A consolidação do Servidor implica a combinação de cargas de tranalho (termo inglês workloads) provenientes da separação de máquinas ou aplicações dentro de um pequeno número de sistemas ou aplicações.

Existem servidores de consolidação que são chamados de *"consolidation".* A medida de consolidação é chamado de *"consolidation ratio"*, que é calculada, fazendo a contagem do nº de máquinas virtuais num determinado servidor – por exemplo um servidor que tenha mais de 8 máquinas virtuais conectadas e que são executadas por uma taxa de 8:1.

A consolidação foi uma mais-valia na isolação das "*data-centers*" e das operações dos gerenciadores, pois, foram resolvidos o numero de problemas quando um nível crítico tinha sido alcançado. Com uma taxa de consolodação de 4:1, foi possível remover três-quartos de serrvidores na data center.

Além da consolidação, um segundo desenvolvimento ocupou o patamar. Como empresas/organizações começou por se ver os benefícios da virtualização, pois estes nunca mais adquirem novo hardware quando estes acabaram as suas concessões, ou quando estes obtêm o equipamento, quando as licenças de manutenção de hardware expiram.

Em vez disso, estes virtualizaram as cargas de trabalho dos servidores de multiplas formas. Isto tem como nome "containment". Containment beneficiou muito as empresas em apenas 1 ano e todos os custos de gerenciamento e manutenção dos servidores, no que toca à energia, arrefecimento, etc. As taxas de consolidação (*consolidation ratios*) da primeira geração de x86 dos *"hypervisors"* estavam numa taxa de 5:1.

(pag. 31 book virtualization vmware).

Operação de software de virtualização

Virtualizando um servidor

O modelo utilizado para a virtualização de um servidor é composto pela parte física de duas soluções de software e hardware. O hypervisor abstrai de uma camada física, apresentando a asbstração para servidores virtuais, assim como máquina virtuais a utilizar.

Um hypervisor é instalado diretamente no servidor sem qualquer tipo de sistema operativo, entre este e os equipamentos físicos. Porém, as máquinas virtuais já os possuem instanciados ou inicializados. Nas máquinas virtuais, podemos os ver e o trabalho entre os recursos de hardware. Assim , o hypervisor, acaba por se tornar uma interface entre os dispositivos num servidor físico e em dispositivos virtuais de máquinas virtuais. O hypervisor apresenta apenas um subconjunto dos testes dos recursos físicos para cada máquina virtual individual e controla a atual I/O da máquina virtual para o dispositivo físico e de volta novamente. Os hypervisors fazem mais do que apenas fornecer uma plantaforma para executar uma máquina virtual.

Enquanto os hypervisors são os ambientes virtuais, as máquinas virtuais são os motores que fornecem desempenho para as aplicações. As máquinas virtuais possuem tudo o que as contrapartes físicas destas fazem (sistemas operativos, aplicações, rede, coneções acesso ao armazenamento e outros recursos fundamentais), mas zipados em um conjunto de ficheiros de data. Este pack torna as máquinas virtuais mais flexíveis e mais fácil de gerir através do uso das propiedades tradicionais numa nova perspetiva. As máquinas virtuais podem ser replicadas, atualizadas e movidas de um lugar para outro, sem ter que interromper

as aplicações do utilizador.

Virtualizando desktops

A computação de desktop para as empresas é caro e ineficiente em muitas frentes. Isto requer equipas de funcionarios para controlar a atualização de um software migrações e processos de patching, não para mencionar o suporte de hardware. Desktops virtuais são executados em servidores do centro de dados pois, estes são muito mais potentes e mais confiáveis ,no que toca ao hardware, do que um computador tradicional. As aplicações onde os utilizadores conectam também se encontram no centro de dados, onde são executados em servidores, porém, toda o tráfico de rede terá que voltar atrás para o centro de dados, reduzindo este e expande os recursos de rede.

Os desktops virtuais são acedidos através dos "*thin clients*" (termo "clientes magros"), ou outros dispositivos. Os *"thin clients"* tem uma expetativa de 7 a 10 anos onde poreão ser recarregados com menos frequencia. Eles apenas utilizam entre 5 a 10% da eletricidade do computador. Nas grandes empresas, estas despesas aumentam rapidamente. Se o thin client faz um break, um utilizador poderá se substituir, em vez de confiar num engenheiro especializado em hardware para o substituir. O desktop virtual onde toda a data tem se mantido não foi afetado pela falha de hardware. Na verdade, todos os dados presentes na data não poderão sair da data center(centro de dados), pois caso isso aconteça, o o risco de roubo desses dados poderia causar sérios problemas a nível de segurança.

A data é gerido e reforçado por um professional, em vez de um

utilizador inexperiente. A criação imagens de desktop como máquinas virtuais, proporcionam economias de custo da virtualização do servidor. Um administrador de desktop pode criar e gerir poucas imagens que são partilhados entre centenas de pessoas. Os patches poderão ser aplicados nestas imagens e poderão garantir para a chegada de um utilizador, levando em consideração que isto não é frequentemente o caso com um desktop físico. No caso de um *rolled patch* ou outro software altera ou dá break na aplicação, o administrador poderá direcionar os utilizadores de volta para a imagem original, pois um simples logout e login irá devolver estes para um novo ambiente de trabalho funcional.

Uma grande diferença proém da área de segurança. Nos dias de hoje, os computadores já trazem o antivírus instalado, pois é uma grande ajuda na proteção da data da presença de malware e outras ameaças. A virtualização permite novos métodos de proteção, pois é preferivel usar esses do que instalar um software de malware em desktops virtuais individuais. Este nomo modelo reduz o *overall I/O* e o uso do processador proveniente do download das novas definições.

Virtualizando Aplicações

Como sabemos, tanto os softwares de computador ou plicações poderão também ser virtualizados. Como ambos o servidor e virtualização de desktop, existem um numero de diferentes soluções para este problema. Existem duas razões para a virtualização da aplicação :

- A primeira razão é a facilidade de implementação . Algumas empresas devem gerir centenas e milhares de diferentes aplicações. A cada altura, uma nova versão de cada destes aplicações é disponibilizada , pois, a empresa decide atualizar para uma nova versão, criando assim uma cópia para todos os computadores. Para um ou pequeno número de computadores, isto torna-se uma tarefa trivial. Como podemos constatar, as equipas de cooperação IT possuem ferramentas que contribuem para gerir e automatizar esta tarefa, para que esta aconteça repetidamente e confiavelmente.

- A segunda razão é como diferentes aplicações interagem umas com as outras. Como podemos ver, é difícil saber como atualizar para uma solução pode afetar outras aplicações. Simples atualizações de softwares como o Adobe Acrobat Reader ou o Mozilla Firefox poderão ser problematicos. Alguns tipos de aplicações de virtualização podem evitar esse problema, encapsulando o processo e o software. Muitas estratégias tomadas pelas aplicações ligadas à virtualização e soluções são disponibilizadas. Isto torna-se rapidamente uma área de evolução com um novo uso de casos a aparecer regularmente, especialmente em conjunto com os dispositivos

móveis como smartphones e tablets.

Hipervisor

Conceito : hipervisor ou monitor de máquina virtual é uma camada entre o software e o hardware e o sistema operativo. Este pode ser definido como um componente de software que pode criar hardware emulado(no que inclui CPU, memória, armazenamento, rede e periféricos, entre outros componentes) para a instalação de um sistema operativo convidado. Este controla o acesso dos sistemas operativos visitantes aos dispositivos de hardware. Este permite que vários sistemas operativos possam ser executados em um mesmo host.

Nota : Sem o hipervisor , mais de um sistema operativo em várias máquinas virtuais poderão querer controlar toda a memória da máquina física. Não só será fatal, como pode resultar num caos total. O hipervisor é importante, pois é responsável por gerir as interações entre a máquina virtual e o hardware.

Tipos de hipervisores :

1. Tipo 1 Bare Metal – software que é executada diretamente sobre o hardware, para fornecer a funcionalidade descrita. Hipervisores conhecidos : Vmware ESXi(grátis), Vmware ESX(software comercial), Xen(código livre), Citrix XenServer(grátis), Microsoft Hyper-V Server;

2. Tipo 2 Hosted – software que é executado sobre um sistema operativo para oferecer a funcionalidade descrita. Hipervisores utilizados: Oracle : VirtualBox, VirtualBox OSE(livre), Vmware Workstation (comercial), server (grátis), Player (grátis), QEMU (livre), oVirt (livre), Microsoft: Virtual PC, Virtual Server;

Semlhança entre o hipervisor bare-metal e hipervisor hosted

O hipervisor do tipo bare-metal interage diretamente com o com o hardware da máquina física. Este é independente do sistema operativo do host. No tipo hosted, o hipervisor é executado por cima do sistema operativo do host, no que torna possível a execução em qualquer tipo de sistema operativo.

Na opção utilizar hipervisor bare-metal ou hosted vai “ter ou não sistema operativo no host”. A primeira opção, pode estar situada diretamente sobre o hardware, conseguindo fornecer um número maior de opções de acesso de entrada e saída (I/O acess), disponibilizando mais desempenho, no caso de se optar por escolher esta arquitetura.

Na segunda opção proporciona maior compatibilidade de hardware, permitindo a execução do software de virtualização em uma gama mais ampla de configurações de hardware, diferentemente do modo bare-metal.

(continue pag 40 book)

Máquinas Virtuais

Conceito : Software responsável por executar sistemas operativos, dando o uso do hardware da máquina física.

Como suporte de armazenamento, o utilizador poderá optar por criar um disco virtual, pois é uma grande valia para armazenar dados proveninetes da máquina virtual.

Memória ram e cpu numa máquina virtual

Como sabemos, as máquinas virtuais são configuradas para serem executadas com um ou mais processadores, dependendo da antecipação no sistema.

Em simples caso, a máquina virtual irá possuir um CPU e , como vimos, se nós examinarmos o hardware proveniente do ponto de vista das máquinas virtuais , nós iremos ver que só irá estar um CPU disponível. Da perspetiva do host, o que foi atribuido foi a abilidade da máquina virtual de “dividir” o CPU em vários ciclos provenientes do host.

Neste caso, o único CPU da máquina virtual pode programar no valor da capacidade de um CPU. O host não reserva unicamente o CPU para o uso em particular da máquina virtual; em vez disso, quando a máquina virtual necessita de recursos de processamento, o hipervisor cumpre esse pedido, isto é, faz a marcação das operações e passa os resultados de volta para a máquina virtual através do driver do dispositivo apropiado para esse efeito.

É importante ter em conta que o host possui mais do que um CPU disponível do que qualuer uma das máquinas virtuais, e isso, o hipervisor é a marcação do tempo sobre os processadores “em nome” da máquina virtual, em vez de uma máquina virtual possuir realmente uma CPU dedicada.

Uma das razões principais para a virtualização em primeiro lugar era tornar mais efeciente o uso dos recursos ao contrário da consolidação, e uma CPU dedicada poderia ser derrotar esse propósito.

Nota: Maioria dos servidores nos dias de hoje possuem mupltiplos *sockets* , e cada desses sockets contém um ou mais cores.

Memória numa máquina virtual

Memória, ou recursos de RAM, é mais simples para entender. Apenas em uma máquina virtual, possuindo recursos de memória sufecientes numa máquina virtual é a diferença entre o sucesso e o falhanço, no que se trata à evolução do desempenho da aplicação. A máquina virtual encontra-se alocada numa quantidade de memória, e

isso é tudo o que se pode utilizar, até mesmo, embora lá pode ser ordens de magnitude e mais memória disponível na máquina física.

Nota: No caso de uma máquina virtual requer mais memória, será possível reconfigurar a quantidade de memória e a máquina virtual irá ter acesso à capacidade adicionada, havendo vezes sem a necessidade de efetuar um reboot.

Recursos de rede numa máquina virtual

Como a parte física, a rede virtual fornece à máquina virtual com uma forma de comunicar com o mundo físico. Cada máquina virtual pode ser configurado com um ou mais cartões de interface de rede ou com placas de rede que representa a conecção a uma rede. No entanto, estas placas de vídeo virtuais não fazem a conecção com as placas de rede físicas. O hipervisor oferece suporte à criação de uma rede virtual que se conecta à placa de rede física que é composta por switches virtuais.

Esta rede virtual também é uma ferramenta vital na criação de ambientes de trabalho seguras para as máquinas virtuais que partilha um host. No ponto de vista, no que toca á segurança, as comunicações máquina-para-máquina pode acontecer através do switch virtual e nunca deixa o host físico. Se a placa de rede virtual de uma segunda máquina virtual conecta ao switch virtual, e se esse switch não estiver conectado à placa de rede física, a única manetira de comunicar com essa máquina virtual, é através da primeira máquina virtual, elaborando um *"buffer"* entre o mundo exterior e essa máquina virtual. Se nesta estiver uma terceira máquina virtual na imagem, pelo menos que foi conectado no mesmo switch virtual, também não haveria nenhuma maneira de aceder à máquina virtual protegida.

Armazenamento numa máquina virtual

Como sabemos, os servidores virtuais necessitam de armazenamento para trabalhar, como os recursos que vimos , o que obtem apresentado para uma máquina e o que uma máquina virtual acredite que está a ver.

Funcionamento de uma máquina virtual

O hipervisor torna-se o transporte e regulador dos recursos e dos “hospedes” virtuais que suporta. Isto atinge a capacidade de “enganar” o utilizador Convidado fazendo-o a acreditar que este hipervisor é na verdade hardware. Quando um programa necessita de dados de um ficheiro ou disco, este faz um pedido através de um comando de uma linguagem de programação, como fgets() em C, que é passado através do sistema operativo. O sistema operativo contém um ficheiro que corresponde à informação do sistema disponível. Este acaba por enviar o pedido para o gestor de dispositivos, que funciona com o disco físico de armazenamento e com o controlador de I/O para recuperar os dados necessários.

A data volta para trás através do controlador I/O e do driver dos dispositivos onde o sistema operativo retorna os dados do programa pedido. Não só os blocos de dados que são solicitados como também o bloco de memória, as marcações de CPU e recursos de rede. AO mesmo tempo, outros programas elaboram pedidos adicionais, dependendo do sistema operativo para manter todas as ligações em linha reta.

As medidas de segurança são elaboradas na arquitetura x86 sozinhas. A implementação destas medidas serve para prevenir de acidentes e de sistemas maliciosos que cujo o nome é *"co-opting"* ou de aplicações corrompidas ou sistema operativo.

A arquitetura x86 fornece proteção sob a forma de quatro níveis , na qual, os comandos do processador podem ser executados. Estes níveis são referidas como anéis (no termo americano *rings*).

Níveis de proteção (composta por anéis/ *rinngs*):

- Ring 0/ Anel 0 – é o anel mais privilegiado , onde o sistema operativo kernel trabalha;

- Ring 1/ Anel 1 e Ring 2/Anel 2 – anel onde os drivers dos dispositivos são executados;

- Ring 3 / Anel 3 - o utltimo anel confiável onde as aplicações são executadas.

Na prática, o anel 1 e 2 são raramente utilizados. As aplicações não podem executar sozinhos as instruções do processador diretamente. Estes pedidos são passados através de níveis via chamadas efetuadas pelo sistema, onde estes são executados por parte da aplicação, como num exemplo simplificado, ou estes poderão lançar um erro devido ao fato de que o pedido poderia ter violado uma restrição.

Caso um programa do sistema pretender afetar algum estado do hardware, este fá-lo executando instruções privilegiadas no anel 0. Um

pedido de encerramento poderia ser um exemplo disto.

Um hipervisor executa no anel 0, e os sistemas operativos nos convidados “acreditam” que é possível serem executados no anel 0. Se o convidado pretender encerrar, o hipervisor intercepta o pedido e responde ao convidado, indicando que esse encerramento é o processo para que o sistema operativo proceda ao encerramento do software. Se o hipervisor não “isolar” este comando, qualquer convidado irá afetar os recursos e o ambiente de todos os convidados no host, o que poderá desencadear uma violação da isolação da regra de definição de Popek e Goldberg, não mencionando as dificuldades que pode desencadear.

Como o sistema operativo nativo que gere os pedidos de programas em execução para os recursos, o hipervisor abstrai de uma camada e gere multiplos pedidos de recursos por parte dos sistemas operativos.

Máquinas virtuais

As máquinas virtuais existem como duas entidades físicas: os ficheiros que fazem a configuração das máquinas virtuais e a instalação da memória que faz com que uma máquina virtual possa ser executada quando inicializada.

Em outras formas, trabalhando com uma máquina virtual é semelhante ao trabalhar num servidor físico. Como um servidor físico, podemos interagir com este através de um tipo de conecção de rede para carregar, gerir, e monitorizar o ambiente ou várias aplicações que este suporta. Também como um servidor físico, é possível alterarmos a configuração de hardware, adicionando ou diminuindo a capacidade, através de métodos para elabrorar e a flexibilidade para elaborar o que são muitos diferentes entre um servidor físico e um servidor virtual.

Desde da origem do computador, os ficheiros foram um método de armazenamento da informação. Devido a essa história e conhecimento, gerir ficheiros é uma rotina. Se alguém necessecita de elaborar um backup a um documento, esta faz uma cópia, movendo-a de seguida para um outro dispositivo para arquivar.

Clones de máquinas virtuais

Provisionamento do servidor usa consideravelmente recursos no que toca aos termos do tempo, trabalho humano e dinheiro. Antes da virtualização do servidor, o processo de ordenar e adquirir um servidor físico pode demorar semanas, ou meses em certas empresas/organizações, não mencionando o custo, que por vezes, poderá ser de milhares de dólares. Uma vez que o servidor chega físicamente, provisionamento do tempo é requerido. Um administrador do servidor poderá necessitar para executar uma ampla lista de tarefas, incluindo carregar um sistema operativo, carregar qualquer outros patches que o sistema operativo necessita para se manter atualizado, configurar o armazenamento adicional, instalar as ferramentas corporativas e as aplicações decididas pela organização/empresa, com o objetivo de gerir a própia infraestrutura. Após isso, o servidor poderá ser entrgue a uma equipa responsável por desenvolver a aplicação destinada, com o objetivo de instalar e configurar esta que poderá ser

executada no servidor. O provisionamento do tempo adicional poderá ser dias, ou mais, dependendo da complexidade do que é necessário para ser instalado e o que mecanismos organizacionais estão no local para completar o processo.

Caso necessitamos de um novo servidor, é possível criarmos um clone (réplica) de um servidor existente. Este processo involve uma pequena cópia dos ficheiros que compoem o servidor existente. Uma vez que essa cópia existe, o sistema operativo nativo necessita de alguma personalização soba forma de um unico sistema de informação, como o nome do sistema, o enderesso de IP, antes de ser instanciado. Sem essas alterações, acabariamos por ter duas máquinas virtuais com a mesma identidade que poderiam ocupar o espaço dedicado à rede e à aplicação, e isso poderia causar estragos em muitos níveis. Ferramentas que gerenciam as máquinas virtuais possuem disposições (em falta: provisões) elaboradas para contribuir com as personalizações durante o processo de clonagem (replicação), que poderá contribuir para o esforço real em si, sem um numero de cliques no rato.

Templates

À semlhança dos clones, os templates das máquinas virtuais são outro mecanismo que contribui para a entrga rápida dos servidores virtuais já configurados. Um template é uma espécie de molde, pre-configurado recarregado presente na máquina virtual, que é usado para terminar com as cópias utilizadas no servidor. A diferença entre um template e um clone é que o clone está a ser executado enquanto que um template não. Em muitos ambientes, um template não pode ser executado, e para se fazer alterações (adicionando patches, por exemplo), este deverá ser convertido de volta para a máquina virtual. Seria após esse procedimento que começaria a máquina virtual, ou seja, deveriamos aplicar os patches necessários, desligar a máquina virtual, e então, converter a máquina virtual de volta para o template. Como clonando, criando a máquina virtual a partir de um template também requer uma única identidade para ser aplicada na nova máquina virtual.

Os templates são usados apenas para entrega de máquinas virtuais “vazias”, servidores que são compostos da máquina virtual que são configuradas. Estes são configurados com um sistema instalado. Estes podem fazer a entrega de máquinas virtuais que possuem aplicações instaladas. Estes são também configurados. Quando os utilizadores

necessitam dos programas para serem carregados, a máquina criada a partir de um template pré-ccontruído, poderá entregar essa aplicação ou um conjunto de aplicações para os utilizadores utilizarem imediatamente.

Snapshots (capturas de ecrã)

Sanpshots (capturas de ecrã) são muito mais do que eles parecem, ou seja, parece que faz uma captura de ecrã do estado (state) da máquina virtual.Caso haja uma alteração na máquina virtual, e que haja problemas nessa, estes possibilitam-nos retornar para a parte salvada. Uma snapshot preserva o estado de uma máquina virtual, a data deste e as configuração de hardware desta. Uma vez que nós damos o snapshot numa máquina virtual, as alterações feitas não irão diretamente para a máquina virtual. Em vez disso, irão ser armazenadas num disco *delta,* havendo vezes que é denominado por disco “filho”. Este dico delta ou disco “filho” acumula todas as alterações até uma ou duas.

Por último, nós podem os reverter de volta o estado de uma máquina virtual quando se tira um snapshot, “desenrolando” todas as alterações que foram feitas nesse tempo.

Os snapshots são muito úteis em teste e em áreas de desenvolvimento, permitindo aos desenvolvedores tentar arriscadamente processos desconhecidos com a habilidade de restaurar o ambiente para um estado “saudável”. Os snapshots poderão ser usados para testar um patch ou uma atualização onde o resultado é incerto, pois, estes fornecem uma forma de desfazer o que foi aplicado.

Nota: Os snapshots não são substitutos de backups adquados.

OVF

Uma outra forma de “empacotar” e de distribuir máquinas virtuais é utilizando o OVF (Open Virtualization Format). OVF consiste num padrão elaborado por uma toda a indústria, que consiste num grupo de pessoas que representam os fornecedores nas diversas áreas da virtualização. A finalidade deste padrão é criar uma plantaforma e um formato neutro de fornecedor para as máquinas que podem ser “transportadas” da plantaforma de virtualização de um lado para o outro.

O padrão OVF suporta dois diferentes métodos para “empacotar” máquinas virtuais. O template OVF cria um número de ficheiros que representam a máquina virtual, pois esta é composta por uma série de ficheiros. O modelo OVF também possui um segundo formato, OVA, que irá encapsular toda a informação num unico ficheiro.