Avaliação de desempenho da migração de máquinas virtuais considerando diferentes configurações de segurança e de recursos computacionais em um ambiente de nuvem

Bruno Batista [1], Paulo Eustáquio [1], Dionisio Leite [1], Júlio Estrella [1], Sarita Bruschi, Marcos Santana [1] Regina Santana [1]

[1]Universidade de São Paulo – Instituto de Ciências Matemáticas e de Computação
São Carlos – SP – Brasil

{batista, psfe, dionisio, jcezar, sarita, mjs, rcs}@icmc.usp.br

Abstract. *This paper aims to conduct a performance evaluation of a cloud computing environment considering the migration of virtual machines available in Xen hypervisor and verify the impact generated in the system in the providing of more computational resources for virtual machines. Two methods of migration in the Live Migration that deal with different security implementations were considered. Furthermore, a prototype was developed which allowed the execution of the experiments.*

Resumo. *Este artigo tem como objetivo realizar uma avaliação de desempenho de um ambiente de computação em nuvem considerando a migração de máquinas virtuais disponíveis no hipervisor Xen e verificar o impacto gerado no sistema no provimento de mais recursos computacionais para as máquinas virtuais. Foram considerados dois métodos de migração disponíveis no Live Migration que lidam com diferentes implementações de segurança. Além disso, foi desenvolvido um protótipo que permitiu a execução dos experimentos.*

1. Introdução

Nos últimos anos um dos tópicos mais discutidos na área de Tecnologia de Informação (TI) tem sido computação em nuvem. Nesse modelo de prestação de serviços os recursos são fornecidos sob demanda e de forma transparente, uma vez que eles estão distribuídos geograficamente e os clientes não tem noção da sua localização e de toda a infraestrutura que compõe esse ambiente. Além disso, computação em nuvem fornece um ambiente totalmente escalável, pois permite aumentar dinamicamente a capacidade de prestação de serviços de uma empresa ou de atender solicitações.

Dessa forma, por se tratar de um sistema distribuído que provê serviços, supõe-se que o sistema computacional que compõe uma nuvem opere apropriadamente, oferecendo desempenho tanto em termos de rapidez na resposta, quanto em termos de disponibilidade (minimizando a interrupção no oferecimento de serviço) e segurança (evitando perda de dados ou mensagens), a fim de conquistar a confiança e satisfação dos seus clientes. Para isso, os provedores de serviços devem garantir diferentes atributos de Qualidade de Serviço (*Quality of Service – QoS*).

Garantir QoS em um ambiente de nuvem não é uma tarefa trivial, pois existem diversos tipos de clientes com as mais variadas exigências de prestação de serviços

[Ferguson and Huston 1998]. Existem várias métricas de QoS que podem ser utilizadas para quantificar um serviço. Entre elas pode-se citar: tempo médio de resposta, *throughput*, perda de pacotes, latência e a segurança. A segurança é métrica de destaque neste artigo.

De acordo com [Subashini and Kavitha 2011], pequenas e médias empresas têm investido cada vez mais em computação em nuvem, pois por meio dela pode-se obter acesso rápido a aplicações em qualquer lugar do mundo, necessitando-se apenas de um terminal com conexão com a Internet. Com essa estratégia é possível aumentar consideravelmente os recursos de infraestrutura da empresa, a um custo mais atrativo. Porém, várias preocupações podem impedir que novos clientes adentrem à nuvem, dentre essas preocupações vale ressaltar a garantia de segurança, aliada a garantia de desempenho e o custo envolvido [Lombardi and Di Pietro 2011, Vaquero et al. 2011, Velev and Zlateva 2011].

Definir até onde a segurança aplicada nas camadas de serviços de um ambiente de computação em nuvem interfere no desempenho do sistema e no custo do serviço oferecido é uma tarefa que carece de mais estudos. Atributos de QoS relacionados a segurança devem ser considerados em conjunto com os atributos relacionados a desempenho. Um fator importante a ser ressaltado nesse estudo é que, em sistemas computacionais em geral e, particularmente em sistemas distribuídos, segurança e desempenho geralmente são grandezas inversamente proporcionais.

2. Trabalhos Relacionados

Há na literatura diversos trabalhos que visam solucionar alguns dos problemas de segurança em computação em nuvem como os apresentados em [Chonka et al. 2011, Hu et al. 2011, Marty 2011, Mohammed et al. 2011, Khorshed et al. 2012, Yang and Jia 2012, Zissis and Lekkas 2012]. Nesses trabalhos são discutidos mecanismos aplicados no gerenciamento de dados na computação em nuvem como: controle de acesso, integridade, compartilhamento, armazenamento e controle de *logs*. Outra abordagem considerada para melhorar a segurança da nuvem refere-se à detecção de ataques, como as consideradas nas arquiteturas apresentadas em [Dhage and Meshram 2012, Khorshed et al. 2012, Li et al. 2012].

Em [Laureano et al. 2007, Weng et al. 2008, Jin and Huh 2011] são apresentadas soluções para ameaças ao isolamento de máquinas virtuais (*VM – Virtual Machine*) como ataques por meio de *system calls*, ataques de sobrecarga de *buffer*, invasão de memória e violação de identidades.

Em [Zhang et al. 2011] os autores propõem um abordagem transparente que protege a privacidade e integridade das máquinas virtuais dos clientes em infraestruturas virtualizadas, enquanto que, [Casola et al. 2011] mostra uma avaliação do impacto gerado sobre o desempenho de um ambiente em nuvem na aplicação de segurança.

De todos os trabalhos analisados não foram encontrados na literatura estudos que se preocupam em realizar uma avaliação de desempenho que considera a aplicação de diferentes níveis de segurança em um ambiente de computação em nuvem e a partir dessa avaliação propor modelos de negócio que relacionem segurança, desempenho e custo. Sabe-se que conforme níveis mais rígidos de segurança são necessários, a interferência

dessas políticas, necessárias para manter a segurança, sobre o desempenho do sistema também cresce. No caso de computação em nuvem, pode-se compensar a sobrecarga gerada pelas políticas de segurança, alocando-se mais recursos para a aplicação. No entanto, a alocação de mais recursos irá interferir no custo a ser pago pelo cliente. Desta forma, quando se considera computação em nuvem, a relação entre desempenho e segurança deve considerar um novo parâmetro, que é o custo dos recursos alocados ao cliente.

Dessa forma, o trabalho apresentado neste artigo tem o objetivo de avaliar o desempenho de uma nuvem durante a migração de máquinas virtuais disponíveis pelo hipervisor Xen e verificar o impacto gerado sobre o ambiente na variação da quantidade de memória e de núcleos disponíveis para as máquinas virtuais. Para atingir o objetivo proposto, foram considerados dois métodos de migração: um que aplica políticas de segurança durante a migração e outro que não. Além disso, foi desenvolvido um protótipo onde os experimentos foram realizados. Os resultados obtidos serão utilizados para o aperfeiçoamento do protótipo e para que novos modelos de negócio que considerem desempenho, segurança e custo sejam propostos em trabalhos futuros.

3. Computação em Nuvem

Segundo o NIST (*National Institute of Standards and Technology*), computação em nuvem é um modelo que permite ubiquidade, conveniência, acesso sob demanda para um conjunto de recursos compartilhados que são configuráveis (redes, servidores, mecanismos de armazenamento, aplicações e serviços) e que podem ser rapidamente entregues com um esforço mínimo de gestão por parte dos usuários [Mell and Grance 2011].

A nuvem em si é uma abstração de toda a infraestrutura lógica (*software*, plataformas de *middleware* ou *frameworks*) e física (*hardware*) de um provedor que oferece seus serviços cobrando por eles ou não. Dessa forma, uma nuvem pode ser classificada conforme a sua localização e finalidade [Velev and Zlateva 2011].

- **Nuvem Privada:** construída exclusivamente para um único cliente (uma empresa, por exemplo) sobre um *data center* privado. Diferentemente de um *data center* privado virtual, a infraestrutura utilizada pertence ao cliente, e, portanto, ele possui total controle sobre como as aplicações são implementadas;
- **Nuvem Pública:** a infraestrutura computacional é hospedada pelo provedor de serviços e é compartilhada entre todas as organizações contratantes. O cliente não tem visibilidade e controle sobre onde essa infraestrutura computacional está hospedada;
- **Nuvem Comunitária:** a infraestrutura de uma nuvem é compartilhada por diversas organizações e suporta uma comunidade específica que partilha as mesmas preocupações como, por exemplo, a finalidade, os requisitos de segurança, políticas e considerações sobre o cumprimento dos serviços;
- **Nuvem Híbrida:** considera a composição dos modelos de nuvens públicas e privadas. Uma nuvem híbrida permite que uma nuvem privada possa ter seus recursos ampliados a partir de uma reserva de recursos em uma nuvem pública. Essa característica possui a vantagem de manter os níveis de serviço mesmo que haja variações rápidas na necessidade dos recursos na prestação de serviços.

Muitos estudos na literatura dividem os serviços prestados pela nuvem em três categorias principais [Foster et al. 2008, Wang et al. 2008, Leavitt 2009, Mell and Grance 2011].

- **Software como Serviço (*SaaS – Software as a Service*):** é o *software* oferecido por um provedor de serviços, disponível sob demanda, geralmente por meio de um navegador *Web*. Assim, um único *software* pode ser fornecido para vários clientes ao mesmo tempo, e esses clientes podem compartilhar informações e interagir com os outros sem a necessidade de instalar novos *softwares* em suas máquinas;
- **Plataforma como Serviço (*PaaS – Platform as a Service*):** permite que os clientes desenvolvam novas aplicações utilizando APIs (*Application Programming Interface*), implementando e operando remotamente. As plataformas oferecem ferramentas de desenvolvimento inclusas e gerenciamento das configurações.
- **Infraestrutura como Serviço (*IaaS – Infrastructure as a Service*):** a IaaS incorpora a capacidade de abstração de recursos assim como toda a conectividade física e lógica desses recursos. Além disso, fornece um conjunto de APIs que permitem o gerenciamento e outras formas de interação com as infraestruturas desenvolvidas pelos clientes.

Um fator a ser considerado, tanto na implementação das categorias de serviços apresentadas, quanto na classificação das nuvens, é a virtualização. Em uma nuvem os recursos são virtualizados independente da localização ou do serviço fornecido.

A virtualização é a técnica para a criação de uma ou mais estações de trabalho/servidores em um único computador físico, que assume o papel de vários computadores lógicos também conhecidos como máquinas virtuais. Cada máquina virtual oferece um ambiente completo similar a uma máquina física. Com isso, cada máquina virtual pode ter seu próprio sistema operacional, aplicativos e serviços de rede [Carissimi 2008].

A virtualização é a tecnologia chave na computação em nuvem. Nesse contexto, ela refere-se principalmente a abstração dos recursos físicos de TI aos clientes e aplicativos que os usam. Além disso, permite que os servidores, dispositivos de armazenamento, *hardware* e outros recursos sejam tratados em conjunto ao invés de sistemas distintos, de modo que esse conjunto de recursos possa ser alocado por demanda [Chieu et al. 2009]. Sendo assim, a virtualização é adaptada a uma infraestrutura de nuvem dinâmica, pois oferece vantagens importantes no compartilhamento, gerenciamento e isolamento dos recursos [Rimal et al. 2009].

A utilização de máquinas virtuais tornou-se uma alternativa concreta para várias soluções domésticas e corporativas. Graças a diversas pesquisas, no futuro será possível utilizar os melhores recursos das mais variadas plataformas operacionais sem a necessidade de investir em equipamentos específicos. No entanto, o gerenciamento de máquinas virtuais assim como de outros recursos que compõem uma nuvem exige algumas medidas de segurança.

4. Segurança em Nuvem

Segurança pode ser compreendida como a qualidade de serviço que visa assegurar seu funcionamento e evitar a ocorrência de violações no sistema. As ameaças enfrentadas por um provedor de serviços ou por um cliente podem ser categorizadas com base nos objetivos e propósitos dos ataques. Dessa forma, o conhecimento funcional dessas categorias de ameaças pode ajudar a organizar uma estratégia de segurança para a implementação de contramedidas.

Nos últimos anos algumas organizações de segurança lançaram alguns resultados de suas pesquisas para conscientizar as empresas interessadas em aderir à computação em nuvem dos riscos associados a essa decisão. Entre esses estudos pode-se destacar [Heiser and Nicolett 2008, Brunette and Mogull 2009, Catteddu 2010, Archer et al. 2010, Khorshed et al. 2012]

De acordo com [Brunette and Mogull 2009, Lombardi and Di Pietro 2011, Subashini and Kavitha 2011, Vaquero et al. 2011] há vários aspectos críticos de segurança em um ambiente de nuvem. Os principais são:

- **Segurança de Identidade:** por meio da segurança da identidade mantém-se a integridade e confidencialidade dos dados e das aplicações ao mesmo tempo que tornam o acesso disponível aos clientes apropriados. Alguns dos principais padrões e soluções utilizadas para a implantação de gerência de identidades são: SAML (*Security Assertions Markup Language*), OpenID, Shibboleth, Higgins, OpenAM, XACML *(Extensible Access Control Markup Language)* e OAuth.
- **Segurança da Informação:** nos tradicionais *data centers*, controles de acesso físico, de acesso ao *hardware* e *software* e de identidade combinam-se para proteger os dados. Na nuvem, a barreira de proteção da infraestrutura é difusa. Assim, a segurança da informação exigirá [Catteddu 2010]:
  - **Isolamento dos dados:** na multi-alocação de recursos os dados do ambiente devem ser armazenados de forma segura, a fim de protegê-los quando vários clientes utilizam os recursos compartilhados. Virtualização, criptografia e controle de acesso são mecanismos que permitem vários graus de isolamento de dados entre empresas e clientes diferentes;
  - **Segurança dos dados:** os provedores de serviços devem fornecer mecanismos de segurança para proteger os dados de seus clientes. Isso envolve o uso de técnicas de criptografia e controle de acesso aos dados;
  - **Segurança de rede:** todo o fluxo de dados da rede deve estar seguro para evitar a perda e manipulação de informações. Para isso, pode-se utilizar técnicas de criptografia ou outras técnicas que garantam a segurança e o monitoramento do tráfego de rede;
  - **Integridade dos dados:** qualquer tipo de transação deve seguir as propriedades de ACID (Atomicidade, Consistência, Isolamento e Durabilidade) para garantir a integridade dos dados;
  - **Vulnerabilidade na virtualização:** uma máquina virtual oferece um ambiente completo similar a uma máquina física. Dessa forma, algumas vulnerabilidades encontradas em uma máquina física são também encontradas nos *softwares* de virtualização. Essas vulnerabilidades podem ser utilizadas por invasores para adquirirem determinados privilégios e violar outras restrições de segurança [Weng et al. 2008, Jin and Huh 2011].
- **Segurança de infraestrutura:** quando uma empresa contrata um serviço de IaaS e presta serviços a outros clientes, o provedor de IaaS é indiferente quanto às operações e ao gerenciamento de pedidos das empresas contratantes do seu serviço. Assim, é importante que o contratante assuma total responsabilidade por assegurar a sua infraestrutura, implantando, por exemplo, mecanismos de controle de acesso, de criptografia dos dados e/ou ferramentas de monitoramento da rede

[Mather et al. 2009, Velev and Zlateva 2011]. Além disso, tem-se a segurança de toda a infraestrutura física pertencente a um provedor que deve ser garantida.

Em sistemas distribuídos, a aplicação de técnicas e metodologias de segurança influencia diretamente sobre o desempenho de um sistema, fazendo com que segurança e desempenho sejam muitas vezes duas variáveis inversamente proporcionais. No entanto, aplicar níveis de segurança em um ambiente distribuído como o de uma nuvem não é uma tarefa trivial. Dessa forma, foram realizados experimentos com o intuito de avaliar os métodos de migração de máquinas virtuais disponíveis no Xen (descritos na próxima seção) e verificar o impacto gerado sobre o desempenho do sistema na variação da quantidade de memória e de núcleos disponíveis para as máquinas virtuais.

5. Experimentos Realizados

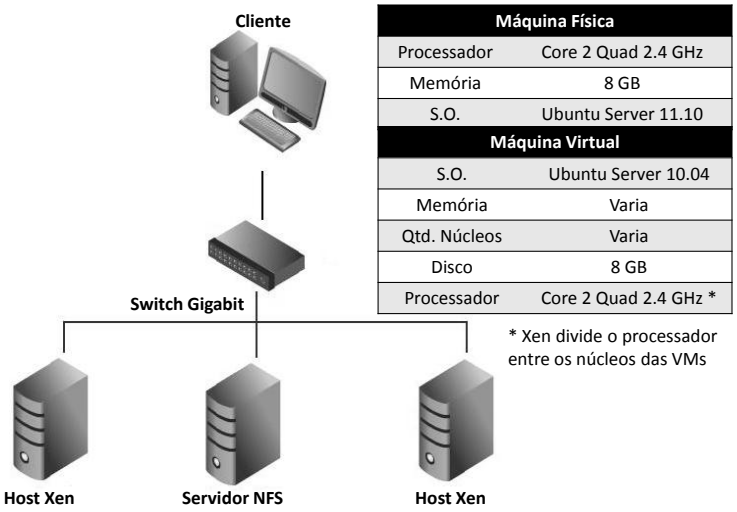

Figura 1. Ambiente de experimentos.

Para a execução dos experimentos foi desenvolvido um protótipo composto por um servidor NFS (*Network File System*) e dois outros servidores, configurados com o virtualizador Xen, conectados por um *switch gigabit*. O servidor NFS é responsável por manter uma imagem (*Ubuntu 10.04*) para a criação de diversas máquinas virtuais, sendo que os outros dois servidores buscam essa imagem no servidor NFS para criar as instâncias das VMs. A Figura 1 apresenta o ambiente considerado nos experimentos.

O servidor NFS facilita a migração de máquinas virtuais, pois não é necessário enviar para o *host* de destino todo o sistema operacional, podendo enviar somente o estado salvo da VM, os contextos de memória, CPU, entre outros. Com isso, o *host* de destino busca apenas a imagem no servidor NFS e a associa com os parâmetros migrados do *host* de origem. Nesse contexto, foram realizadas migrações de um *host* de origem para um de destino por meio do *Live Migration*.

O *Live Migration* mantém o sistema convidado, ou seja, a máquina virtual, em execução no *host* de origem e inicia a migração de uma cópia da memória do sistema convidado sem interrompe-lo para o *host* de destino. Todas as páginas de memória são monitoradas e caso ocorra alguma alteração, a memória é atualizada com as páginas alteradas [Jiang et al. 2012]. Quando a migração termina, os registros são carregados no *host*

de destino e a VM retorna a sua execução. Dessa forma, a máquina virtual é interrompida apenas durante o carregamento dos parâmetros de memória no *host* de destino.

Para realizar o *Live Migration* no Xen, pode-se utilizar o parâmetro padrão *–live*. Esse parâmetro não aplica metodologias de segurança durante a migração. Ele baseia-se na política de melhor esforço (*best-effort*), onde um pacote pode chegar desordenado, duplicado, ou pode ser perdido. Dessa forma, algumas falhas como perda de pacotes com informações da memória de uma máquina virtual durante as migrações podem ocorrer, o que pode gerar problemas durante o carregamento dos registros no *host* de destino. Para realizar o *Live Migration* de forma segura é utilizado o protocolo SSL (*Secure Sockets Layer*). O protocolo SSL provê a privacidade e a integridade de dados entre dois *hosts* que se comunicam pela Internet. [Rescorla 2001].

5.1. Planejamento dos Experimentos

Foram executados dois conjuntos de experimentos. Em ambos foram analisados os métodos de migração de máquinas virtuais e o impacto gerado no desempenho do ambiente com a alteração dos recursos das VMs. Com relação a carga aplicada ao ambiente desenvolvido, cada máquina virtual executa uma carga representada pelo *benchmark Phoronix Test Suite Apache*.

No Experimento 1 foram considerados três fatores, dois com três níveis e um com dois níveis e cada VM possui apenas um núcleo virtual. Esses fatores e seus respectivos níveis são apresentados a seguir.

- **A – Método de migração:** *Live Migration* com segurança (*–ssl*) e sem segurança (*–live*);
- **B – Quantidade de Máquinas Virtuais:** 4, 6 e 8;
- **C – Quantidade de Memória RAM:** 256, 512 e 1024 MB.

No Experimento 2 foram considerados três fatores, dois com dois níveis e um com três níveis e cada VM possui 512 MB de memória RAM. Esses fatores e seus respectivos níveis são apresentados a seguir.

- **A – Método de migração:** *Live Migration* com segurança (*–ssl*) e sem segurança (*–live*);
- **B – Quantidade de Máquinas Virtuais:** 4, 6 e 8;
- **C – Quantidade de Núcleos:** 1 e 2.

Nos dois experimentos foi utilizado o modelo fatorial completo que mede a variável de resposta utilizando a combinação entre todos os níveis dos fatores [Jain 1991]. A variável de resposta analisada foi a **Quantidade de Requisições por Segundo**, obtida através do *benchmark Phoronix Test Suite Apache*. Os resultados apresentados referem-se à média dos resultados, ao intervalo de confiança com 95% de confiança e à 10 repetições.

5.2. Migração de VMs com Diferentes Configurações de Memória RAM

Pode-se verificar que as migrações realizadas sem segurança apresentaram um intervalo de confiança alto devido às falhas que ocorreram durante as migrações. Esse método de migração utiliza a política de melhor esforço, onde não há garantia de entrega dos pacotes durante a migração. Dessa forma, essas falhas geraram perdas de máquinas virtuais

e influenciaram negativamente sobre o desempenho do ambiente, representado nos experimentos pela quantidade média de requisições atendidas por segundo pelas VMs. Por isso, o comportamento do ambiente foi considerado instável. Vale lembrar que todas as análises consideraram o sistema como um todo e não o comportamento de uma única VM. Dessa forma, a quantidade de requisições por segundo foi obtida pelo total de requisições atendidas pela quantidade de VMs disponível. Em caso de falha, considerou-se que a VM não atendeu nenhuma requisição, pois a integridade e a disponibilidade dos dados não foram garantidas.

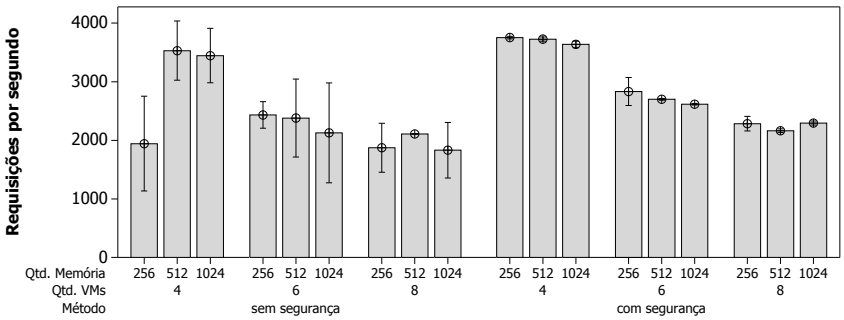

Figura 2. Migração sem segurança vs migração com segurança.

Por outro lado, na migração com segurança verificou-se que o comportamento do sistema é estável, pois todas as migrações foram executadas com sucesso e os intervalos de confiança foram baixos. Isso ocorreu graças às características do protocolo SSL. As migrações com 4 VMs apresentaram os melhores resultados referentes as requisições por segundo. Essas máquinas virtuais possuem apenas um núcleo virtual (VCPU). Dessa forma, o hipervisor Xen atribui um núcleo virtual para cada núcleo físico, ou seja, 4 núcleos virtuais para 4 núcleos físicos (como apresentado nas configurações da Figura 1).

Com 6 e 8 máquinas virtuais tem-se uma redução na quantidade de requisições por segundo, pois a concorrência pelos núcleos físicos é maior. A quantidade média de requisições por segundo teve uma redução que variou, aproximadamente, entre 24% e 28% na alteração de 4 para 6 máquinas virtuais, e entre 12% e 20% na alteração de 6 para 8. Ou seja, em um aumento de 100% na quantidade de VMs disponíveis para atender as requisições dos clientes, obteve-se uma redução entre, aproximadamente, 36% e 42% da quantidade média de requisições por segundo.

Além disso, observou-se que com as quantidades de memória utilizadas para as VMs, a análise da influência da alteração desse fator sobre a variável de resposta tornou-se complicada. Isso porque, com 256 MB de RAM, foi possível executar a carga imposta sem danos aparentes ao desempenho. Dessa forma, são necessários mais experimentos com quantidades de memória inferiores a 256 MB para que se analise, por exemplo, o comportamento do ambiente com o estouro de memória ou com a utilização constante de SWAP.

5.3. Migração de VMs com Diferentes Configurações de Núcleos Virtuais

Pode-se observar na Figura 3 que, assim como ocorreu nos experimentos onde alterou-se a quantidade de memória das VMs, a migração sem segurança mostrou-se instável. Os altos intervalos de confiança e a grande variação da quantidade de requisições atendidas

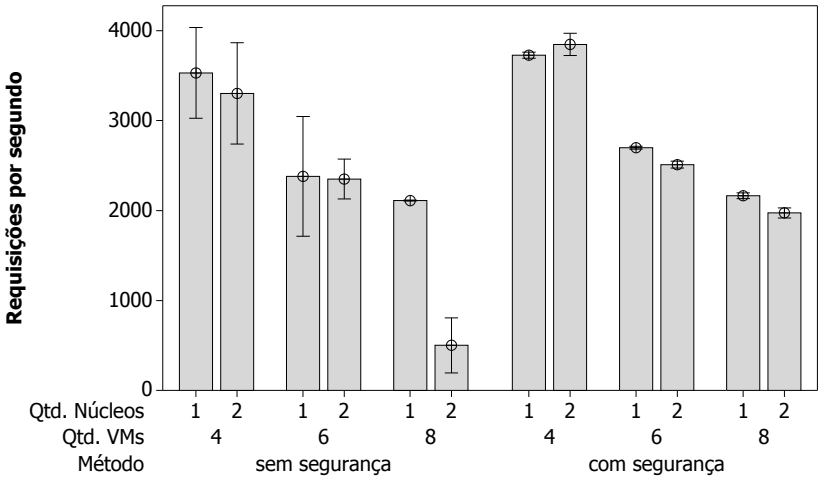

Figura 3. Migração sem segurança vs migração com segurança.

por segundo comprovam isso. Por outro lado, na migração com segurança os intervalos de confiança foram pequenos e todos, com exceção dos experimentos com 4 VMs e cada uma com 1 e 2 núcleos, não se sobrepuseram. Na exceção apresentada verificou-se que nada pode ser afirmado, pois em nenhum dos experimentos, a média de um é sobreposta pelo intervalo inferior ou superior do outro. Nesse caso são necessárias mais repetições e análises dos experimentos para que uma conclusão concreta seja realizada.

Nos demais experimentos com migração segura verificou-se que conforme a quantidade de máquinas virtuais e de núcleos é aumentada, menor é a quantidade de requisições atendidas por segundo. Isso ocorre devido a maior concorrência por recursos físicos de processamento. Essa concorrência gerou uma redução entre 27% e 35% na alteração de 4 para 6 VMs, e entre 19% e 22% na alteração de 6 para 8 VMs. Com o aumento de 100% na quantidade de VMs, ou seja, de 4 para 8, essa redução foi maior, variando entre aproximadamente, 41% e 49%.

Analisando o impacto sobre a variável de resposta gerado pela alteração da quantidade de núcleos, verificou-se um redução de aproximadamente 7% para 6 VMs e de 9% para 8 VMs. Dessa forma, fica claro que o simples aumento de recursos virtuais não implicou em um aumento na quantidade de requisições atendidas por segundo, pois os recursos físicos foram limitantes.

6. Conclusões

Inicialmente, nos experimentos realizados não foi possível mensurar o tempo gasto para a migração das VMs, uma vez que no método sem segurança do *Live Migration*, o comportamento do sistema foi bastante instável devido às falhas ocorridas durante as migrações. Dessa forma, não foi possível avaliar o impacto da utilização da migração com segurança sobre o desempenho do ambiente devido à ineficiência da migração sem segurança que não proporcionou dados plausíveis para uma comparação.

Por outro lado, o simples aumento da quantidade de núcleos e da quantidade de memória não implicou no aumento da quantidade de requisições atendidas por segundo. Isso significa que, o aumento de recursos virtuais das VMs não implicará em um melhor desempenho do sistema se a quantidade de recursos físicos for atingida.

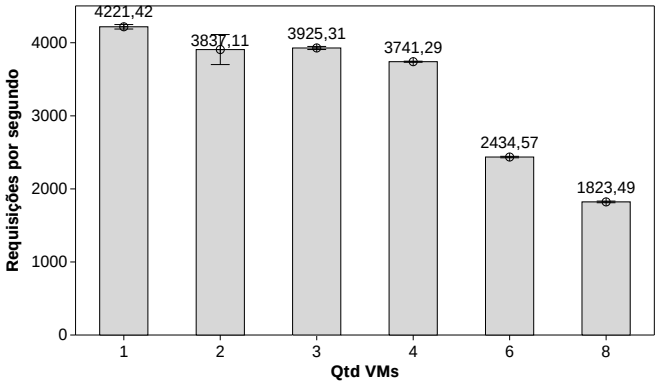

Figura 4. Requisições por segundo executadas por cada VM.

Nota-se no gráfico da Figura 4 que a média das requisições por segundo do experimento com uma VM até o experimento com quatro VMs é muito próxima. Isto ocorre, pois o *host* que hospeda as VMs possui quatro núcleos físicos e o escalonador do Xen, por padrão, aloca uma CPU física para cada CPU virtual. Dessa forma, o desempenho médio das VMs será similar para até quatro VMs em um mesmo *host* se a aplicação que estiver sendo executada for a mesma. Quando o número de VMs aumenta para seis, é possível notar uma degradação no desempenho das VMs. Isto ocorre, pois os quatro núcleos do *host* são compartilhados para as seis VMs, diminuindo a média de requisições por segundo. O mesmo ocorre quando o número de VMs é aumentado para oito.

Dessa forma, novos experimentos serão executados utilizando outros virtualizadores e o aprendizado obtido com os experimentos apresentados neste artigo. Serão analisadas outras técnicas e metodologias de segurança disponíveis na literatura que visam resolver desafios que envolvem o isolamento de dados por meio de máquinas virtuais, para garantir a integridade, disponibilidade e confidencialidade desses dados. Essas técnicas permitirão que análises sobre o impacto gerado por elas sobre o desempenho do sistema sejam realizadas, bem como a análise do provisionamento de mais recursos computacionais para as máquinas virtuais para fazer frente ao impacto gerado sobre o desempenho pela utilização de segurança. Todas essas avaliações permitirão a definição de modelos de negócio para computação em nuvem que considerem desempenho, segurança e custo e que serão apresentados em trabalhos futuros.

Agradecimentos

Os autores agradecem o apoio financeiro fornecido pelo CNPq, CAPES e FAPESP para o desenvolvimento de projetos no grupo de Sistemas Distribuídos e Programação Concorrente do ICMC-USP.

Referências

Archer, J., Boehme, A., Cullinane, D., Kurtz, P., Puhlmann, N., and Reavis, J. (2010). Top threats to cloud computing v1. 0. *Cloud Security Alliance*.

Brunette, G. and Mogull, R. (2009). Security guidance for critical areas of focus in cloud computing v2. 1. *Cloud Security Alliance*, pages 1–76.

Carissimi, A. (2008). Virtualização: da teoria a soluções. *Minicursos do Simpósio Brasileiro de Redes de Computadores–SBRC*, 2008:173–207.

Casola, V., Cuomo, A., Rak, M., and Villano, U. (2011). The cloudgrid approach: Security analysis and performance evaluation. *Future Generation Computer Systems*.

Catteddu, D. (2010). Cloud computing: benefits, risks and recommendations for information security. *Web Application Security*, pages 17–17.

Chieu, T., Mohindra, A., Karve, A., and Segal, A. (2009). Dynamic scaling of web applications in a virtualized cloud computing environment. In *e-Business Engineering, 2009. ICEBE'09. IEEE International Conference on*, pages 281–286. IEEE.

Chonka, A., Xiang, Y., Zhou, W., and Bonti, A. (2011). Cloud security defence to protect cloud computing against http-dos and xml-dos attacks. *Journal of network and computer applications*, 34(4):1097–1107.

Dhage, S. and Meshram, B. (2012). Intrusion detection system in cloud computing environment. *International Journal of Cloud Computing*, 1(2):261–282.

Ferguson, P. and Huston, G. (1998). *Quality of service: delivering QoS on the Internet and in corporate networks*. Wiley New York.

Foster, I., Zhao, Y., Raicu, I., and Lu, S. (2008). Cloud computing and grid computing 360-degree compared. In *Grid Computing Environments Workshop, 2008. GCE'08*, pages 1–10. Ieee.

Heiser, J. and Nicolett, M. (2008). Assessing the security risks of cloud computing. *Gartner Report*.

Hu, H., Ahn, G., and Kulkarni, K. (2011). Anomaly discovery and resolution in web access control policies. In *Proceedings of the 16th ACM symposium on Access control models and technologies*, pages 165–174. ACM.

Jain, R. (1991). *The art of computer systems performance analysis: techniques for experimental design, measurement, simulation, and modeling*. New York, NY, USA, Wiley.

Jiang, X., Yan, F., and Ye, K. (2012). Performance influence of live migration on multi-tier workloads in virtualization environments. In *CLOUD COMPUTING 2012, The Third International Conference on Cloud Computing, GRIDs, and Virtualization*, pages 72–81.

Jin, S. and Huh, J. (2011). Secure mmu: Architectural support for memory isolation among virtual machines. In *Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP 41st International Conference on*, pages 217–222. IEEE.

Khorshed, M., Ali, A., and Wasimi, S. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems*.

Laureano, M., Maziero, C., and Jamhour, E. (2007). Protecting host-based intrusion detectors through virtual machines. *Computer Networks*, 51(5):1275–1283.

Leavitt, N. (2009). Is cloud computing really ready for prime time. *Growth*, 27(5).

Li, J., Li, B., Wo, T., Hu, C., Huai, J., Liu, L., and Lam, K. (2012). Cyberguarder: A virtualization security assurance architecture for green cloud computing. *Future Generation Computer Systems*, 28(2):379–390.

Lombardi, F. and Di Pietro, R. (2011). Secure virtualization for cloud computing. *Journal of Network and Computer Applications*, 34(4):1113–1122.

Marty, R. (2011). Cloud application logging for forensics. In *Proceedings of the 2011 ACM Symposium on Applied Computing*, pages 178–184. ACM.

Mather, T., Kumaraswamy, S., and Latif, S. (2009). *Cloud security and privacy: an enterprise perspective on risks and compliance*. O'Reilly Media, Incorporated.

Mell, P. and Grance, T. (2011). The nist definition of cloud computing (draft). *NIST special publication*, 800:145.

Mohammed, S., Servos, D., and Fiaidhi, J. (2011). Developing a secure distributed osgi cloud computing infrastructure for sharing health records. *Autonomous and Intelligent Systems*, pages 241–252.

Rescorla, E. (2001). *SSL and TLS: designing and building secure systems*, volume 1. Addison-Wesley Reading, Massachusetts.

Rimal, B., Choi, E., and Lumb, I. (2009). A taxonomy and survey of cloud computing systems. In *INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on*, pages 44–51. IEEE.

Subashini, S. and Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1):1–11.

Vaquero, L., Rodero-Merino, L., and Morán, D. (2011). Locking the sky: a survey on iaas cloud security. *Computing*, 91(1):93–118.

Velev, D. and Zlateva, P. (2011). Cloud infrastructure security. *Open Research Problems in Network Security*, pages 140–148.

Wang, L., Tao, J., Kunze, M., Castellanos, A., Kramer, D., and Karl, W. (2008). Scientific cloud computing: Early definition and experience. In *High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on*, pages 825–830. IEEE.

Weng, C., Luo, Y., Li, M., and Lu, X. (2008). A blp-based access control mechanism for the virtual machine system. In *Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for*, pages 2278–2282. IEEE.

Yang, K. and Jia, X. (2012). Data storage auditing service in cloud computing: challenges, methods and opportunities. *World Wide Web*, 15(4):409–428.

Zhang, F., Chen, J., Chen, H., and Zang, B. (2011). Cloudvisor: Retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization. In *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles*, pages 203–216. ACM.

Zissis, D. and Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3):583–592.