Grupo 046
Hugo Fernandes (1161155), Norberto Sousa (1120680), Pedro Barbosa (1150486)

Administração de Sistemas

Tarefa Complementar 2, 18 de novembro 2018

Tarefa Complementar

Virtual Machine (VM) vs. *Container* (CT) & Segurança de VM

*Virtual Machine*s (VM) vs. *Container* (CT)

Virtual Machine

- Uma **VM** é uma simulação de um computador, com uma **VM** dá para correr múltiplos "computadores" num só, simulando-os.

- Utilizando **VM's** cada uma requer o seu próprio ***OS*** enquanto que o hardware é virtualizado, todas as **VM's** partilham recursos do mesmo ***host***. Para gerir e virtualizar as **VM's** é usado um ***hypervisor*** que faz a conexão entre ***hardware*** e a ***virtual machine***.

- **VM's** são uma boa maneira de diminuir custos e aumentar a eficiência de múltiplos departamentos de ***IT***, uma desvantagem é que utiliza muitos recursos do sistema, porque para alem de cada ***VM*** necessitar de uma cópia completa do seu ***OS*** também precisa de uma cópia virtual do ***hardware***, isto acaba por ser bastante pesado para o ***CPU*** e usar bastante ***RAM***.

Container

- Nos **CT's** em vez de virtualizar todo o computador apenas o ***OS*** é virtualizado, ao contrário das **VM's** os **CT's** estão colocados acima do ***OS*** do ***host***, cada **CT** partilha o ***kernel*** do ***OS*** do ***host*** com todos os outros **CT's** e com o próprio ***host***.

- Como partilham os mesmos recursos faz com que **CT's** sejam muito leves para o sistema á volta de alguns ***megabytes*** e começam em segundos.

- Devido aos seus requisitos mais baixos, é possível correr mais aplicações num só ***host*** com **CT's** do que com ***VM's***, e consegue-se fazer um ambiente para **desenvolver**, **testar** e dar ***deploy***.

Comparação

VM's são sem dúvida mais "pesadas" para o sistema que **CT's**, contudo o mesmo sistema pode ter múltiplas **VM's** diferentes a correr com ***OS's*** diferentes o que pode ser um fator que faz com que a escolha de **VM's** seja mais adequada. As **VM's** são também mais seguras que os **CT's** porque são completamente isoladas ao contrário dos **CT's** que apenas são isolados ao nível dos processos.

CT's são mais leves, tem performance nativa ao contrário da performance limitada das **VM's**, demoram apenas minutos a serem iniciados, exigem menos espaço de memoria que as **VM's**. **CT's** serão uma melhor escolha em casos em que seja pretendido correr um grande número de dispositivos com o mesmo sistema operador.

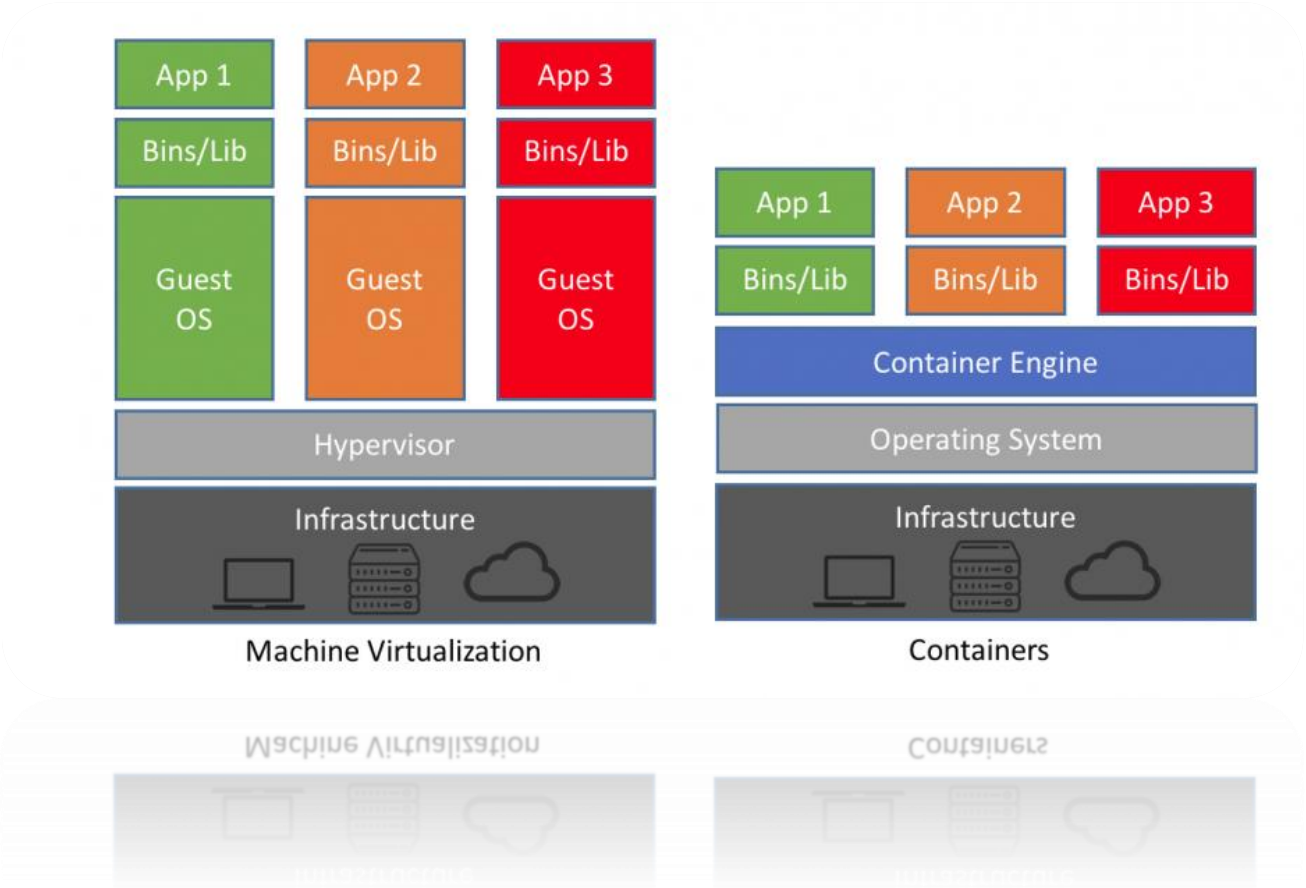

FIGURA 1 - ESTRUTURA VM & CT

Segurança da *VM*

1. **Adicionar regras às IPTABLES:**

```
asist@AsistServer:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -s 192.168.126.1/32 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j DROP
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -s 192.168.126.1/32 -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j DROP
-A OUTPUT -d 192.168.126.1/32 -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 0 -j DROP
asist@AsistServer:~$
```

Os comandos introduzidos respetivamente são para:

- **1º - 2º, Permite IP's das máquinas pessoais bloqueia os restantes**
- **3º, Permite pedidos WEB de qualquer origem**
- **4º-7º, Permite ICMP de e para as máquinas pessoais**

2. **Representação das regras das IPTABLES:**

```
asist@AsistServer:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.126.1        anywhere            tcp dpt:ssh
DROP       tcp  --  anywhere             anywhere            tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:http
ACCEPT     icmp --  192.168.126.1        anywhere            icmp echo-request
DROP       icmp --  anywhere             anywhere            icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             192.168.126.1       icmp echo-reply
DROP       icmp --  anywhere             anywhere            icmp echo-reply
asist@AsistServer:~$
```

3. **Pacote de persistência de IPTABLES:**

```
asist@AsistServer:~$ sudo apt-get install iptables-persistent
Reading package lists... Done
Building dependency tree
Reading state information... Done
iptables-persistent is already the newest version (1.0.4).
0 upgraded, 0 newly installed, 0 to remove and 78 not upgraded.
asist@AsistServer:~$
```

4. **Guardar IPTABLES:**

```
asist@AsistServer:~$ sudo netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
asist@AsistServer:~$
```

5. **Script que fecha sessão de *ssh* após um intervalo de tempo:**

```
#!/bin/bash

#o script corre no background mal a sessao ssh é iniciada
#vai esperar 300seg (5min) antes de correr o resto do codigo
sleep 300

#ao fim do tempo dado, lista os processos do sistema (ps aux),
#filtra os que dizem sshd (grep sshd),
#substitui multiplos espacos por apenas um espacos (tr -s " "),
#seleciona a primeira(user) e a segunda(pid) coluna do output (cut -d " " -f1,2)
#filtra os do utilizador currente (grep $USER)
for i in $(ps aux | grep sshd | tr -s " " | cut -d " " -f1,2 | grep $USER)
do
        #para cada linha do output vai pegar na segunda coluna(pid) e executar um kill command
        #terminando assim essa sessao
        sessionPID=$(echo $i | cut -d " " -f2)
        kill $sessionPID 2>null
done

exit
```

6. **Linha do ficheiro /etc/ssh/sshd_config que chama o script:**

```
Match all
        ForceCommand (/etc/ssh/ssh_session_limit.sh)& bash
```

Bibliografia

Virtual Machines vs. Containers:

- https://www.backblaze.com/blog/vm-vs-containers/ - 18 nov. 18.
- https://blog.netapp.com/blogs/containers-vs-vms/ - Figura 1 – 18 nov. 18
- https://www.sdxcentral.com/cloud/containers/definitions/containers-vs-vms/ - 18 nov. 18.

Segurança da Virtual Machine:

- https://www.digitalocean.com/community/tutorials/iptables-essentials-common-firewall-rules-and-commands?fbclid=IwAR2luKU7sG0pe3YFAEut5wpxo3zgk-RWCfpgyeon3I98B9UbPnItOiBZAFU – IPTABLES – 18 nov. 18.

- https://superuser.com/questions/1136785/is-it-possible-to-set-a-time-limit-on-an-active-ssh-connection-for-a-specific-li?fbclid=IwAR3cXwbDJSDrI6yp7_lkX3xLHjJ9lY1d4cwyOkPzOr_bb__KkPY7-mMKKhI – Conexão SSH – 18 nov. 18.

- https://tinyurl.com/yddxc8dw - Conexão SSH - 18 nov. 18.