudo make $ sudo make install

### *B. Segundo passo: Testar as instalações*

Para testar se a instalação ocorreu da forma correta, basta acessar o link http://localhost/nagios, nesta página no canto esquerdo terá um link chamado **HOSTs**, neste link haverá apenas um host que é a máquina Nagios. Para seguir com os testes, é necessário acessar a máquina virtual VM_TESTE e execute os seguintes comandos:

Fig. 2. Nagios - hosts


$ apt update
$ apt install snmp
Acesse o arquivo /etc/snmp/snmpd.conf e realize as seguintes alterações:

**Alterar a string da comunidade SNMP v1 somente leitura como 'pública':**
$ rocommunity public

**Comente as seguintes linhas:**
#agentAddress udp:127.0.0.1:161

**Retire o comentário da linha:**
agentAddress udp:161,udp6:[::1]:161

**Reinicie o serviço SNMP com o seguinte comando:**
$ service snmpd restart

**Realize os seguintes comandos para permitir a utilização das portas necessárias:**
$ ufw allow 161/udp
$ ufw allow 162/udp

**Depois de instalado o SNMP em ambas VMs, realize um teste na VM com nagios com o comando:**
$ snmpwalk -v1 -c public IP_DA_VM_TESTE

Caso apareça algum resultado que se caracteriza com um grande número de linhas de resultado, significa que o SNMP está funcionando corretamente e após isso, basta configurar o Nagios para realizar o monitoramento.

### *C. Terceiro passo: Configuração de hosts e serviços*

Agora acesse "/usr/local/nagios/etc/objects",nessa pasta contém diversos arquivos de configurações. Iremos alterar 2 arquivos.

**No arquivo localhost.cfg, adicione o seguinte trecho de código:**

*define host{*
*use linux-server*
*host_name VM_TESTE*
*alias VM_TESTE*
*address IP_DA_VM_TESTE }*

No final deste mesmo arquivo, adicione o seguinte trecho de código:

*define service{*
*use localservice*
*host_name VM_TESTE*
*service_description snmp_cpu1*
*check_command*
*check_snmp2!1.3.6.1.4.1.2021.10.1.3.1!5.0!10.0*
*}*

Agora no arquivo commands.cfg, adicione o seguinte trecho de código no final do arquivo:

*define command {*
*command_name check_snmp*
*command_line $USER1$/check_snmp2 -H*
*$HOSTADDRESS$ -C public -o $ARG1$*
*-w $ARG2$ -c $ARG3$ -v }*

Após isso, reinicie o Nagios

**Reiniciando o Nagios**
$ sudo systemctl restart nagios.service

**Conferindo se o serviço está ativo:**
$ sudo systemctl status nagios.service

**Em caso de erro dos passos anteriores:**
$ sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

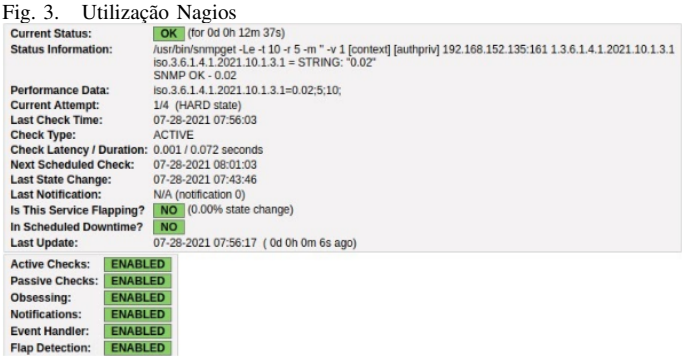
Esse comando irá mostrar de modo específico o erro que ocorreu, caso não tenha ocorrido nenhum erro, não é necessário executar esse comando.

### *D. Quarto passo: Conferindo integração do Nagios com o SNMP*

**Conferindo se o serviço está ativo:**

Para conferir se a integração entre o Nagios e o SNMP está funcionando corretamente basta acessar o https://localhost/nagios, note que agora no link de HOSTs terá um novo host adicionado, que é a VM_TESTE, se ao clicar em SERVICES e depois em snmp_cpu1 a CPU estiver com algum consumo vai aparecer um warning com código 5 e um alerta crítico com código 10, conforme a imagem 3.

Fig. 3. Utilização Nagios

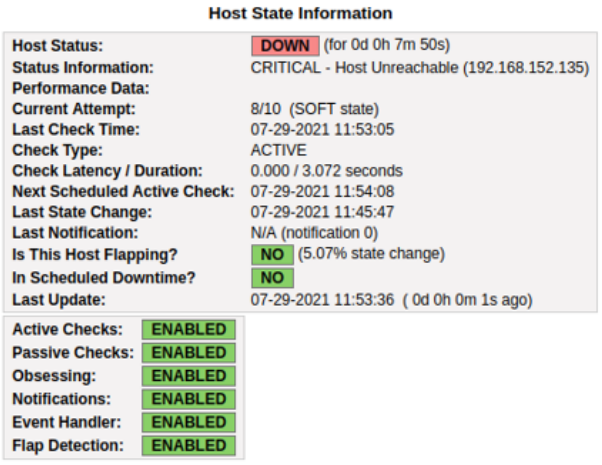



## III. Fase de utilização

Nesta seção serão apresentados alguns prints das tela de utilização do Nagios.

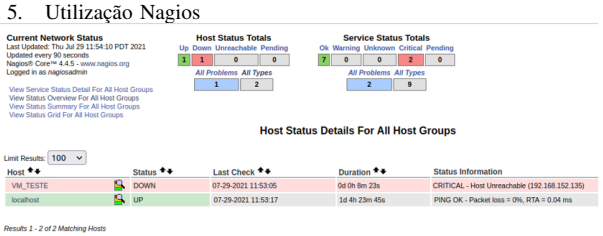
A figura abaixo mostra ao gerenciador da rede entre outras informações, o estado do host, quando ocorreu a última checagem de tempo, a latência e para quando está agendada a próxima checagem. Além disso mostra se o host está com Flapping e demais status como mostrado na figura.

Fig. 4. Utilização Nagios



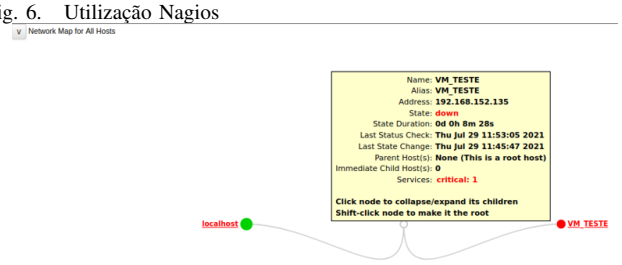

Este próximo print apresenta ao gerenciador todos os hosts, o localhost está up e a VM_TESTE está down.

Fig. 5. Utilização Nagios



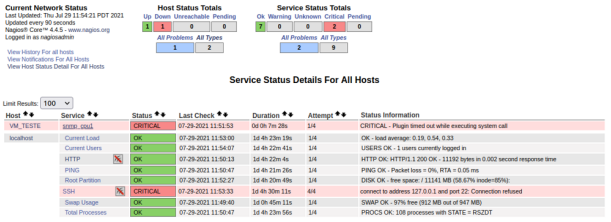

Esta próxima imagem traz o mapa dos Hosts para melhor monitoramento e com a VM_TESTE desligada, mostrando o tempo de duração em que ela esta desligada, os últimos estados checados.

Fig. 6. Utilização Nagios



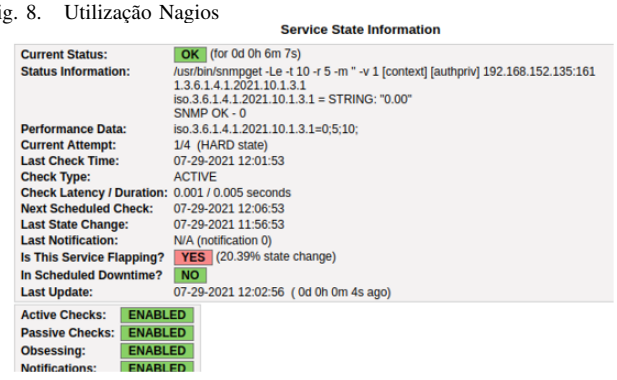

A imagem abaixo mostra a Aba de Services onde possui a VM_TESTE que esta com estado CRITICAL pois esta desligada.

Fig. 7. Utilização Nagios




A próxima imagem traz na Aba de Service/snmp_cpu1 mostrando as informções da VM_TETSTE mas dessa vez com a VM_TESTE ligada. Observamos que antes de 'SNMP OK = 0' temos STRING: '0.00', o que significa que o uso da VM esta em 0.00, conforme for sendo utilizada vai aumentando esse uso.

Fig. 8. Utilização Nagios



## REFERENCES

[1] Wolfgang Barth, 2008. Nagios, 2nd Edition: System and Network Monitoring Wirel. Netw.