LAB 08 - *Clusters* de alta disponibilidade

Tópicos

1. Implementar um cenário de rede em GNS3 que simule um *cluster web* de alta disponibilidade que implemente redundância e balanceamento de carga.

1. *Cluster web* em GNS3

Para se implementar um *cluster* para um qualquer serviço é necessário ter em atenção que o serviço que este disponibiliza nunca pode falhar, ou seja, tem de estar sempre disponível (consoante as especificações da alta disponibilidade pretendida). Para tal é necessário implementar redundância, balanceamento de carga e principalmente segurança.

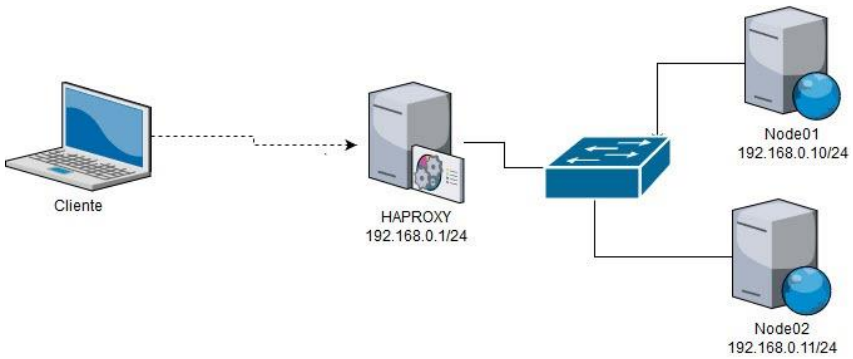

Figura 1 – Arquitetura HAProxy

A ferramenta HAProxy (Figura 1) permite ter alta disponibilidade (HA) do serviço, implementando redundância e balanceamento de carga (do serviço apenas), mas é necessário ter em conta que o próprio HAProxy pode falhar, o que significa que este é um ponto de falha crítico. De forma a mitigar esse ponto de falha é necessário implementar redundância no próprio HAProxy, nomeadamente utilizando ferramentas como o Heartbeat, o Pacemaker ou o KeepAlived (VRRP). Outro aspeto importante é que além da redundância do serviço (L7) é necessário também implementar redundância a nível de equipamentos de rede, seja a nível da camada 3 (routers) ou da camada 2 (*switches* e interfaces em modo *bridge*).

Neste laboratório será implementado um cenário no qual estará representado um *cluster web* que terá todos os aspetos referidos anteriormente, de forma a se conseguir simular um cenário de ambiente real que tenha todas as proteções de falha necessárias.

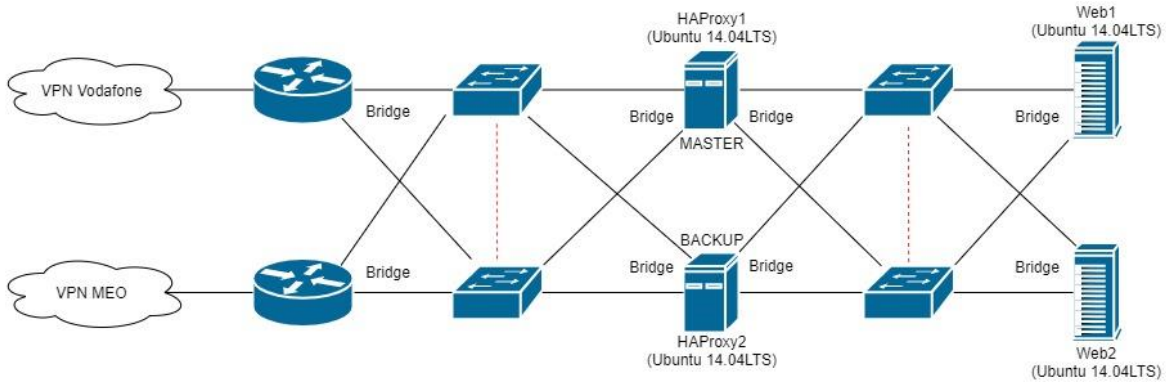

Figura 2 – Cenário em GNS3

Na Figura 2 está representado o cenário a implementar (de notar que as ligações entre os *switches* não podem existir para não causar *broadcast storms* no cenário), serão utilizadas as ligações VPN existentes para utilização no Trabalho Laboratorial nº2 para interligar os vários cenários dos alunos. Será necessário configurar *port-forward* nos routers de modo a permitir a comunicação de fora da rede (VPN) para dentro do cenário (nomeadamente acesso ao HAProxy). Será necessário implementar redundância L2 tanto nos routers como nos servidores (*bridges*) e redundância L3 na saída dos servidores HAProxy para a VPN (HSRP/VRRP/GLBP). Os servidores *web* internos não poderão aceder ao exterior e apenas poderão ser acedidos pelos servidores HAProxy, garantindo assim segurança aos servidores *web*. Na implementação dos diferentes serviços necessários utilize as configurações que achar necessárias, reutilizando o *know-how* adquirido nos laboratórios anteriores.