VIRTUALIZAÇÃO
VIRTUALIZAÇÃO E SEGURANÇA

Autor: Me. Ricardo César Ribeiro Dos Santos
Revisor: Luciana de Castro Lugli

INICIAR

introdução

Introdução

Segurança da informação é um assunto bastante discutido atualmente, com usuários cada vez mais conscientes da ação de cibercriminosos, que podem obter de maneira ilegítima seus dados. Dessa forma, os provedores de serviços se veem cada vez mais pressionados a manter seus recursos atualizados e seus clientes informados sobre as medidas de proteção tomadas. Nesse sentido, a segurança no ambiente virtualizado é vital, já que um papel importante da virtualização é a criação de servidores para a utilização em ambientes de rede.

Nesta unidade, será detalhado como implementar as boas práticas de segurança em virtualização, com ênfase em criar uma plataforma de rede que dê suporte à criação de um ambiente de servidores. Conhecer essa plataforma não só detalha a forma de criação de serviços que pode ser utilizado por clientes e empresas, mas garante que o profissional tenha capacidade de especificar a segurança que espera para suas aplicações também.

Plataforma como um Serviço (PaaS - Platform as a Service)

O paradigma de PaaS (*Platform as a Service*) denomina um ambiente que possua amplo acesso à rede a uma plataforma com *pooling* de recursos, em que o próprio usuário possa escalar o seu ambiente conforme a necessidade de maneira mais automatizada possível, pagando somente o que utilizar. Essa definição foi elaborada pelo NIST (MELL; GRANCE, 2011) e é interessante notar que, apesar de não restringir quais softwares ou serviços que podem ser prestados para o usuário, define três modelos de serviço:

No Local - Quando o cliente escolhe por gerenciar o sistema localmente, se torna responsável pela manutenção de hardware e de software do ambiente completo, mas tem a liberdade total de configurações de rede, armazenamento, servidores, sistemas operacionais e aplicativos do ambiente.

> *1. Software as a Service (SaaS) - o provedor de serviço oferece aplicações executando em uma infraestrutura em nuvem que podem ser acessíveis através de navegadores de internet, thin clients ou programas específicos. Neste modelo o cliente não tem controle ou gerência sobre a infraestrutura da nuvem [...], com a possível exceção de configurações da aplicação executada.*

2. Platform as a Service (PaaS) - neste modelo, o provedor de serviços oferece a capacidade de instalar na nuvem aplicações do cliente. As configurações do ambiente de infraestrutura não estão acessíveis ao cliente, que detém o controle das aplicações e das configurações do ambiente em que a aplicação está executando.
3. Infrastructure as a Service (IaaS) - O cliente pode provisionar processamento, rede, armazenamento e outros recursos computacionais fundamentais, em que pode executar quaisquer softwares [...]. O cliente administra as informações do armazenamento, mas não o hardware de armazenamento em si. (MELL; GRANCE, 2011, p. 2, tradução nossa).

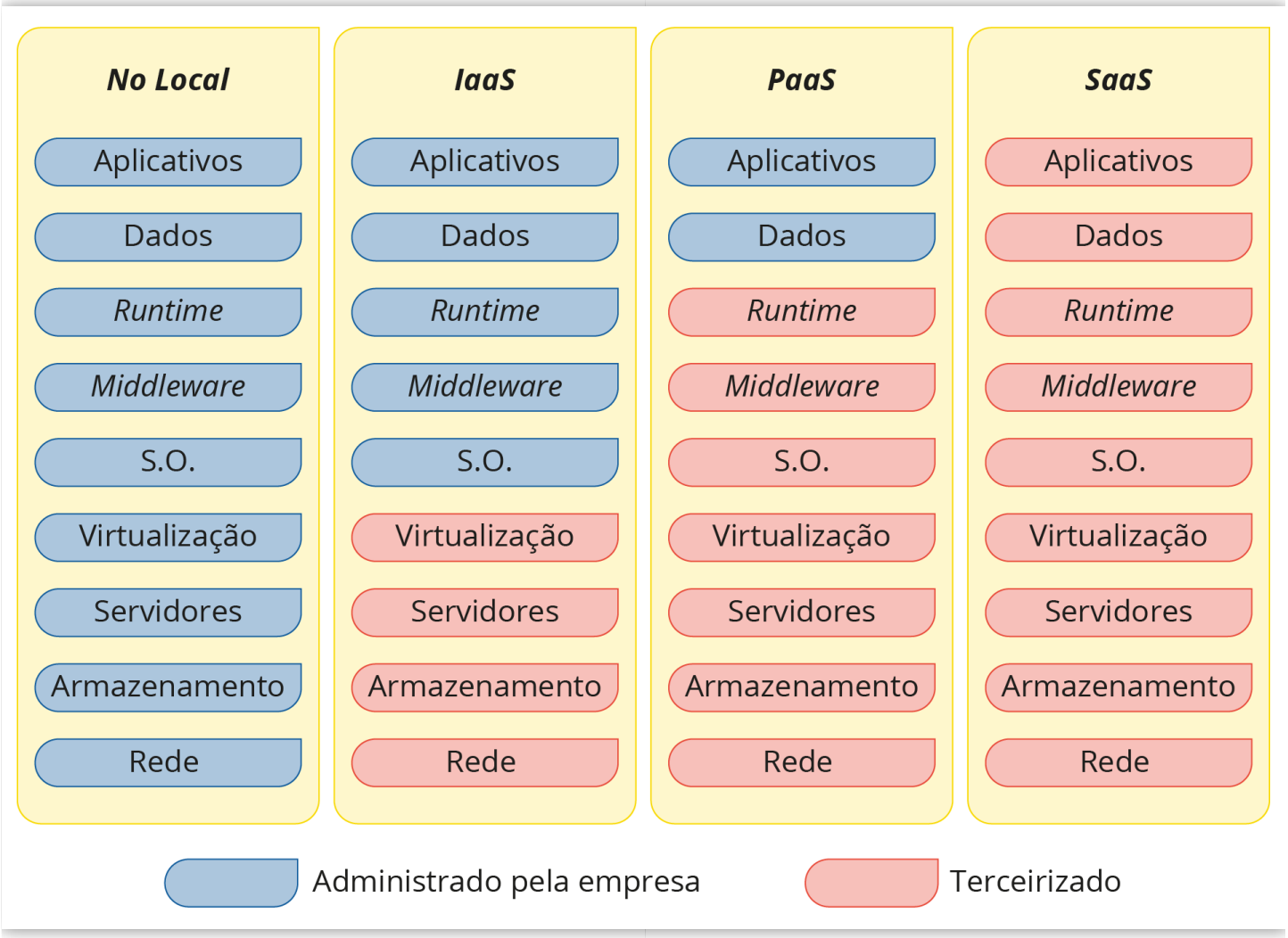


Figura 2.1 - Comparação entre os modelos de negócio de Cloud Computing
Fonte: Adaptada de Watts e Raza (2019, tradução nossa).

O modelo de Plataforma como um Serviço - PaaS prevê uma plataforma sobre a qual desenvolvedores podem criar suas aplicações sem ser responsáveis por dar manutenção ao software de banco de dados, ao sistema operacional

sobre o qual a plataforma executa ou até mesmo à infraestrutura de rede. Esses serviços são possíveis somente através da implantação de uma plataforma completa, instalada sobre um sistema operacional apropriado.

Inclusive, é necessário notar que a base para esse tipo de serviço é realizada pelos mesmos equipamentos que os presentes no modelo de Infraestrutura como um Serviço. Esse fato se dá por conta da necessidade de que os equipamentos da plataforma devem ser atendidos pela infraestrutura de rede, que é o produto do modelo IaaS.

Inicialmente, dar o controle da infraestrutura sobre a qual o ambiente executa pode parecer um contrassenso do ponto de vista estratégico. Quando se idealiza um serviço, pode se pensar em criar o ambiente inteiro, de forma a não ter que dividir a infraestrutura com outros clientes de um serviço de computação em nuvem ou permitir que seus dados fiquem armazenados em servidores externos à empresa. Esse raciocínio, porém, pode se refletir em custos de negócio.

Uma boa prática de gerência de ambientes de rede é manter um serviço por servidor - caso um servidor seja comprometido, não mais que um serviço será afetado. Em uma plataforma de desenvolvimento web, por exemplo, temos, no mínimo, dois serviços: o servidor web e o servidor de banco e dados. Pensando no *framework* “um serviço, um servidor”, já temos duas máquinas para administrar ao invés de uma, aumentando o trabalho e custos operacionais.

Em seguida, vamos pensar no ciclo de vida de um serviço web qualquer. É comum que esses serviços iniciem de forma pequena e vão aumentando de porte de acordo com as necessidades e com o tempo (isso, claro, se tiverem sucesso). Esse comportamento reflete no tipo de equipamentos e plataforma que são necessários.

É comum desenvolvedores com serviços pequenos optarem por hospedar seus sistemas em um servidor web compartilhado a fim de otimizar o uso do *hardware* . Ou seja, um servidor que atende a mais de uma aplicação ao mesmo tempo, dividindo a capacidade de processamento entre vários clientes

que tenham aplicações com necessidades de processamento suficiente baixas.

Entretanto, à medida que as necessidades do sistema vão aumentando, também aumenta o consumo de recursos da plataforma. Como todos os processos de uma mesma plataforma compartilham os mesmos recursos, o desempenho de uma aplicação pode ser afetado caso outra utilize mais recursos que o esperado - um sistema pode exigir muito de armazenamento, por exemplo, criando um gargalo para todos os outros clientes utilizando a mesma infraestrutura.

Quando se depara com tal desafio, o desenvolvedor pode sentir que a solução é criar um parque de informática para si, em que tenha controle absoluto de todos os aspectos operacionais. Porém, ao fazer isso, se torna responsável por toda a manutenção de hardware e software, o que pode elevar os custos operacionais da empresa e algumas vezes até torná-la inviável.

Na tentativa de achar um meio termo (um sistema seguro e compartilhado que mantenha os custos baixos, otimize o uso de hardware e não seja gerenciado pela própria empresa), criou-se o conceito de PaaS, ou *Platform as a Service* .

Nesse contexto, cada usuário tem os servidores virtualizados que realizam as funções necessárias, mantendo os requisitos de segurança para os serviços e mantendo a estrutura escalável de maneira automatizada.

Para que possamos entender melhor este tipo de serviço, vamos voltar para o final da unidade passada, em que tratamos de Amazon AWS. Uma das características do AWS é exatamente a capacidade de escalar de maneira transparente, de acordo com a necessidade. Essa capacidade vem da possibilidade de executar uma máquina virtual sobre um sistema distribuído que pode englobar regiões geográficas distantes.

Como os servidores virtuais são criados para o cliente, ele tem privilégios de administração da infraestrutura como se fosse o proprietário do sistema. Esse controle total que o cliente tem sobre os servidores virtuais permite que os serviços sejam configurados de acordo com a necessidade. Caso o cliente

sinta necessidade de mais serviços, ou ache que não precisa mais de algum, é possível que seja requisitado que este seja retirado da sua cesta de produtos.

Por outro lado, o custo operacional e de manutenção das máquinas pode ser dividido entre vários outros desenvolvedores, mantendo os valores baixos. Essa manutenção engloba a disponibilidade e a estabilidade do serviço, *software* e *hardware* . Ou seja, o desenvolvedor não precisa se preocupar com a infraestrutura dos servidores, somente com os dados que estão presentes nele.

praticar

Vamos Praticar

A maioria das soluções SaaS provêm uma oportunidade de utilizar *software* ou uma plataforma sobre a qual uma aplicação pode ser desenvolvida ou entregue. Um ambiente de *software-as-a-service* não fornecerá o ambiente necessário para projetar, desenvolver e testar a aplicação. A maioria dos ambientes *storage-as-a-service* somente se foca nas necessidades de um dos componentes de armazenamento da empresa, seja em backups, armazenamento de arquivos ou colaboração.

ART OF SERVICE. **Cloud Computing Certification Kit** : Specialist: Platform Management & Storage Management. Londres: The Art of Service, 2009. p. 20. Tradução própria.

Com relação ao ambiente PaaS, é correto afirmar que:

- **a)** O ambiente PaaS oferece uma alternativa para se utilizar *softwares* , o provedor de serviço detém licenças que é capaz de locar por tempo determinado.

- **b)** No modelo PaaS, a empresa não deve escalar o ambiente do cliente. O cliente deve providenciar novos contratos com a empresa.
- **c)** O ambiente PaaS fornece um sistema para clientes que não têm disponibilidade ou expertise em administrar a infraestrutura subjacente.
- **d)** O ambiente PaaS oferece ao cliente a terceirização da infraestrutura de rede, serviços devem ser implementados pelo cliente.
- **e)** Apesar de PaaS ser um conceito interessante, não é relevante para o assunto de virtualização, uma vez que a criação desse serviço não depende de virtualização.

Modelos de Máquinas Virtuais

Uma das classificações comuns em virtualização é com relação ao tipo de hypervisor em que o sistema virtualizado executa; os hypervisores Tipo 1 e Tipo 2 são respectivamente denominados *bare-metal* e hospedado. Nesse caso, o primeiro não necessita de sistema operacional, enquanto o segundo se comporta como um software executando no computador hospedeiro.

Virtualização Total

A técnica de virtualização total cria um ambiente virtual em que a máquina virtual recebe através do Hypervisor uma cópia exata do *hardware* em que o ambiente está instalado. Dessa forma, não só o sistema operacional hóspede não precisa ser modificado para a virtualização, como também não precisa receber informação nenhuma sobre estar ou não executando em uma máquina virtual.

Porém, a facilidade de executar o sistema operacional sem modificações vem com a necessidade do hypervisor implementar uma interface virtual que simula o *hardware* real do computador. Considerando-se a variedade de

dispositivos existentes no mercado, é efetivamente impossível que todos os casos sejam previstos a *priori* .

Para mitigar essa complexidade, os desenvolvedores de hypervisores implementam dispositivos virtuais padrão, que podem ser acessados pelo dispositivo virtual. Esses dispositivos, entretanto, são genéricos e podem não implementar as funcionalidades que os dispositivos reais oferecem.

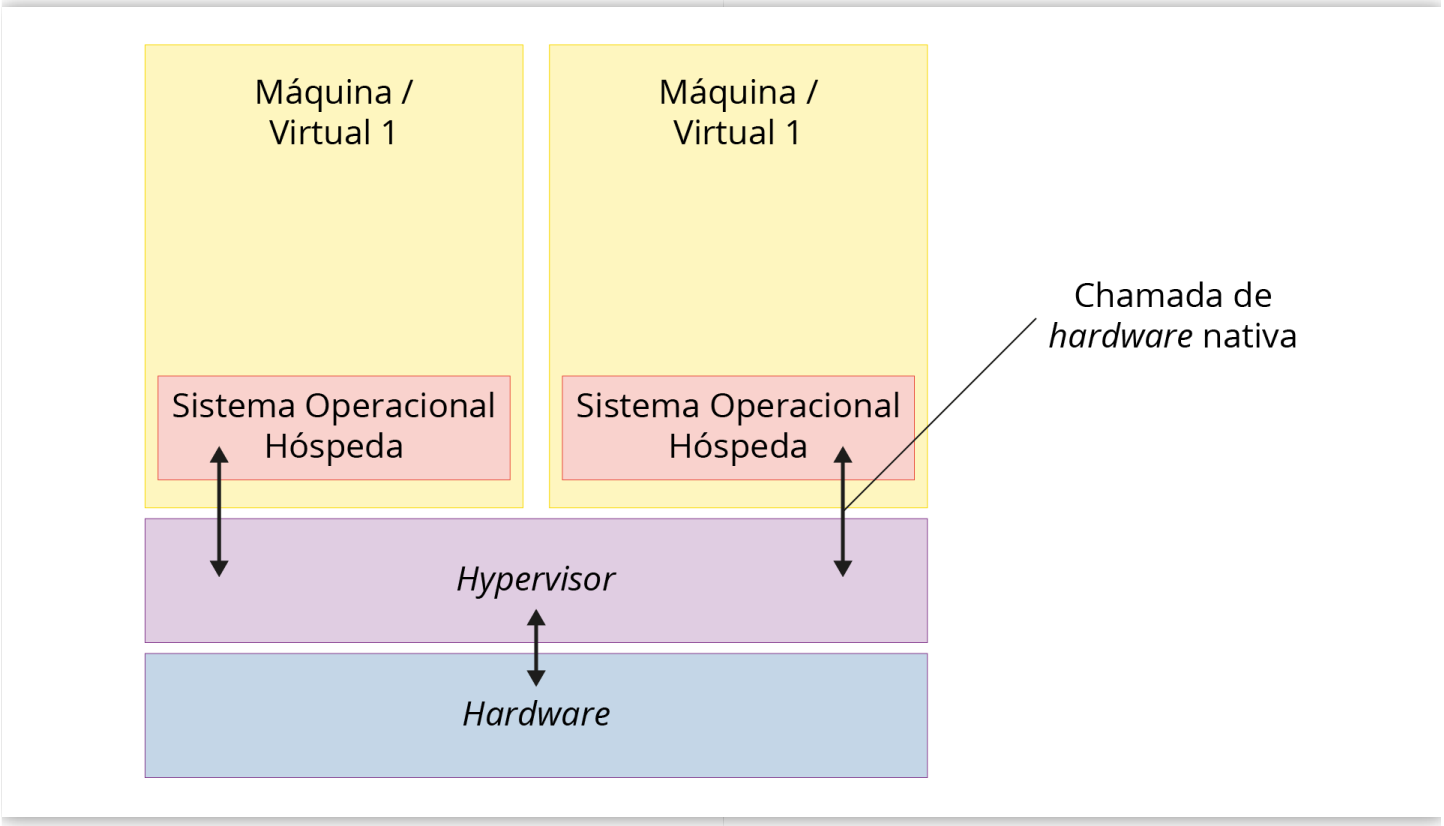


Figura 2.2 - Diagrama mostrando a troca de mensagens em Virtualização Total
Fonte: Adaptada de Carissimi (2008).

Paravirtualização

Para tratar os gargalos de processamento que foram discutidos anteriormente, foi desenvolvida a técnica de paravirtualização, em que a principal diferença é que o sistema operacional sabe que está rodando em uma máquina virtual e realiza as operações de acordo com o necessário.

Nessa técnica, o sistema operacional hóspede faz a chamada ao hypervisor

quando precisaria acessar o *hardware* do sistema, como no modelo anterior. A grande diferença é que nesse modelo o hypervisor tem os drivers do sistema instalados em si.

Nota-se que esta chamada de hardware para um driver instalado no hypervisor não se confunde com outras mensagens trocadas entre o sistema operacional hóspede e o hypervisor.

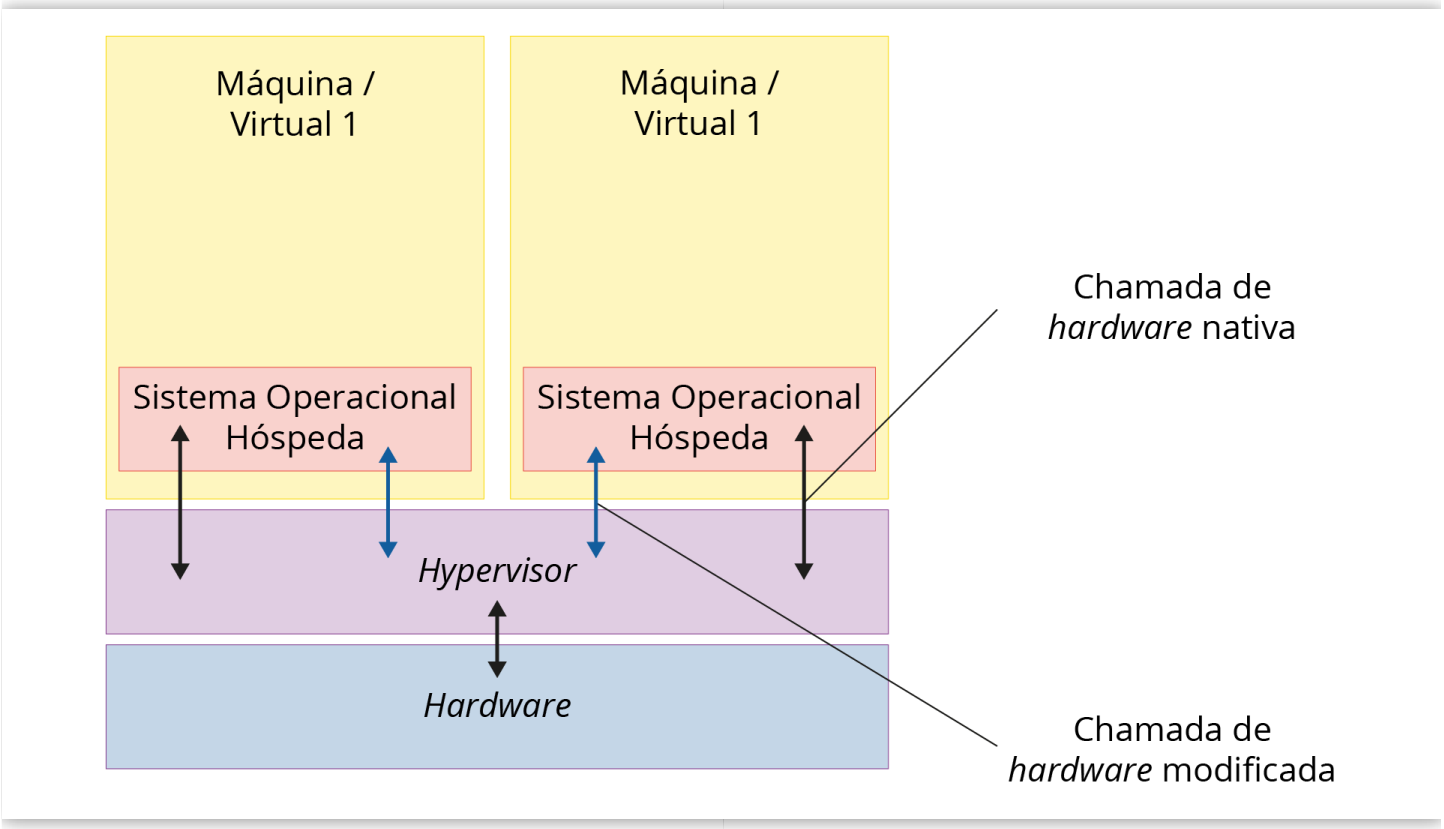


Figura 2.3 - Diagrama mostrando a troca de mensagens em Paravirtualização
Fonte: Adaptada de Carissimi (2008).

Para o usuário, é difícil pensar em aplicativos de paravirtualização como virtualização. Normalmente, imagina-se como sendo uma camada de compatibilidade entre sistemas operacionais ou uma forma de adaptar softwares entre plataformas. Isso é sinal que essa forma de virtualização é mais transparente para o usuário, uma vez que ele percebe o processo como inicializar um terminal de um sistema operacional em outro.

saiba mais

Saiba mais

Normalmente, quando se pensa em virtualização, vem à mente o modelo de Virtualização Total, em que um sistema operacional é instalado sobre um hypervisor e que executa da mesma forma que executaria em um *hardware* dedicado. Ou seja, um contexto em que a virtualização é transparente para o sistema operacional da máquina virtual.

Porém, as aplicações de Paravirtualização possuem recursos que são bastante interessantes e úteis nos mais variados contextos. Dois exemplos da aplicação dessas tecnologias são o Bochs e o QEMU. Ambos são emuladores de linha de comando que podem atender usuários que desejem emular sistemas operacionais Linux, DOS e Windows 95/98/XP/2000/NT.

Fonte: Jones (2007, *on-line*).

ACESSAR

Ao sentir a necessidade de utilizar somente softwares específicos ao invés de um sistema completo, convém ter em mente a utilização de plataformas de paravirtualização, devido às características dessa técnica. Não existem apenas diferenças em relação ao overhead das chamadas de funções do sistema, mas uma plataforma de paravirtualização dispensa a necessidade de se inicializar um novo ambiente inteiro com sistema operacional somente para utilizar softwares isolados.

praticar

Vamos Praticar

“Primeiro, dada a diversidade de dispositivos existentes que compõem um computador, é muito difícil implementar uma máquina virtual que imite o comportamento exato de cada tipo de dispositivo. A solução consiste em prover na VMM suporte a um conjunto genérico de dispositivos. [...] Sendo assim, pode-se ter uma subutilização de um recurso de hardware real. Segundo, por não ser modificado, as instruções executadas pelo sistema hóspede devem ser testadas na VMM para saber se elas são sensíveis ou não, o que representa um custo de processamento. Terceiro, a implementação de VMM com virtualização total deve contornar alguns problemas técnicos devido à forma que os sistemas operacionais são implementados” (CARISSIMI, 2008, *on-line*).

CARISSIMI, A. Virtualização: da teoria a soluções. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS, 26., 26 a 30 maio 2008, Rio de Janeiro. **Anais [...]** . Rio de Janeiro: SBC, 26 a 30 maio 2008. Disponível em: http://hostel.ufabc.edu.br/~marcelo.nascimento/BC1518Q3/arquivos/virtualizacao_cap4-v2.pdf . Acesso em: 11 dez. 2019.

Com relação à paravirtualização e à virtualização total é correto afirmar que:

- **a)** A paravirtualização somente virtualiza alguns dos componentes de uma máquina, na virtualização total, a máquina virtual é capaz de realizar todas as funções de uma máquina real.
- **b)** Na paravirtualização, o sistema hospedeiro sabe que está rodando em uma máquina virtual, enquanto na virtualização total ele não tem essa informação.
- **c)** Um ambiente virtual com virtualização total utiliza os drivers do hypervisor, uma vez que ele sabe que está rodando em uma máquina virtual.

- **d)** Nas duas alternativas o custo computacional da virtualização não é desconsiderável. Porém, no caso da paravirtualização, os custos são maiores.
- **e)** A paravirtualização não pode ser utilizada se existirem drivers modificados no sistema operacional hospedado.

Segurança de Virtualização

Para que o conceito “um serviço, um servidor” seja funcional, é necessário garantir a segurança do modelo, através de uma plataforma que traga comodidade nas aplicações e facilidade de manutenção. Porém, ainda é necessário discutir a segurança em si e como pode ser implementada através de virtualização para proteger os servidores da aplicação de ataques provenientes de usuários maliciosos.

Porém, no ambiente virtual, não é somente no contexto de redes que existe o aumento de segurança. Em um nível mais abstrato, pode-se considerar que, como o sistema necessita de um administrador, todos os dados serão geridos de maneira profissional, não por um usuário sem experiência em segurança de sistemas.

Aliado ao backup periódico que um gerente de sistemas deve realizar, existe ainda a possibilidade de se instalar um antimalware no hypervisor (no caso do Hypervisor Tipo 1) ou no sistema operacional hospedeiro (no caso do Hypervisor Tipo 2). Dessa forma, é possível controlar a segurança da máquina virtual em um único ponto centralizado que pode ser gerenciado também de maneira centralizada.

Porém, essas formas de se assegurar as máquinas virtuais não são únicas, sendo possível utilizar mecanismos para a criação de pontos de segurança para redes de servidores virtuais e impedir o ataque de usuários maliciosos à estrutura de rede que se forma no data center.

Mas, antes de entrarmos no cenário virtualizado, é necessário pensarmos em uma rede de computadores e como um usuário malicioso pode tentar explorar as fraquezas do sistema e tentar ganhar controle das máquinas lá presentes.

A principal defesa de uma rede de computadores é o *firewall* , que atua como um filtro do tráfego que entra e sai de uma rede. Esse tipo de equipamento é responsável por realizar o controle das portas e endereços de rede que estão acessíveis para acesso externo e são programados utilizando um conjunto de regras que podem definir o acesso a uma rede. Originalmente, um firewall é colocado logo após o roteador que conecta a rede à internet, conforme ilustrado na figura 2.4:

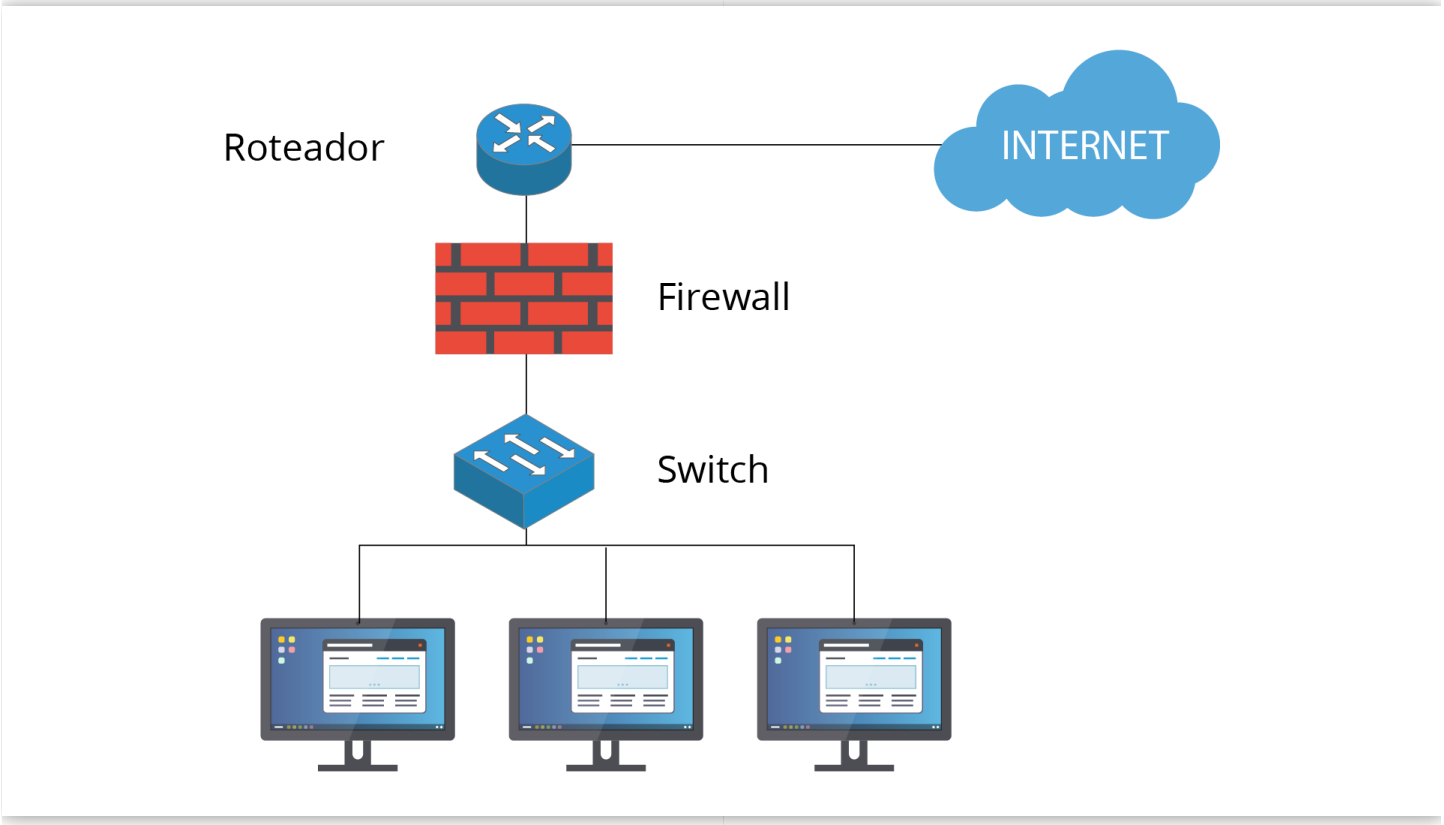


Figura 2.4 - Arquitetura de rede com firewall
Fonte: Adaptada de Nonan e Dubrawsky (2006).

Essa arquitetura da rede permite que o *firewall* proteja a rede contra-ataques

externos, uma vez que os hosts da rede estão protegidos. É importante lembrar que esses *hosts* não são somente estações de trabalho, mas são servidores de aplicação dentro da infraestrutura de uma rede.

Esse equipamento de segurança tem duas ou mais interfaces de rede, uma para a rede externa e outra para a rede interna. O tráfego de rede, então, obrigatoriamente passa entre essas interfaces e é filtrado conforme as regras definidas pelo administrador de rede. Essa topologia é importante de ser observada, uma vez que pode ser transposta para o contexto virtualizada de maneira quase direta, como demonstra a figura a seguir.

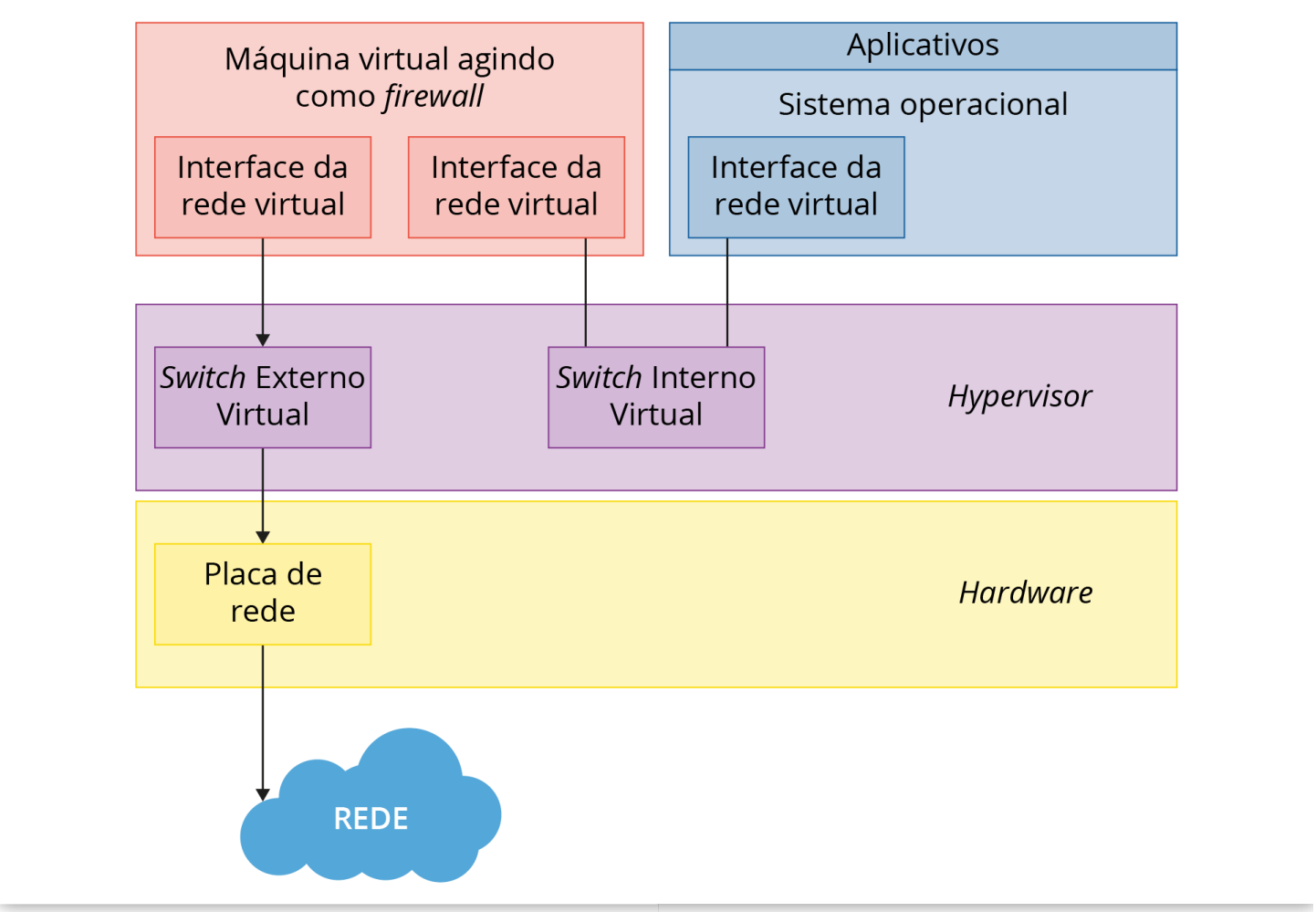


Figura 2.5 - Arquitetura de rede com firewall
Fonte: Elaborada pelo autor.

A vantagem em relação à outra arquitetura é que a infraestrutura de rede é toda virtual, sem a necessidade de equipamentos de rede externos à planta. Note que o *switch* que interliga os hosts que são responsáveis por prover serviços também é virtual e é um componente do hypervisor. Como não há

acesso externo ao ambiente virtualizado, evitam-se ataques que visam o *hardware* dos ativos de rede de uma infraestrutura.

reflita

Reflita

Durante o texto foram mencionados os benefícios que as técnicas de virtualização trazem para a segurança dos dados para os provedores de serviço e para os clientes. Porém, as boas práticas de segurança ainda são necessárias, uma vez que o fator humano é um dos fatores determinantes para as faltas nas empresas.

Uma das principais preocupações atuais gira em torno da privacidade de dados de terceiros e quão confiáveis são os repositórios dessas informações na nuvem. O assunto afeta tanto aos provedores de serviço, que devem lidar com as desconfianças dos clientes, quanto aos clientes, que devem lidar com questões sobre quão confiáveis são os servidores.

Para que esse assunto seja tratado da forma mais eficiente possível, é necessário que práticas de governança sejam aplicadas e que os clientes sejam informados e estejam de acordo com as mesmas.

Fonte: Zanutto (s.d.).

Esta forma de acesso remoto à máquina virtual é a que deve ser utilizada para a criação de servidores virtuais em data centers, em que o firewall define o limite da zona desmilitarizada, que é o local considerado seguro. Normalmente é a parcela de equipamentos que está depois dos dispositivos de segurança da rede e é vista como uma área de comunicação mais confiável que nas redes em geral.

praticar

Vamos Praticar

“Quando a maioria das pessoas pensa em um *firewall* , pensam em dispositivo que está conectado na rede e que controla o tráfego que passa entre segmentos da rede [...]. Entretanto, *firewalls* podem ser implementados em um sistema, [...] sendo conhecidos no caso como *firewalls* baseados em *host* . Essencialmente, os dois tipos de firewall têm o mesmo objetivo: prover um método de assegurar as diretrizes de controle de acesso” (NONAN; DUBRAWSKY, 2006, p. 5, tradução própria).

NONAN, W.; DUBRAWSKY. **Firewall Fundamentals** . 1 ed. Indianapolis: Cisco Press, 2006.

Com relação à segurança em servidores virtuais é **correto** afirmar que:

- **a)** As máquinas virtuais não devem ser capazes de se comunicar com o ambiente externo. Por essa razão, *Cloud Computing* é considerado mais seguro.
- **b)** Um firewall não pode ser virtualizado. Dessa forma, mesmo em um sistema virtualizado, é necessário utilizar um equipamento dedicado que executa de maneira standalone.
- **c)** Apesar de ser possível executar o *firewall* em uma máquina virtual, não é recomendável. É necessário que essa função seja executada por um *firewall* por *hardware* .
- **d)** Ao utilizar a virtualização, é possível ter um sistema de *firewall* integrado às demais máquinas virtuais, utilizando conexões de rede virtualizadas. Dessa forma, um único hardware pode desempenhar as funções de rede correspondentes a segurança e serviços.

- **e)** Um *firewall* virtual é restrito somente aos serviços rodando na mesma máquina. Assim, outras plataformas devem implementar seus próprios sistemas de *firewall* .

Portabilidade em Virtualização

Como você já deve ter notado, uma das aplicações da virtualização é a possibilidade de dissociar os ambientes de *hardware* e *software* através do hypervisor. Ou seja, dada uma máquina virtual que esteja executando sobre um hypervisor é possível portá-la para outro hypervisor com pouco esforço de migração.

Isso significa, por exemplo, que para fazer o upgrade de hardware em um ambiente virtualizado é necessário copiar a máquina virtual e transferir para o novo hardware hospedeiro. Após essa operação, considerando que a nova máquina atenda aos pré-requisitos, todas as configurações, arquivos e *softwares* estarão executando do mesmo jeito no novo ambiente.

Uma máquina virtual nada mais é do que um ou mais arquivos de dados que descrevem o comportamento da máquina bem como contêm o disco rígido dessa máquina virtual com sistema operacional, arquivos de usuário, configurações da máquina etc.

Clonagem de Máquinas Virtuais

O processo mais simples para realizar a cópia de uma máquina virtual é a clonagem. Nesse método é realizada a cópia dos arquivos da máquina virtual e transfere-se estes para outro ambiente, caso seja o desejado, ou, ainda, é possível guardar os dados em um backup para caso seja necessário restaurar o sistema virtual para algum outro estado.

Esse procedimento é útil para a criação de cópias de segurança em ambientes virtualizados. Caso um ambiente sofra algum tipo de revés, o administrador do sistema pode restaurar uma versão antiga da máquina virtual utilizando cópias de backup.

Para o administrador do sistema também é cômoda essa abordagem. Caso seja necessário realizar alguma manutenção no sistema hospedeiro, é possível realizar o backup das máquinas virtuais que estejam executando sobre determinada plataforma e, posteriormente, restaurar o funcionamento do sistema.

Apesar de ser a forma mais simples de realizar o serviço, a clonagem de máquinas virtuais ainda tem suas limitações. A principal é a dificuldade de escalar esse procedimento para várias instâncias. Realizar o backup de uma quantidade pequena de máquinas virtuais pode não representar um investimento grande de horas de trabalho, mas quando começa a se considerar que podem existir centenas ou milhares de máquinas executando no mesmo hospedeiro e que podem precisar ser copiadas, essa tarefa pode se tornar inviável.

É importante verificar, antes de iniciar o processo, quais as limitações do hypervisor em relação ao processo de clonagem. Existem sistemas que somente permitem a clonagem a frio (quando a máquina virtual não está executando) e outros que permitem a clonagem, inclusive, a quente (quando a máquina virtual está executando).

Salvar o Estado de uma Máquina Virtual

Como foi visto no item anterior, uma máquina virtual nada mais é do que um conjunto de arquivos que contém as informações que descrevem um sistema computacional, contendo informações inclusive da execução de *softwares* .

Assim, é possível que seja conveniente garantir que uma máquina virtual possa ser interrompida em um determinado momento para se retomar a execução futuramente. Esse recurso é implementado através da funcionalidade de salvar o estado da máquina virtual.

Para entender a utilidade dessa função, suponha-se um servidor de aplicação virtualizado que seja comprometido e que se deseje restaurar ao funcionamento. Com o recurso de clonagem é possível criar um *backup* do sistema que possa ser utilizado no lugar do sistema comprometido. Porém, ainda é necessário incorrer no tempo de inicialização do sistema (seja somente o boot, ou até mesmo a inicialização de *softwares* também).

Caso exista um estado salvo, é possível somente desligar o sistema corrompido e inicializar o arquivo com o sistema já funcionando, sem precisar inicializar serviços ou realizar o *boot* da máquina. É importante ressaltar que esses clones de imagens com estados contêm também os arquivos, dados e configurações do momento em que a máquina foi salva. Caso exista um descompasso entre as máquinas salva e que está executando, haverá perda de informações.

Templates

Ao ver os conceitos de clonagem de máquinas virtuais, é possível vislumbrar a utilização do recurso para a criação de novas máquinas virtuais a partir de um modelo padrão. Ou seja, criar uma máquina virtual com configurações e *softwares* padronizados e replicar essa configuração como ponto de partida para a criação de máquinas-clientes. Essa noção não é irrazoável, uma vez que o investimento de tempo necessário para a criação de um sistema que atenda às necessidades de uma empresa pode ser considerável - e o retrabalho, custoso.

Nesse sentido, é interessante ter uma máquina virtual que seja somente leitura, com um estado salvo que possa ser replicado quantas vezes necessário for. Para tanto, alguns gerenciadores de máquinas virtuais incluem a possibilidade de se criar um template a partir de uma máquina já configurada.

Em uma definição simplista, um template é uma máquina virtual que não é possível inicializar. Ou seja, uma vez configurada a máquina virtual e feito o template, este fica protegido contra alterações acidentais. Na prática, cria-se uma imagem de uma máquina virtual.

Como nas funcionalidades anteriores, esse processo apresenta uma forma de criar uma máquina virtual que possa ser transferida entre sistemas. Nesse caso, garantindo que as cópias sejam iguais ao que foi estratificado durante a criação da imagem.

praticar

Vamos Praticar

“Máquinas virtuais são compostas por arquivos em disco que tornam certas atividades menos morosas que trabalhar com suas contrapartes físicas. Criar uma nova máquina virtual é frequentemente tão complicado quanto fazer a cópia de um arquivo e modificar algumas configurações. Instalar uma nova máquina virtual pode demorar alguns minutos, em contraste com dias ou semanas que leva para servidores serem pedidos, montados, entregues e instalados. Templates permitem a administradores de sistemas criar imagens de máquinas virtuais padronizadas e que podem ser copiadas à vontade. Até mesmo backup e recuperação podem ser mais simples no ambiente virtual. Além das mesmas técnicas e estratégias utilizadas em servidores físicos, é possível realizar o backup de um servidor inteiro, com

configurações e dados através de uma cópia. No caso de um problema, a mesma operação pode ser utilizada para recuperar a máquina virtual" (PORTNOY, 2012, p. 191, tradução própria).

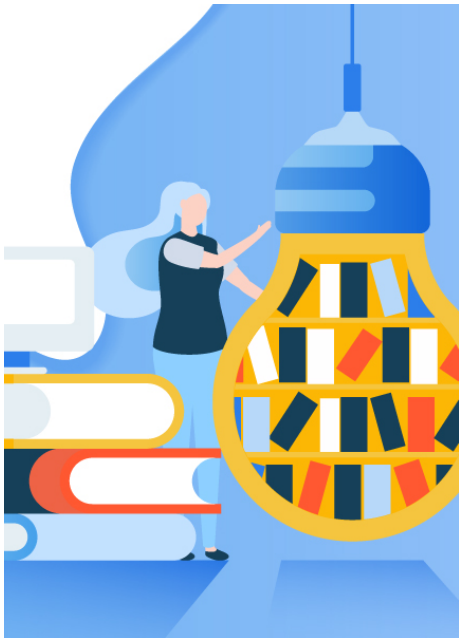
PORTNOY, M. **Virtualization Essentials** . Indianapolis: Indiana Published, 2012.

Com relação à cópia de máquinas virtuais, assinale a afirmativa correta:

- **a)** A cópia de máquinas virtuais afeta apenas seus dados, não sendo possível copiar as informações referentes aos dispositivos do sistema. Os dispositivos devem ser criados novamente em um novo sistema virtual.
- **b)** A clonagem de máquinas virtuais cria cópias de somente leitura, que não podem ser inicializadas, somente copiadas e replicadas no formato de máquinas virtuais padrão.
- **c)** Clonagem a quente, quando a máquina virtual está executando, é sempre possível. A clonagem a frio depende do tipo de gerenciador de máquinas virtuais.
- **d)** A clonagem de máquinas virtuais é um processo eficiente para a replicação de máquinas virtuais para vários usuários.
- **e)** Ao criar backups de máquinas virtuais, são incluídos todos os dados e softwares. Porém, caso não haja uma rotina de backups, estes podem ficar desatualizados.

indicações

Material Complementar



LIVRO

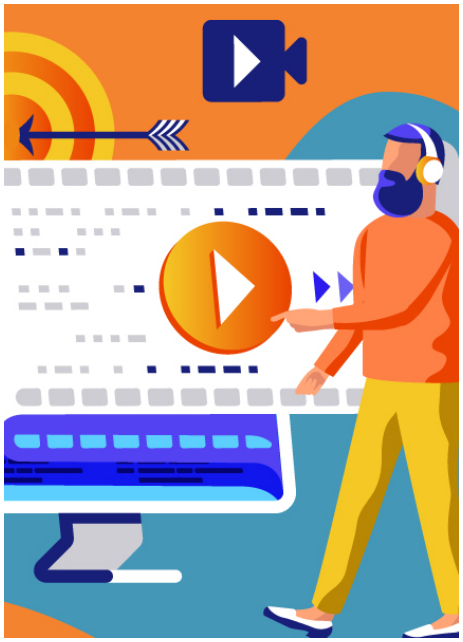
Computação em Nuvem Cloud Computing. Tecnologias e Estratégias.

Brian J. S. Chee e Curtis Franklin Jr.

Editora: M BOOKS

ISBN: 8576802074

Comentário: Esse livro é voltado para profissionais de TI mais experientes e que têm interesse em utilizar Cloud Computing para tentar atingir um outro patamar de proficiência e criação de soluções utilizando essa técnica. Para que o leitor entenda a posição atual, o autor busca na história da informática mais informações e ancora conceitos novos em ideias clássicas e bem conhecidas.



FILME

O Jogo da Imitação

Ano: 2014

Comentário: O filme mostra uma versão romanceada da vida do matemático inglês Alan Turing, o criador da Máquina de Turing, o princípio no qual se baseiam os computadores modernos. Apesar da falta de compromisso histórico do filme, é possível ter noção do contexto em que se desenvolveu a informática, a motivação e alguns dos algoritmos que foram utilizados

no equipamento que é o antepassado dos servidores de aplicações.

Para conhecer mais sobre o filme, acesse o trailer:

TRAILER

conclusão

Conclusão

Nesta unidade foi possível verificar que o ambiente virtualizado tem vários benefícios com relação à segurança e ao tempo necessário para a instalação. Os benefícios para a segurança podem ser através da utilização de máquinas virtuais para o controle do tráfego de rede com a utilização de *firewalls* virtualizados e ambientes de rede virtuais para a proteção de servidores internos à rede, que podem ser virtuais ou não, dependendo do caso.

Para a segurança dos dados, foi detalhada a possibilidade de criar cópias das máquinas virtuais para backup, seja já em um estado específico através do salvamento de estados, ou da clonagem de máquinas virtuais que podem estar executando ou não. Como efeito colateral, ainda é possível criar uma máquina virtual padronizada e distribuí-la para usuários interessados através de templates.

Esses conceitos podem ser aplicados para a implementação e manutenção de um serviço tipo PaaS (*Platform as a Service* - Plataforma como um Serviço), em que um cliente utiliza uma plataforma já pronta para auxiliar no desenvolvimento das suas aplicações.

referências

Referências Bibliográficas

ART OF SERVICE. **Cloud Computing Certification Kit** : Specialist: Platform Management & Storage Management. Londres: The Art of Service, 2009.

CARISSIMI, A. Virtualização: da teoria a soluções. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS, 26., 26 a 30 maio 2008, Rio de Janeiro. **Anais [...]** . Rio de Janeiro: SBC, 26 a 30 maio 2008. Disponível em: http://hostel.ufabc.edu.br/~marcelo.nascimento/BC1518Q3/arquivos/virtualizacao_cap4-v2.pdf . Acesso em: 11 dez. 2019.

CHEE, B. J. S.; FRANKLIN JR., C. **Computação em Nuvem Cloud Computing** - Tecnologias e Estratégias. São Paulo: M Books, 2013.

JONES, M. **Emulação do Sistema com o QEMU** . 25 set. 2007. Disponível em: https://www.ibm.com/developerworks/br/library/l-qemu/index.html . Acesso em: 19 dez. 2019.

MELL, P.; GRANCE, T. **NIST Special Publication 800-145** : The NIST Definition of Cloud Computing. Galithesburg: [S.n.], 2011.

NONAN, W.; DUBRAWSKY, I. **Firewall Fundamentals** . 1. ed. Indianapolis: Cisco Press, 2006.

PORTNOY, M. **Virtualization Essentials** . Indianapolis Canada: Indiana Published, 2012.

WATTS, S.; RAZA, M. **SaaS vs PaaS vs IaaS** : What's The Difference and How To Choose. 15 jun. 2019. Disponível em: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/ . Acesso em: 11 dez. 2019.

ZANUTTO, B. G. **Segurança em Cloud Computing** . [s.d.]. Disponível em: https://dcomp.sor.ufscar.br/verdi/topicosCloud/Artigo-Seguranca-Cloud.pdf . Acesso em: 17 dez. 2019.