Introdución á Virtualización de Sistemas

Introdución

A virtualización consiste na creación a través de software dunha versión virtual de algún recurso tecnolóxico, como pode ser unha plataforma hardware, un dispositivo de almacenamento ou outros recursos de rede.

Normalmente cando falamos de virtualización nos referimos á *virtualización de plataformas*, que fai referencia á creación de máquinas virtuais que actúan como ordenadores normais co seu propio sistema operativo.

Para conseguir esto se empregan dúas aproximacións distintas, a Virtualización Hardware e a Virtualización a nivel de Sistema Operativo.

Virtualización Hardware

O software que se executa nesas máquinas virtuais non accede directamente aos recursos hardware, se non que o fai a través dun software chamado ***hypervisor*** ou ***virtual machine monitor***, que é o que vai a determiñar o modo no que o sistema virtualizado actúa co hardware real da máquina.

A máquina real recibe o nome de ***Host***, mentras que a máquina virtualizada denomínase ***Guest***.

Segundo o modo de funcionamento do *hypervisor* podemos distinguir entre:

- **Hypervisor Type I, "nativo" ou "*bare-metal*"**

  O hypervisor funciona directamente encima do hardware, sendo realmente o sistema operativo da máquina. Normalmente se proporciona unha primeira máquina virtual *(en terminoloxía Xen, dom-0)* con privilexios especiais e cun sistema operativo mínimo para poder xestionar os sistemas virtualizados *(en terminoloxía Xen, dom-U).* Neste tipo de sistemas o acceso ao hardware por parte do hypervisor pode ser directo.

  Exemplos deste tipo de hypervisores son **KVM, Hyper-V, VMWare ESXi ou Xen.**

- **Hypervisor Type II ou "hosted"**

  O hypervisor é unha aplicación que funciona sobre o sistema operativo, polo que o acceso ao hardware real se realiza normalmente a través de chamadas ao sistema.

  Exemplos deste tipo de hypervisores son **VirtualBox ou VMWare Fusion/Player/Server**

A misión do Hypervisor é proporcionar ao sistema anfitrión un entorno virtual hardware donde executar o sistema. O sistema virtualizado dispón dos distintos recursos hardware que lle ofrece o hypervisor (cpu, memoria, tarxetas de son e vídeo, etc...) exactamente igual que si foran recursos reais, aínda que están implementados por software en lugar de hardware, de xeito que se poderá instalar calqueira sistema operativo compatible co hardware emulado. Evidentemente, esto supón unha penalización grande no rendimento.

Co obxectivo de acelerar a execución de estas máquinas emuladas, as CPU modernas ofrecen varias extensións que o hypervisor pode utilizar para darlle un aceso máis directo á CPU real, sen

necesidade de emulala completamente. Estas extensións se chaman ***Intel VT*** (VT-x, VT-d) nas CPU Intel, e **AMD-V** (amd-v, amd-vi) nas CPU AMD.

Outra posibilidade de acelerar a execución das máquinas virtuais é modificar o sistema invitado (guest) de xeito que en lugar de realizar chamadas ao hardware emulado chame directamente ao hypervisor que ofrece unha interfaz moi similar ao hardware real, evitando a necesidade de emulación. *Esta técnica recibe o nome de* ***paravirtualización***, a as chamadas a estas interfaces reciben o nome de ***hypercalls***.

A *paravirtualización* consigue un excelente rendemento, pero o problema é que é necesario modificar o sistema operativo de xeito que sexa capaz de acceder as características proporcionadas polo hypervisor o que non sempre é posible.

Actualmente todos os Kernel de Linux están preparados para aproveitar as extensións de paravirtualización ofrecidas por Xen, polo que é posible virtualizar sistemas Linux baixo este *hypervisor* sen necesidade de extensións na CPU (amd-v ou vt-x).

Windows soporta algunhas chamadas paravirtualizadas Hyper-V, ás que chama "*enlightements*".

Unha solución intermedia é o uso de drivers no sistema invitado que permitan un acceso máis directo ao hardware real do sistema (*drivers paravirtualizados*) ademáis da posibilidade de utilizar diferentes características ofrecidas polo hypervisor mediante as distintas "guest-additions" dos diferentes hypervisors ou os drivers "virtio" utilizados por KVM. Esta solución normalmente se emprega para acelerar o acceso ao disco, á rede e para mellorar a xestión da RAM.

A virtualización hardware nos permite executar distintos sistemas operativos nunha mesma máquina que fan uso dos seus propios recursos dun xeito completamente aillado da máquina principal, o que facilita o deseño de sistemas de alta dispoñibilidade evitando que unha caída dunha máquina afecte ao resto, e melloran o aproveitamento dos recursos físicos dispoñibles reducindo polo tanto o custe operativo.

Virtualización a Nivel de Sistema Operativo

A virtualización a nivel de sistema operativo consiste na execución de varios entornos operativos de xeito aillado baixo un mesmo kernel. Cada entorno ve o sistema como si fora o único entorno en execución dispoñendo do seu propio árbol de arquivos, memoria e recursos de CPU, polo que tamén reciben o nome de "***containers***"

Sistemas de este tipo son as ***Solaris Zones, BSD Jails, VirtuoZZo, OpenVZ ou LXC***.

Hoxe en día, se están popularizando entornos deste tipo orientados a execución de aplicacións específicas en lugar de entornos operativos completos. Exemplos deste tipo son ***Dockers*** ou ***Snap***.

A virtualización a nivel de sistema operativo en realidade non precisa emular ningún tipo de hardware, polo que non ten ningunha pérdida de rendimento respecto ao host, ademáis como todos os sistemas comparten Kernel, precisan moitos menos recursos.

O principal inconvinte é que o aillamento dos distintos sistemas virtualizados non é tan completo como no caso da virtualización hardware, o que pode ocasionar problemas de seguridade e dispoñibilidade. Además únicamente se poderán virtualizar sistemas que podan funcionar baixo o mesmo Kernel que o host.

Libvirt / KVM

Libvirt é unha librería de virtualización de Linux que nos proporciona unha serie de utilidades de xestión da virtualización independentes do hypervisor, sendo capaz de xestionar máquinas virtuais KVM, VirtualBox, Xen, Containers LXC ... etc.

Mediante libvirt podemos xestionar os distintos elementos das redes virtualizadas que son:

- **As configuracións de rede**

  E posible definir "redes" onde se conectarán as máquinas virtuais que vaiamos creando con distintas configuracións de conectividade. Cando as máquinas virtuais arranquen se conectarán as redes predefinidas. Deste xeito, podemos ter preconfiguradas distintas redes para a integración das máquinas virtuais.

- **As configuracións de almacenamento**

  Tamén se poden definir "Pools" de almacenamento, que son os lugares onde se poden crear e coller os distintos discos que utilizarán as máquinas virtuais. Libvirt soporta moitos tipos de Pools, dende unha carpeta do sistema ata almacenamentos de rede NFS, iSCSI... etc.

- **Os Hosts de Virtualización**

  Outro dos elemento son os hosts de virtualización. Mediante libvirt podemos acceder a distintos equipos da rede e crear, arrancar, parar máquinas virtuais en eles, crear configuracións de rede e de almacenamento e migrar máquinas virtuais que se están executando nun host a outro (migración en vivo).

As máquinas virtuais xestionadas dende libvirt se constrúen a partir dunha definición da máquina en XML que indica o distinto hardware de que se vai a compoñer: CPU, tarxetas de rede, discos fixos e dvds, memoria RAM ... etc. Os hardware paravirtualizados baixo KVM son de tipo VirtIO,

Dende a liña de comandos poderemos xestionar a virtualización en cada host da rede mediante o comando ***virsh***. O comando virsh soporta multitude de configuracións de máquina virtual que se deben importar a partir da súa definición XML. Para editar e modificar a configuración XML dunha máquina virtual existente podemos utilizar ***virsh edit nomemaquina***, o que nos permitirá acceder a configuracións de rede, de discos, de hardware... etc.

Si lanzamos unha máquina virtual dende a liña de comandos podemos acceder áo sistema virtualizado mediante un visor de VNC ou SPICE (segundo o tipo de pantalla elexido) ou mediante mecanismos típicos de acceso remoto, como ssh, RDP ... etc.

Máis práctico para a creación de máquinas virtuais (pero máis limitado) é o uso dunha aplicación gráfica chamada ***virt-manager***, que permite a configuración do hardware dun modo moi simple, xestionar as operacións básicas sobre as VM e de proporcionar un visor apropiado para a máquina.

Xestión de Discos

libirt e KVM soportan multitude de formatos de discos como ***raw, qcow, qcow2, vmdk, qed, vpc*** ou ***vdi.*** Dende o virt-manager poderemos crear e asignar a unha máquina virtual discos de calqueira de estes formatos, sen embargo os formatos máis importantes son ***qcow2*** e ***raw***

- ***qcow2*** : Imaxes “CopyOnWrite”, so utilizarán espacio en disco cando se escriba e irán crecendo a medida que se escribe información neles. Soportan características avanzadas, como a creación de “snapshots”. Un “snapshot” é unha imaxe que únicamente irá almacenando as diferencias de información entre unha imaxen orixinal (imaxen base) e a actual. A súa creación é instantánea e so ocuparán a información que sexa distinta da orixinal. Isto permite o despregue rápido de máquinas virtuais, prácticamente instantáneo.
- **raw** : A maior vantaxe das imaxes raw son a velocidade e a compatibilidade. Son simples imaxes binarias de disco, e non teñen características especiais (como snapshots). A súa ocupación en disco é a indicada na súa creación (salvo si se utilizan sistemas de arquivos con soporte de ***extents*** coma ext4, que únicamente reservan o espazo utilizado de disco).

Si xestionamos a máquina virtual editando o XML (***virsh edit nome_máquina***), é posible engadir discos / particións reais para o uso da VM .

Si queremos xestionar os discos con máis control dispoñemos da utilidade ***qemu-img.*** Mediante esta utilidade podemos realizar operacións que non permite o virt-manager como a creación e xestión de snapshots, conversión de formatos, cambios de tamaños, chequeos e reparacións.... etc.

Xestión de Rede

A xestión da configuración de rede varía segundo utilizamos hypervisores de tipo I ou de tipo II. Os hypervisores de tipo II (VirtualBox) xestionan a rede mediante comandos do Hypervisor, mentras que normalmente os hypervisores de tipo I poden xestionar a rede coas ferramentas habituais de configuración de rede.

Cando arrancamos unha máquina virtual con tarxeta de rede, o sistema creará unha parella de ethernets virtuais conectadas, unha estará situada na máquina virtualizada e a outra no hypervisor. O hypervisor xestionará a conectividade da máquina virtual colocando o seu extremo como se lle indique, normalmente recurrindo a bridges ou switchs virtuais (openvswitch) si se necesitan conectar varias máquinas entre sí.

A configuración da conectividade nos hypervisores tipo I se realizará exactamente igual que en calqueira máquina real.

Xestión de Hosts

Normalmente a virtualización se utiliza para gañar dispoñibilidade e mellorar o aproveitamento de recursos establecendo redes de virtualización mediante varios Hosts capaces de executar varias máquinas virtuais.

Para xestionar esto se recurre a Pools de almacenamento en rede (para os discos do sistema) compartidos mediante NFS ou iSCSI, redes preconfiguradas (bridges e switch virtuais) onde se poden enganchar as máquinas arrancadas ... etc.

Unha das características máis importantes en canto a dispoñibilidade é a posibilidade de mover unha máquina virtual dun host da rede de virtualización a outro, sen necesidade de parar o seu funcionamento e sin interrupción do servicio. Esto permite o mantemento e ampliación do hardware, e a solución de problemas sen perda de dispoñibilidade.

Para facer posible a migración (Live-Migration) é necesario que se cumplan varias condicións:

- Os Hosts da rede que interveñen na migración deben soportar as características do hardware virtualizado. En particular a CPU.
- Os Kernels dos Hosts que intervelñen na migración deben ser iguais para asegurar o éxito.
- Os sistemas de almacenamento utilizados deben estar accesibles dende todos os hosts na misma dirección (na mesma carpeta, iqn iSCSI ... etc)
- As configuracións de rede no host destiño deben ser compatibles coas establecidas nos hosts orixen.

Para garatizar esto, o máis simple é o uso do mesmo hardware e versión de sistema, e a creación da mesma estructura de rede (bridges e switches virtuais) en todos os hosts da rede de virtualización.

Tamén é tipico de recurrir a NAS ou SAN para proporcionar á rede o espazo físico de almacenamento para a creación do almacenamento virtual de xeito que sempre sexa accesible dende todos os hosts da rede, o que fai máis sencillo a xestión dos discos e sistemas de almacenamento.