PROJETO INTEGRADOR DO 4º SEMESTRE DA LEI-ISEP

RCOMP - Ambiente de rede para testes das aplicações

O projeto comporta o desenvolvimento de 3 aplicações/componentes na área de RCOMP, no sprint 4 / sprint C as interações relevantes para RCOMP são:

- Simulador/emulador de máquina

Existem várias instâncias em execução.

Envia pedidos (**cliente TCP**) ao SCM (**US1011**)

Recebe pedidos (**servidor UDP**) do SMM (**US1012**)

- Serviço de comunicação com as máquinas (SCM)

Existe apenas uma instância em execução.

Recebe pedidos (**servidor TCP**) das máquinas (**US4002**)

- Sistema de monitorização das máquinas (SMM)

Existe apenas uma instância em execução.

Envia pedidos (**cliente UDP**) às máquinas (**US6001**)

Recebe pedidos HTTP (**servidor TCP**) de acesso ao Web Dashboard (**US3008**)

Ambiente para testes das aplicações

Nas primeiras fases de desenvolvimento as aplicações de rede podem ser testadas todas no mesmo nó, nessa situação todas as aplicações estão acessíveis no endereço 127.0.0.1 (localhost). Em fases de teste mais avançadas e durante as demonstrações, este cenário deixa de ser suficiente porque não é possível ter várias aplicações no mesmo nó a utilizarem o mesmo número de porto.

Existe uma grande variedade de soluções quanto a criar um ambiente de testes composto por múltiplos nós de rede adequado para este conjunto de aplicações, mas muitos introduzem dificuldades relevantes relacionadas com bloqueios por ***firewalls*** e utilização de endereços privados (NAT).

Assim no sentido de minimizar as dificuldades propõe-se que a solução se baseie na utilização dos servidores SSH do DEI e nos serviços de VPN do DEI, tal como foi proposto e exaustivamente analisado na aula PL09.

Os servidores SSH do DEI estão todos ligados à mesma rede privada 10.8.0.0/16. Quando ligado ao serviço de VPN do DEI, também o posto de trabalho do utilizador está ligado a esta mesma rede.

Acresce que se os elementos de um grupo estão ligados ao serviço de VPN do DEI, então os respetivos postos de trabalho estão todos ligados à mesma rede.

Nestas circunstâncias não existem barreiras às comunicações com a exceção do ***firewall*** do posto de trabalho do utilizador, cabe ao utilizador criar regras de exceção que permitam a entrada do tráfego desejado.

Notas sobre comunicações entre aplicações cliente/servidor UDP ou TCP

Recordando, para uma aplicação cliente UDP ou TCP poder enviar um pedido a uma aplicação servidora UDP ou TCP é necessário que:

- A aplicação cliente conheça o **endereço e número de porto da aplicação servidora**.

  Por essa razão as aplicações servidoras devem usar um número de porto fixo pré acordado (normalmente hardcoded na aplicação cliente e na aplicação servidora).

  O endereço de uma aplicação é o endereço da máquina onde essa aplicação é colocada em execução. Dependendo do sistema operativo é possível saber o endereço da máquina de várias formas, por exemplo o comando **ip config** em sistemas Windows.

- Não exista nenhum firewall a bloquear o tráfego.

  Os nós de rede, incluindo os postos de trabalho, têm firewalls que tipicamente bloqueiam qualquer tráfego de entrada que seja desconhecido. Ao colocar uma aplicação servidora em funcionamento num nó é necessário adicionar uma exceção ao firewall no sentido de permitir o tráfego destinado à aplicação. Alguns sistemas operativos detetam quando a aplicação servidora é colocada em funcionamento e questionam diretamente o utilizador se pretende adicionar uma exceção para permitir o tráfego.

  As configurações típicas dos firewalls permitem o tráfego de saída sem restrições.

  Normalmente os firewalls permitem todo o tráfego interno usando a interface de loopback (localhost/127.0.0.1), assim as comunicações entre duas aplicações em execução no mesmo nó de rede não sofrem interferências do firewall.

- O endereço da aplicação servidora seja acessível à aplicação cliente.

  Se a aplicação cliente está numa rede pública e o servidor está numa rede privada a comunicação não é possível a menos que sejam definidas regras no dispositivo de interface entre a rede pública e a rede privada. Ou seja regras de NAPT estático muitas vezes designadas de port forward.

  Note-se que a maioria das implementações de virtualização (e.g. containers e máquinas virtuais) usam por omissão configurações de rede virtual em que a rede é privada. **Isso significa que aplicações servidoras executadas em ambientes virtuais não são acessíveis fora do ambiente virtual a menos que o sistema de virtualização seja configurado nesse sentido.**