Lab 04 - Sistemas de monitorização

Tópicos

1. Noção de sistema de monitorização.
2. Soluções existentes para monitorização de redes informáticas.
3. Instalar um sistema Nagios Core para monitorização.
4. Componentes existentes no Nagios Core.
5. Implementação de um cenário de testes em GNS3 para monitorizar com o Nagios.
6. Implementação de um cenário de testes com equipamentos físicos e virtuais.

1. Enquadramento

As redes informáticas estão sempre a evoluir e são cada vez mais essenciais, não só no nosso trabalho, mas também na nossa vida privada. Há uma necessidade dos sistemas informáticos e de rede estarem sempre a funcionar, o que leva a que seja obrigatório garantir que estes não falham, ou que falhem durante muito pouco tempo. Uma forma de garantir isso é utilizar um sistema de monitorização que esteja constantemente a verificar se está tudo a funcionar como deveria, tanto a nível de equipamentos de rede, como de servidores e respetivos serviços. A virtualização, a Cloud e principalmente a Internet das Coisas (IoT) vieram tornar ainda mais complexas as infraestruturas de rede, tendo passado a existir centenas ou milhares de equipamentos e serviços numa rede empresarial.

Devido à necessidade de nada falhar, é necessário implementar sistemas de monitorização em tempo real que verifiquem o estado da rede e reportem em caso de falhas. Estas ferramentas são atualmente indispensáveis em qualquer rede informática que se preze e permitem aos técnicos responder a situações anormais em tempo real. Os administradores de rede conseguem ter noção de tudo o que se passa na rede e de que forma se estão a comportar os equipamentos e os serviços.

Figura 1 - Equipamentos IoT interligados

2.Soluções de monitorização

Existem vários sistemas de monitorização de rede, uma pagas outras gratuitas, e consoante a finalidade/fiabilidade/robustez desejada há sempre uma escolha a ser feita pelos administradores de rede no que toca a qual ferramenta utilizar. Uma das soluções mais utilizadas é o Nagios, na sua vertente Open Source (gratuita), o Nagios Core, que contém as ferramentas essenciais para fazer a monitorização de uma rede e dos seus serviços.

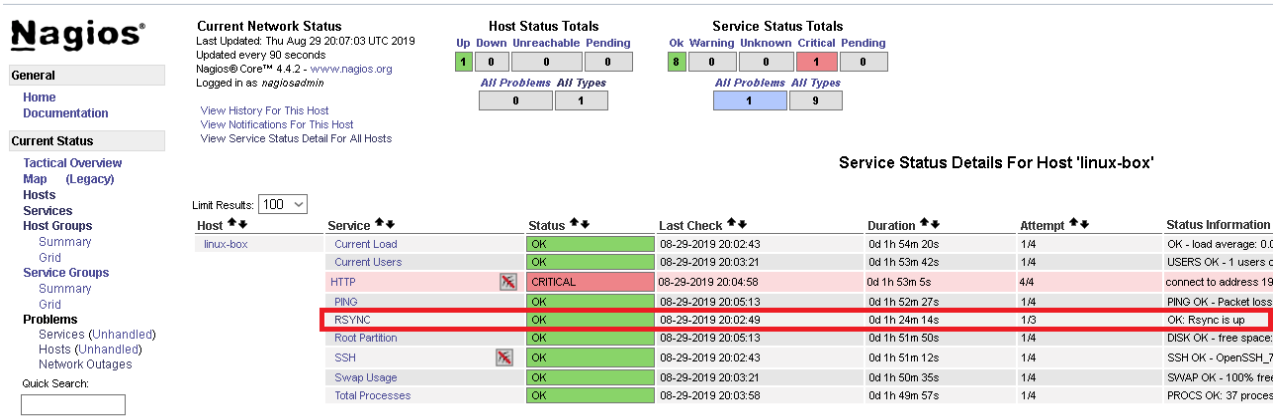

Figura 2 - Nagios Core

Outras soluções que existem a nível de monitorização são as seguintes:

- Zabbix: Uma solução também ela Open Source que utiliza templates out-of-the-box de fácil utilização;
- Icinga: Outra solução Open Source, feita pela mesma equipa de programadores que criou o Nagios;
- Solarwinds NPM: Uma solução comercial (paga) com capacidades avançadas de monitorização incorporadas e que consegue obter informações dos equipamentos de várias marcas nativamente.
- PRTG Network Monitor: Outra solução comercial com uma configuração simples e que tem um dashboard muito completa e de fácil utilização.

As duas soluções mais utilizadas são o Nagios e o Zabbix, tendo este último ganho muita popularidade devido à sua interface web mais apelativa e configuração mais simplificada.

Key Features	Zabbix	Nagios Core
Configuration	Web-based interface configuration.	By changing configuration text files.
User Interface	Full-blown and modern web-interface which also allows configuration changes.	Web-based interface available but only for basic monitoring and reporting.
Alerting	Email and/or SMS	Email and/or SMS
Main Protocol Monitoring (SSH, HTTP, FTP, POP3, SMTP, SNMP, MySQL etc)	YES	YES
Graphs	YES (out of the box)	YES (with the NagVis plugin)
Log Monitoring	YES	Only with Nagios log server
Plugins	NO	YES
Auto-discovery	YES	YES (with custom scripts)

Figura 3 - Comparação entre o Zabbix e o Nagos

3.Instalação do Nagios Core

Nesta ficha laboratorial iremos implementar um servidor de monitorização utilizando o Nagios Core (a vertente gratuita). O Nagios monitoriza a existência de equipamentos IP na rede utilizando o PING e serviços utilizando os mais diversos protocolos (SMTP, SNMP, POP3, HTTP, etc…).

Para se instalar o Nagios iremos usar uma máquina com Linux Ubuntu Server 14.04 LTS x64 e utilizaremos o Nagios Core na sua versão 3 (a versão presente nativamente nos repositórios). O primeiro passo atualizar os repositórios de software do nosso servidor (apt-get update) e de seguida instalar o Nagios3 (apt-get install nagios3).

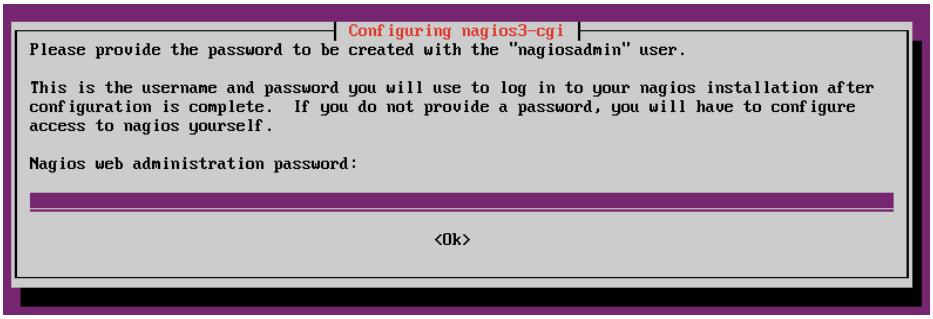

Figura 4 - Janela de configuração do utilizador web

É necessário criar um login para a interface web, que neste caso irá ter por defeito o utilizador **nagiosadmin** e a palavra-passe **cpd2020#**.

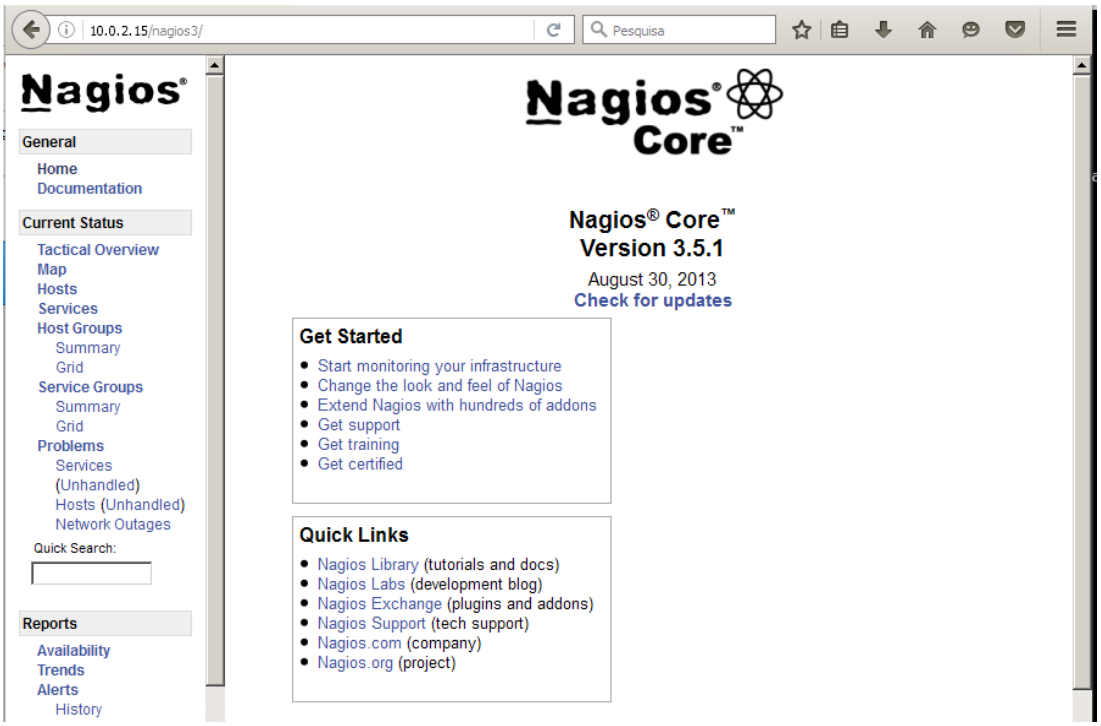

Figura 5 - Interface web de acesso ao Nagios3.

Após a instalação estar concluída é possível aceder à interface web do Nagios3 através do url http://xxx.xxx.xxx.xxx/nagios3 (utilizando o IP do servidor) usando o login de administração **nagiosadmin** / **cpd2020#**.

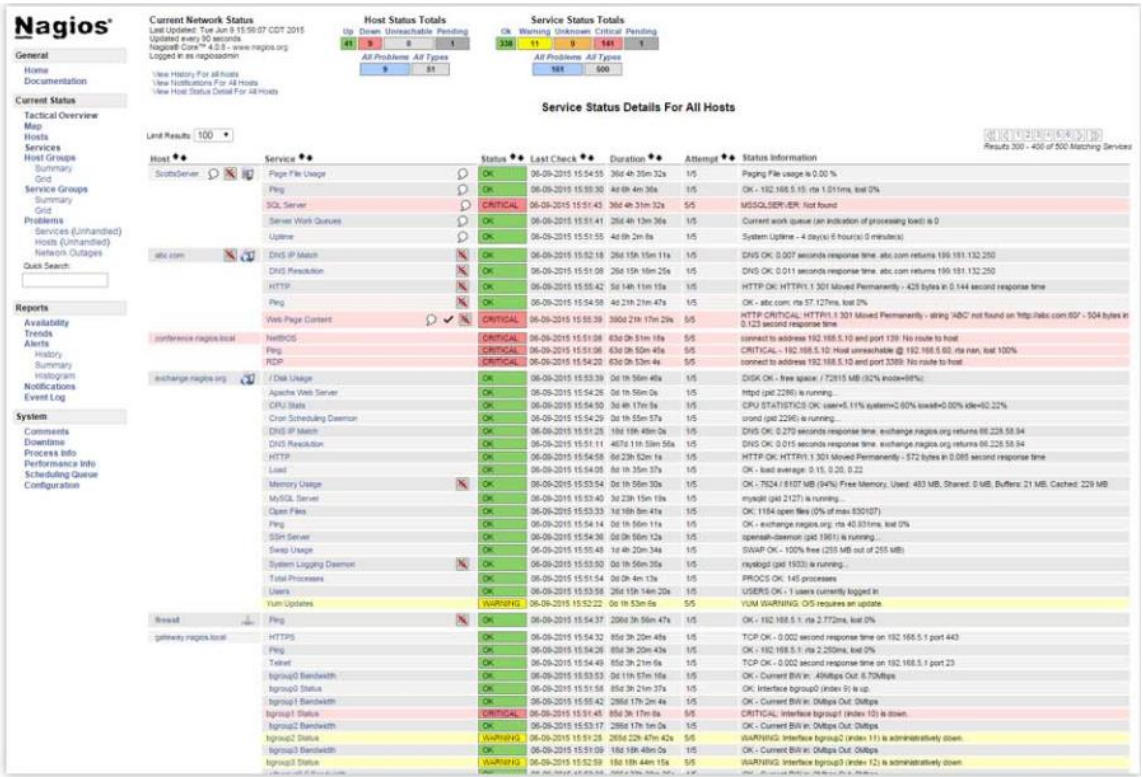

Figura 6 - Dashboard "Tatical Overview" do Nagios

A partir deste ponto já temos acesso aos dashboards web, sendo o principal o "Tactical Overview", que nos mostra o estado da nossa rede de uma forma resumida.

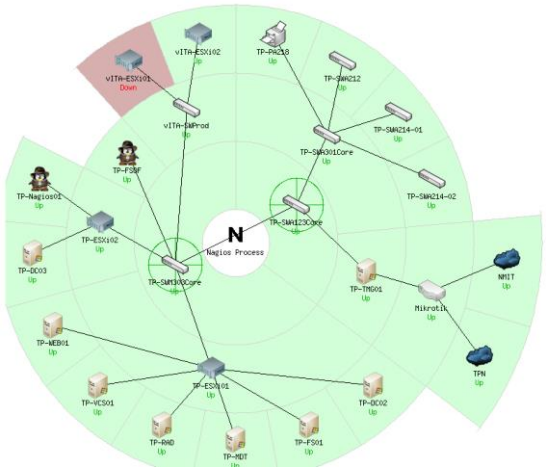

Figura 7 - Dashboard "Map" do Nagios

Ou podemos aceder ao "Map" que nos apresenta um diagrama de rede gerado automaticamente com as informações necessárias.

4.Componentes e funcionamento do Nagios Core

O Nagios utiliza uma arquitetura cliente/servidor onde existe o servidor (o Nagios), que faz os pedidos e centraliza toda a informação, e os clientes (ou agentes) que estão instalados nos equipamentos a monitorizar e que adquirem os dados necessários para o servidor.

Por sua vez o Nagios é constituído por 3 componentes principais:

- Scheduler (ou core): Executa todos os plugins ativos periodicamente, conforme a temporização definida na configuração, e consoante os resultados de certos plugins, executa ações pré-definidas;
- Plugins: Programas/scripts definidos pelo gestor/administrador, cuja função é verificar o estado de um equipamento ou serviço em concreto, obtendo informações necessárias para o Scheduler efetuar ações;
- Graphical Unit Interface (GUI): O ambiente gráfico web que mostra toda a informação necessário ao gestor/administrador de uma forma simples e estruturada.

Todas as configurações do Nagios são efetuadas através de ficheiros de texto, com a respetiva extensão "CGF", onde são definidas as configurações do Scheduler, os plugins, os hosts (equipamentos de rede) e os serviços.

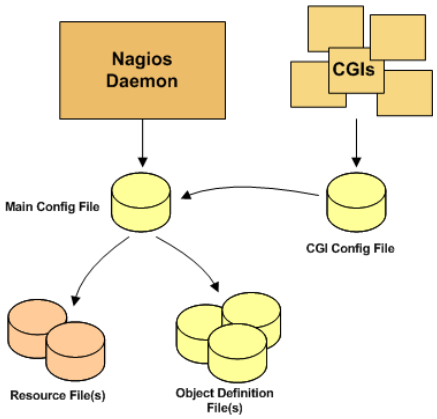

Figura *8 - Componentes do Nagios*

Existem 2 tipos de ficheiros principais de configuração:

- Ficheiro nagios.cfg: O ficheiro de configuração principal do Nagios onde estão definidas várias variáveis do sistema e caminhos para os outros ficheiros de configuração (https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/configmain.html);
- Pasta objects: Pasta que contém todos os ficheiros de configuração dos hosts (equipamentos e serviços), commands (scripts) e contacts (contactos em caso de falha) personalizados.

Na figura seguinte está apresentado um exemplo de um ficheiro de configuração de um router:

```
define host{
        host_name                       bogus-router
        alias                           Bogus Router #1
        address                         192.168.1.254
        parents                         server-backbone
        check_command                   check-host-alive
        check_interval                  5
        retry_interval                  1
        max_check_attempts              5
        check_period                    24x7
        process_perf_data               0
        retain_nonstatus_information    0
        contact_groups                  router-admins
        notification_interval           30
        notification_period             24x7
        notification_options            d,u,r
        }
```

Figura 9 - Ficheiro de configuração de um host

Neste ficheiro é possível ver o que foi definido pelo administrador:

- Fazer o quê: Executar o comando check-host-alive;
- A quem: ao Host 192.168.1.254;
- Quando: de 5 em 5 minutos, todo o dia, todos os dias;
- Notificar a quem: ao grupo router-admins;
- Em que situações: em caso de falha (d), de perca de comunicação (u) ou de recuperação (r);
- De quanto em quanto tempo: de 30 em 30 minutos, todo o dia, todos os dias.

A estrutura de pastas do Nagios3 num servidor Ubuntu é a seguinte:

- /etc/nagios3: Pasta principal
- /etc/nagios3/objects: Pasta dos ficheiros de configuração dos objetos (hosts e serviços)
- /etc/nagios-plugin/configs: Pasta dos plugins
- /usr/share/nagios3/htdocs: Pasta da página web do interface
- /usr/share/nagios3/htdocs/images/logos/base: pasta dos ícones dos hosts e do mapa
- /var/log/nagios2: pasta de logs

O modo de funcionamento e bastante simples de perceber e pode ser visto no esquema seguinte:

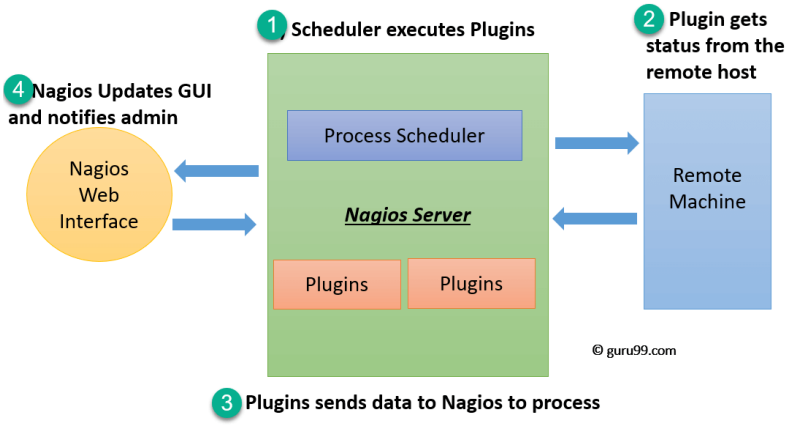

Figura 10 - Diagrama de funcionamento do Nagios

Inicialmente o Scheduler executa os plugins existentes. Os plugins obtêm os dados dos hosts e dos serviços monitorizados. Esta informação é devolvida ao Nagios e guardada. O Nagios atualiza a informação no ambiente gráfico.

Na figura seguinte vê-se o Nagios a executar um plugin que vai recolher informações sobre uma máquina Windows utilizando um agente instalado na máquina.

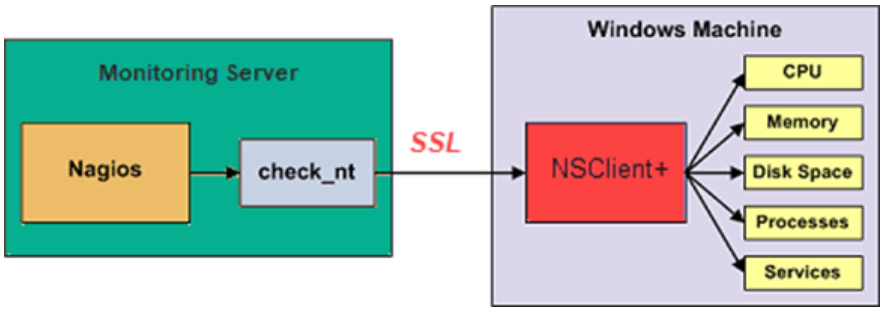

Figura 11 - Nagios a executar o plugin check_nt

Nesta outra figura pode-se ver o Nagios a executar um plugin que vai recolher informações sobre um router utilizando o protocolo SNMP.

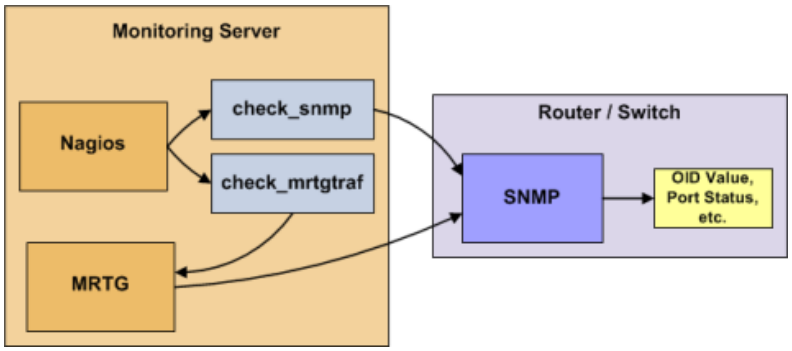

Figura 12 - Nagios a executar o plugin check_snmp

5.Cenário de monitorização de rede local em GNS3

Neste ponto iremos implementar um cenário de testes em GNS3 para validar o funcionamento do Nagios Core.

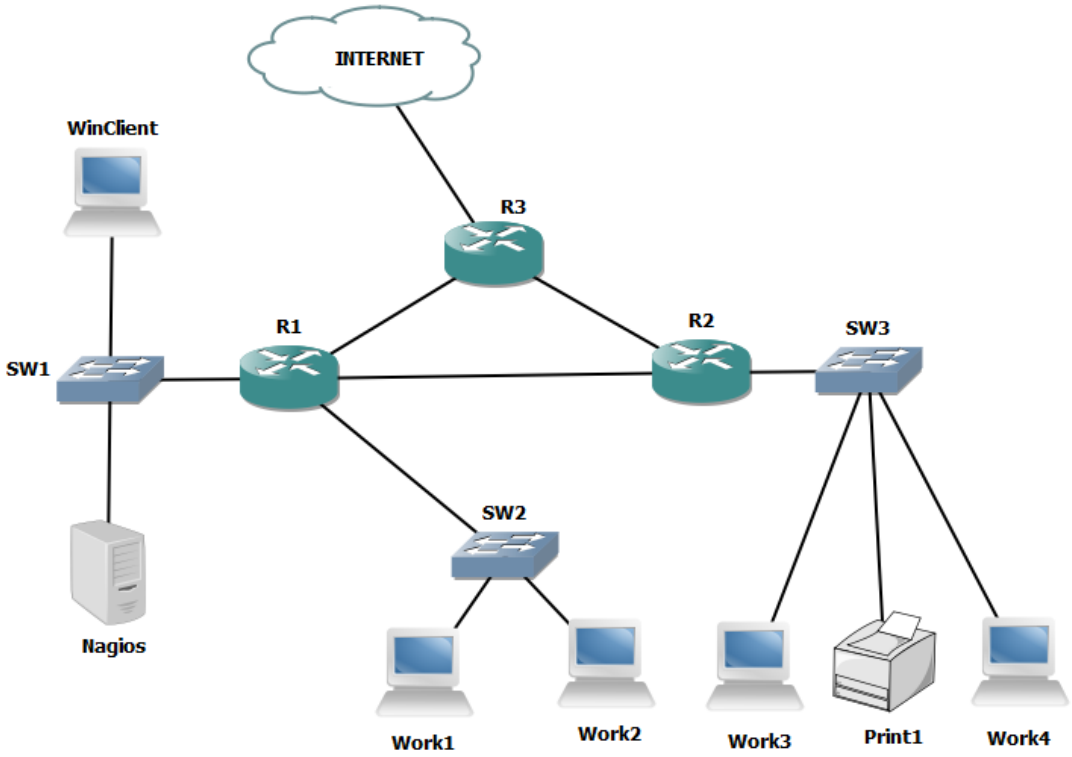

Figura 13 - Cenário de testes do Nagios utilizando o GNS3

Atendendo à arquitetura ilustrada na Figura 13, serão apresentadas de seguida as principais operações a realizar:

1. Criar o cenário utilizando o GNS3, definir o endereçamento IP e utilizar o protocolo RIPv2;
2. Instalar o servidor Nagios e todos os componentes necessários;
3. Configurar o sistema para monitorizar todas as máquinas especificadas;
4. Implementar um cliente web em Windows para visualizar a interface de gestão web;
5. Criar várias falhas nos diferentes hosts e serviços para visualizar os alertas do Nagios.

6.Monitorização de vários equipamentos físicos e virtuais

Neste ponto iremos implementar um cenário de testes em GNS3, interligado um cenário físico, que por sua vez interliga vários cenários virtuais.

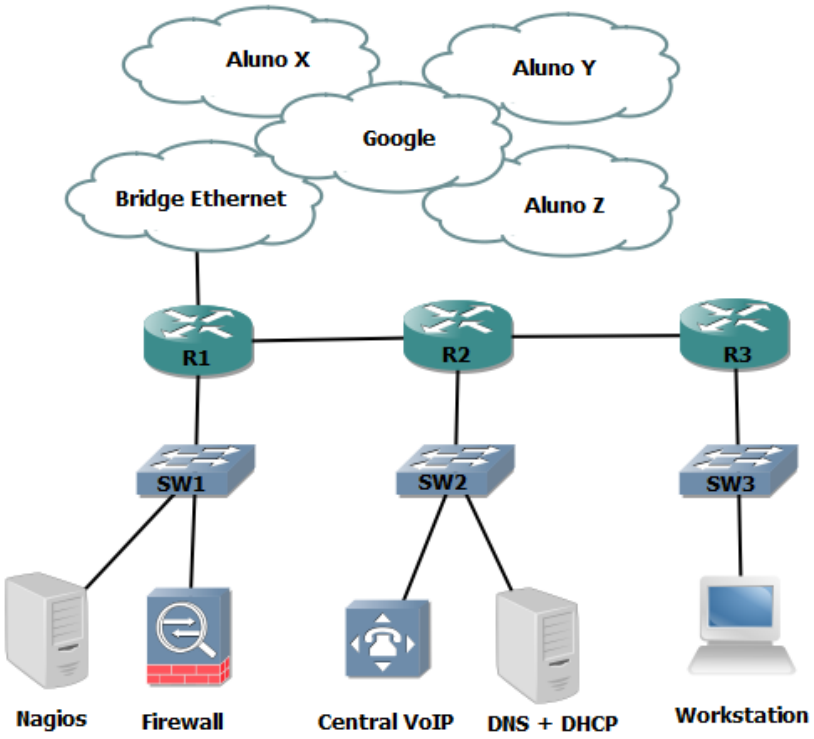

Figura 14 - Cenário de testes físico + virtual

Atendendo à arquitetura ilustrada na Figura 14, serão apresentadas de seguida as principais operações a realizar:

1. Criar o cenário utilizando o GNS3, definir o endereçamento IP, configurar o acesso à bridge manualmente utilizando a gama de IPs 5.22.0.0/16, utilizando também o protocolo RIPv2;

2. Configurar o sistema para monitorizar todas as máquinas e os serviços web das mesmas (instale um servidor web para verificar a funcionalidade do Nagios);

3. Configurar a monitorização do DNS da Google (8.8.8.8) como acesso à Internet;

4. Interligar o cenário em GNS3 com um outro aluno e testar as diferentes falhas;

5. Criar várias falhas nos diferentes hosts e serviços para visualizar os alertas do Nagios.

7. Exercícios complementares

Como exercício complementar propõe-se:

- A implementação de um servidor de monitorização baseado em Zabbix, juntamente com um cenário de testes em GNS3.

8. Documentos de apoio

- Site oficial do Nagios - https://www.nagios.org/
- Site oficial do Zabbix - https://www.zabbix.com/