VIRTUALIZAÇÃO III **3° ANO**

1-VIRTUALIZAÇÃO DE REDE

Por que a virtualização é importante?

- Ao usar a virtualização, você pode interagir com qualquer recurso de hardware com maior flexibilidade. Os servidores físicos consomem eletricidade, ocupam espaço de armazenamento e precisam de manutenção.
- Muitas vezes, você fica limitado pela proximidade física e pelo design da rede se quiser acessá-los. A virtualização remove todas essas limitações ao abstrair a funcionalidade do hardware físico no software. Você pode gerenciar, manter e usar sua infraestrutura de hardware como uma aplicação na Web.

Exemplo de virtualização

Considere uma empresa que precisa de servidores para três funções:

1. Armazenar o e-mail comercial com segurança.
2. Executar uma aplicação voltada para o cliente.
3. Executar aplicações de negócios internas.

Quais são os benefícios da virtualização?

A virtualização oferece vários benefícios para qualquer organização:

Uso eficiente de recursos

- A virtualização melhora os recursos de hardware usados em seu datacenter. Por exemplo, em vez de executar um servidor em um sistema de computador, você pode criar um grupo de servidores virtuais no mesmo sistema de computador usando e retornando servidores ao grupo conforme necessário.

Gerenciamento automatizado de TI

- Agora que os computadores físicos são virtuais, você pode gerenciá-los usando ferramentas de software. Os administradores criam programas de implantação e configuração para definir modelos de máquina virtual

Recuperação de desastres mais rápida

- Quando eventos como desastres naturais ou ataques cibernéticos afetam negativamente as operações de

negócios, recuperar o acesso à infraestrutura de TI e substituir ou consertar um servidor físico pode levar horas ou até dias. Por outro lado, esse processo leva minutos em ambientes virtualizados.

Virtualização de rede

- Todas as redes de computadores têm elementos de hardware como switches, roteadores e firewalls. Uma organização com escritórios em várias localizações geográficas pode ter várias tecnologias de rede diferentes trabalhando juntas para criar a rede corporativa.

Virtualização de rede

- **A virtualização de rede** é um processo que combina todos esses recursos de rede para centralizar as tarefas administrativas. Os administradores podem ajustar e controlar esses elementos virtualmente sem tocar nos componentes físicos, o que simplifica muito o gerenciamento da rede.

Por que a virtualização de redes?

A NV separa os serviços de rede do hardware subjacente e permite o aprovisionamento virtual de toda a rede. Recursos da rede física, como switches e roteadores, são agrupados e ficam acessíveis para qualquer usuário por meio de um sistema de gerenciamento centralizado.

A NV também permite a automação de muitas tarefas administrativas, diminuindo os erros manuais e o tempo de aprovisionamento. Ela pode proporcionar maior produtividade e eficiência de rede.

Exemplo de virtualização de redes

Um exemplo de virtualização de redes é a LAN virtual (VLAN, pela sigla em inglês). VLAN é a subseção de uma rede local (LAN) criada com software que combina dispositivos de rede em um grupo, seja qual for a localização física deles. As VLANs podem melhorar a velocidade e o desempenho de redes com muito tráfego e simplificar alterações ou adições à rede.

Tipos de virtualização de redes

Os tipos de virtualização de redes incluem virtualização **externa e interna. A virtualização externa** combina várias redes ou partes de redes em uma unidade virtual. **A virtualização interna** usa contêineres de software para

imitar ou fornecer a funcionalidade de uma única rede física.

2-SIMULADORES E EMULADORES

São sistemas baseados em software ou hardware, com propósito de ajudar a analisar um determinado problema em escalar menor; de certa forma, poupando tempo e dinheiro; no caso, em redes de computadores, possibilitam a simulação ou emulação de equipamentos físicos reais.

Simuladores e emuladores

Sumular "Imitar! Construir modelos que apresentam o maior número possível de características reais, e então experimentar, para depois aprender".

Emulação imitar algo próximo o suficiente para que possa ser substituto de coisas reais.

Principais simuladores e emuladores

GNS3 PACKET TRACER (CISCO) VIRL (CISCO)

Packet Tracer (Cisco)

O Cisco Packet Tracer é um produto Cisco oficial para estudantes da Cisco Academy. Simula redes Cisco.

Vantagens:

- Fácil de Instalar;
- Simula multiplos dispositivos e protocolos (routers, switches, wireless, etc..,)

Desvantagens:

- Nenhum suporte para outros fabricantes;
- Não é possível integrar-se a dispositivos físicos reais;
- Nenhum suporte para Mac OS.

VIRL (Cisco)

Esta é uma solução muito mais poderosa quando comparada ao Cisco Packet Tracer e permite não só aprender, mas a simulação de redes reais.

Vantagens:

▪Suporta Cisco router, switch, firewall e PC, etc);

▪Apropriado para estudantes de CCNA, CCNP e CCIE;

▪Grande número de protocolos e recursos suportados:

Desvantagens:

▪Não é gratuito (Custa entre $79.99 e $299.99 por ano);

▪Número limitado de dispositivos suportados.

▪Requer software de virtualização (VMware Workstation, Fusion, Player Pro ou ESXi);

GNS3

Permite que você execute uma pequena topologia consistindo apenas em alguns dispositivos em seu laptop, para aqueles que têm muitos dispositivos hospedados em vários servidores ou mesmo hospedados na nuvem.

Vantagens:

É possível conectar o GNS3 a qualquer rede real: aproveite seu hardware existente;

•Topologias e laboratórios personalizados dentro do GNS3 para treinamento em certificação de rede.

Desvantagens:

▪Não é Apropriado para estudantes;

▪Difícil de Instalar;

Virtualização de SO

3-MIGRAÇÃO DA VIRTUALIZAÇÃO EM TEMPO REAL

O que pode ser uma Migração?

Por simplis termos, este é considerado como deslocamento de elentos, matérias para um outro lugar, que a mesma pode ser de formas temporária ou permanentre.

- A computação em nuvem usa o conceito de virtualização, prmitindo que vários servidores virtualizados de forma isolada e com seguraça possam roradar um, é um único

servidor físico. Facilitando que muitas máquinas virtuais estejam hospedadas no mesmo servidor físico para otimizar a utilização dos recursos deste servidor, reduzindo assim os custo de implementação de Data Center.

Então a megração de virtualização em tempo real, passa a ser uma técnica onde todo sistema operacional e seus aplicativos associados a ele são migrados, ou seja, são transferidos de uma máquina física origem para uma outra máquina física destino.

As máquinas virtuais são migradas sem pertubações, nas aplicações em execução. Os benefícios da migração de máquinas virtuais incluem conservação de energia do servidor, balaciamento de carga física entre os servidores físicos e tolerância, a falhas em caso de falhas súbitas.

Para tal, existem parâmetros que afetam o desempenho de uma migração que devem ser considerados, para amigração em tempo real de uma máquina virtual. Tempo total de migração – o tempo decorrido desde o início de migração da primeira VM no host ogirem até o final da migração da última VM

No host destino; Donwtime – período de tempo em que a VM é totalmente suspensa durante a migração

Existem situações de migração da virtualização em tempo real, as quais podem gerar problemas no desempenho das aplicações e serviços, que estão a ser executados. Pesquisas foram realizadas para avaliar os problemas de migração de virtualização de máquinas viartuais em tempo real, para tal foram sujeridas várias métricas de desempenho.

A baixo são discritas as métricas que são normalmente utilizadas para medir o desempenho de migração em tempo real:

1. **Tempo de preparação (*Preparation Time*)**- momento que a migração inicia, até que começa a trasferência do estado da VM para máquina destino.
2. **Downtime-** tempo da interopção da máquina que está sendo migrada, inclui o estado da trasferência do processador.
3. **Tempo de retorno (*resume Time*)-** este é o tempo entre retomar a execução de VMs destino e final de migração quando são elimenados todas a depedências da origem.

4. **Páginas transferidas-** (*pages traferred*)- está é a quantidade de páginas de memórias transferidas, isto inclui uma duplicata em todos períodos de tempos sitados a cima.
5. **Tempo total de migração (*Total Migration Time*)-** tempo total de todos tempos, citados acima do início ao fim. O tempo total é importante porque afeta a liberação de recursos em ambos nós participantes, bem como dentro das VMs.
6. **Degradação da aplicação-** (*aplication degradation*)- está é a extensão a que a migração retarda os apliacativos em execução dentro da VM.

4- SEGURANÇA E ISOLAMENTO DE MÁQUINAS VIRTUAIS

Como acontece com toda tecnologia de computação a virtualização de agregados virtuais apresenta riscos próprios de segurança. Algumas destas questões vêm inerentemente devido á tecnologia em si enquanto muitos ocorrem quando a tecnologia de virtualização é implantada de forma incorreta.

Vetores de ataque e problemas de segurança

É comum que as novas tecnologias ou implementações surjam com algum prejuízo, e infelizmente a virtualização não escapa á regra. Riscos tradicionais de segurança da informação são herdados pela tecnologia de virtualização, a acrescentar às novas maneiras e métodos de executar e manipular a segurança de um agregado virtualizado.

Para avaliar adequadamente os riscos para uma infraestrutura de virtualização, as equipas de segurança e operações devem analisar e avaliar as vulnerabilidades que possam existir nessa mesma tecnologia, bem como as ameaças ao meio ambiente, que poderiam explorar essas vulnerabilidades, de forma a analisar o potencial impacto desses eventos de segurança.

Os resultados destes processos de avaliação de risco tendem a despoletar ações tais como aplicação de patches bem como configurações de sistema que tendem a restringir o acesso aos recursos da rede ou limitar os utilizadores que podem aceder as plataformas de gestão, VMs, ou a muitos outros controles e processos.

Analise dos tipos de vulnerabilidades e ataques em infraestruturas de virtualização.

Todos os ambientes de TI enfrentam uma série de ameaças sendo elas do foro operacional ou não. As ameaças operacionais são de **natureza acidental**, alguns exemplos podem ir a erros de operação realizados por funcionários, a ameaças mais maliciosas como insiders procurando comprometer os dados.

Normalmente, gerir a segurança de uma máquina física pode ser visto como um procedimento familiar e bem conhecido já que este tem sido o caso há largos anos. No entanto, num ambiente virtual tudo é composto por código, de modo a suportar diferentes camadas de elementos tais como sistemas operativos, interruptores virtuais, discos virtuais, etc

Segue-se uma detalhada listagem de vulnerabilidades e fraquezas encontradas em ambientes virtuais adaptado.

VM Sprawl

A vulnerabilidade de VM Sprawl refere-se á implementação descontrolada de máquinas virtuais em ambientes produtivos consistindo num processo simples curto e rápido de implementar as novas VMs em servidores já existentes.

O perigo está, se a entidade em questão não tem uma política de autorização para:

1. Uma gestão de mudanças em máquinas virtuais.
2. Um processo de revisão formal para a segurança das máquinas virtuais antes destas serem implementadas.
3. Um conjunto restrito de modelos de VMs autorizados.

A vulnerabilidade de VM Sprawl é parte integrante de um ambiente virtualizado, mas podemos reduzir a sua gravidade se:

- A equipa de engenharia de sistemas consegue ver a big picture, ou seja, entender exatamente o que o seu centro de dados suporta, e saber o que está sendo usado e onde. Pois saber as suas limitações irá ajudar a lidar melhor com os pedidos dos utilizadores para implementar novas VMs.
- Saber quais os recursos que cada nova máquina virtual requer, pois quando uma nova máquina virtual é colocada em produção, deve-se conhecer quais os recursos atribuídos á mesma bem como o tempo necessário que a equipa de administração de sistemas requer para gerir a infraestrutura virtual.

- Educar os utilizadores. Há uma série de maneiras de passar a palavra para a organização que a implementação de uma nova máquina virtual tem um custo real associado.
- Auditar regularmente as máquinas virtuais. Há duas maneiras para abordar esse tipo de auditoria. Analisar as estatísticas de utilização, ou ser informado pelos utilizadores que uma determinada máquina já não é necessária.