Segurança e ampla disponibilidade em ambientes de computação em nuvem

Conteúdo

Resumo executivo

A computação em nuvem vem se tornando uma forma cada vez mais popular de fornecer serviços de negócios valiosos e voltados para TI. A adoção da tecnologia da nuvem torna mais acessível um ambiente de computação virtualizado e dinamicamente escalável. Recursos que poderiam não estar disponíveis por uma perspectiva de custos como gerenciamento de infraestrutura, software e hardware otimizados podem ser implementados rapidamente e de maneira rapidamente escalável. Os serviços, aplicações e processos ficam disponíveis on demand, independente da localização do usuário ou dispositivo de acesso. O fornecedor de nuvem é o responsável pelo ambiente, o que significa que as organizações podem utilizar os recursos por curtos períodos de tempo sem ter que se preocupar em mantê-lo quando ele estiver ocioso.

Enquanto os modelos de computação em nuvem são atraentes por sua flexibilidade e efetividade de custos, certos desafios devem ser observados para que ela se torne uma opção viável em relação aos serviços de TI tradicionais. A primeira e mais importante questão é a segurança. O aspecto externo da terceirização pode significar um desafio à manutenção da integridade de dados e privacidade, à disponibilidade de dados e serviços, à conformidade regulatória e à disponibilidade de acesso altamente seguro à aplicações e à informação. Em suma, a computação em nuvem pode representar um nível adicional de risco para o negócio.

As organizações precisam, portanto, estabelecer um relacionamento de confiança com seus provedores de computação em nuvem e compreender os riscos em relação a como esses provedores implementam, implantam e gerenciam a segurança. Seja como parte de um serviço ou como componentes opcionais, o fornecedor de nuvem deve trabalhar alguns recursos específicos de gerenciamento de riscos e segurança.

Este documento discute os desafios relacionados à segurança e disponibilidade em ambientes de computação em nuvem. Mais especificamente, o texto introduz o Framework de Segurança IBM, e como elas podem endereçar os desafios de segurança na nuvem através de uma abordagem mais holística. Este documento analisa ainda as responsabilidades de segurança compartilhada que existem entre o cliente e o provedor. Por fim, investiga também as preocupações com o alto nível de disponibilidade e demonstra como é possível melhorar a resiliência de seus servidores virtuais em um ambiente de computação na nuvem.

Computação em nuvem: visão geral e benefícios

Cada modelo de computação em nuvem, seja público, privado ou híbrido, enfrenta diferentes níveis de risco de TI. No modelo de fornecimento de nuvem privada, o proprietário da nuvem não compartilha recursos com qualquer outra empresa. As nuvens privadas são propriedade de uma única organização e por ela operadas, fornecendo serviços de TI somente no próprio perímetro da rede interna.

No modelo de computação em nuvem pública, as atividades e funções de TI são fornecidas como um serviço que pode ser cobrado (como uma assinatura ou no sistema de pagamento conforme o uso), e que utiliza recursos que não são do cliente, ou seja, que estão hospedados nas redes de fornecedores externos, O compartilhamento de recursos de TI em um ambiente público e de vários usuários acarreta melhores taxas de utilização e uma significativa redução de custos, enquanto mantém o acesso à tecnologia de alta qualidade. Em uma nuvem pública, uma organização opta por alugar recursos de TI ao invés de investir em sua própria infraestrutura física ou manter equipamentos periodicamente ociosos para ser capaz de suportar as cargas de pico de serviços. No caso da computação em nuvem pública, é possível lidar com isso, simplesmente escalando os recursos de TI de acordo com a necessidade e com custos diretamente proporcionais, evitando prejuízos.

Muitas organizações acabam adotando tanto a computação pública quanto a privada, integrando os dois modelos em uma nuvem híbrida. Esses modelos híbridos são voltados a atender negócios específicos e requisitos especiais de tecnologia, de forma que as atividades e tarefas são alocadas em nuvens internas, externas ou de TI tradicional, conforme se considera adequado, o que auxilia na otimização da segurança e da privacidade com um investimento fixo mínimo em recursos de TI.

Além dos diferentes modelos de computação em nuvem, existem também distinções entre os modelos de serviço de nuvem mais comuns, como exibido na Figura 1. Os modelos de serviços em nuvem estão disponíveis para qualquer um com acesso à Internet e incluem:

- Software como Serviço (SaaS): permite que o software seja fornecido através de servidores e distribuído por uma rede, sem requerer instalações ou implementações in loco
- Plataforma como Serviço (PaaS): permite que sistemas operacionais e serviços de middleware sejam fornecidos de fontes gerenciadas através da rede
- Infraestrutura como um Serviço (IaaS): permite que toda uma infraestrutura seja fornecida como um serviço através da rede, o que inclui capacidade de armazenamento, roteadores, sistemas virtuais, hardware e servidores.

Neste documento, focaremos nos modelos de computação em nuvem IaaS.

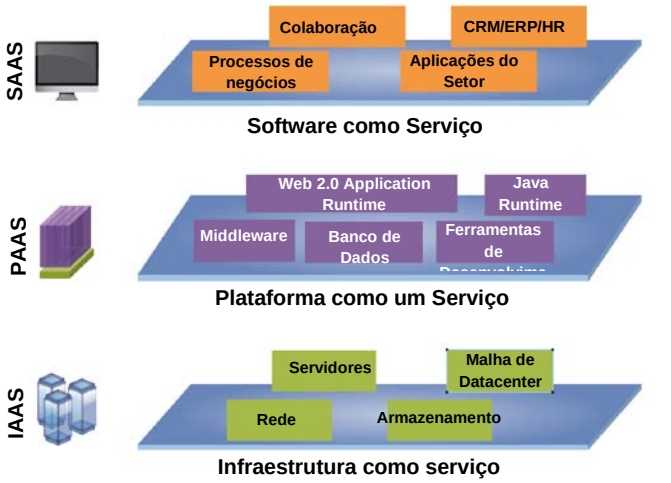

Figura 1. Modelos de computação em nuvem

A computação em nuvem e a segurança: o grande desafio

Apesar de a computação em nuvem transferir parte da gestão de dados e operações do cliente para o fornecedor da nuvem, da mesma forma que acontece quando as organizações confiam suas operações de TI a empresas terceirizadas, operar um ambiente baseado numa nuvem segura é uma responsabilidade compartilhada entre ambos. Mesmo as tarefas mais básicas, como aplicar correções e configurar a segurança da rede são responsabilidades tanto do provedor de serviços na nuvem quanto do cliente. Vamos examinar um exemplo.

Em um modelo IaaS, é responsabilidade do provedor da nuvem oferecer um número de máquinas virtuais pré-configuradas que constantemente são atualizadas com as últimas versões dos patches de segurança. Quando os clientes fornecem as máquinas virtuais, eles precisam confiar no provedor de nuvem para fornecer os sistemas de segurança. Os clientes não possuem acesso à camada do hypervisor (o sistema operacional subjacente que gerencia as máquinas virtuais que são executadas em uma máquina física) que tipicamente não compartilha a rede virtual com nenhuma outra máquina hospedada de forma a evitar invasões de outras redes. Os provedores de nuvem podem também oferecer uma rede virtual privada (VPN), um, opcional para que o cliente possa garantir uma rede protegida que esteja sujeita à ataques provenientes da rede aberta, a Internet. É de responsabilidade do cliente manter os patches atualizados em todas as máquinas virtuais fornecidas após a implantação inicial, assim comoa manutenção da configuração da VPN para proteger os dados e infraestrutura mais valiosos. Entretanto, se um cliente não optar pela aquisição de uma VPN ou não atualizar suas interfaces Web nas máquinas virtuais, as máquinas poderão ficar vulneráveis.

Se uma organização decide implementar tais mecanismos em uma nuvem privada usando o departamento de TI interno, ela poderá confiar nas suas políticas de negócio para governar os aspectos como confidencialidade de dados, controle de acessos a aplicações e sistemas, e assim por diante.

Os funcionários precisam observar e obedecer às diretrizes regulatórias e internas. Além disso, também serão encarregados de lidar com a infraestrutura de TI pois normalmente são certificados de acordo com as políticas de negócio. Nesse contexto, as organizações precisam lidar com os riscos de acesso privilegiado a usuários não autorizados, prevenção de perda de dados, invasão maliciosa e erros não intencionais de usuários.

Se a organização decide implementar tais mecanismos em uma nuvem pública utilizando o provedor de nuvem discutido no exemplo acima, ela poderá confiar nos acordos de negócio que governam esses mesmos aspectos, conforme explicado no exemplo anterior (nuvem privada). De uma forma ou de outra, essas organizações também precisam lidar com os mesmos riscos e diretrizes regulatórias.

As organizações precisam estabelecer um relacionamento de confiança com seus provedores de computação em nuvem e compreender, antes de optar por uma ou outra abordagem, os riscos em relação a como esses provedores implementam, implantam e gerenciam a segurança em nome delas. Esse relacionamento *trust-but-verify* entre os provedores de serviço de nuvem e clientes (de confiança porém certificado) é crítico já que os clientes dos serviços na nuvem são os principais responsáveis pela conformidade e proteção de seus dados mais importantes, mesmo que nas movimentações do *workloads* pela nuvem.

Outros aspectos da computação em nuvem também exigem uma avaliação mais profunda dos riscos à segurança Na nuvem, é difícil localizar fisicamente onde um dado está armazenado. Processos de segurança que uma vez eram visíveis, agora são ocultos por entre camadas de abstração. Essa falta de visibilidade pode levantar uma série de questões de conformidade e segurança e pode limitar a utilização dos recursos de TI em uma nuvem estritamente pública, por exemplo. Os clientes precisam se certificar de selecionar um ponto para a alocação física de uma implantação de nuvem pública e que os contratos garantam o armazenamento dos dados desta localidade.

O compartilhamento em massa da infraestrutura na nuvem precisa de uma abordagem diferenciada em relação à que é necessária nos ambientes de TI tradicionais. É comum que diversas organizações com níveis variados de exigências de segurança interajam em um mesmo conjunto de recursos. computação em nuvem. Ao mesmo tempo, o balanceamento de carga de trabalho, a alteração de acordos de nível de serviço e outros aspectos do ambiente de TI dinâmico atual criam cada vez mais oportunidades para a desconfiguração, comprometimento de dados e conduta maliciosa.

O compartilhamento de infraestrutura também requer um alto grau de padronização e automatização de processos, o que aumenta a segurança ao eliminar o risco de erros do operador e as distrações. De qualquer forma, os riscos inerentes à infraestrutura massivamente compartilhada existem e requerem que os modelos de computação em nuvem tenham cuidado especial com as questões de isolamento, identidade e conformidade.

Outro requisito crítico é proteger o ambiente de produção da aplicação contra falhas. Isso significa ter o cuidado para que uma aplicação esteja disponível e acessível ininterruptamente.

Aplicando o Framework de Segurança IBM nos negócios com ambientes na nuvem

Para proteger seus processos de negócio, uma organização precisa ter uma abordagem holística e sinérgica para garantir que todos os domínios de segurança trabalhem alinhados com os objetivos do negócio. Caso contrário, a falta de alinhamento de prioridades entre TI e a estratégia da organização levam a um aumento da vulnerabilidade e dos ricos aos quais a empresa está exposta. Utilizar uma abordagem com base em padrões para mapear os negócios e fazer uma varredura de segurança de TI é muito difícil e, muitas vezes, considerada uma atividade de segundo plano.

A IBM desenvolveu uma estrutura abrangente (como mostrado na Figura 2) para melhor compreender os aspectos da segurança empresarial em termos de recursos que precisam ser protegidos e examinou os diferentes domínios de um ponto de vista de negócios. Nas próximas seções, abordaremos esta estrutura de forma mais detalhada para demonstrar os diferenciais de uma arquitetura de segurança holística além de como aplicar os requisitos de segurança da computação em nuvem.

Figura 2. O Framework de Segurança IBM

Controle de segurança, gerenciamento de risco e conformidade

As organizações precisam prover visibilidade em relação à segurança de suas nuvens. Isso inclui ampla visibilidade do gerenciamento de incidentes, de imagens e de mudanças, assim como da comunicação dos incidentes para os usuários e dos dados de auditoria.

A visibilidade pode ser especialmente crítica para os que buscam alcançar a conformidade. O Sarbanes-Oxley Act, o Health Insurance Portability and Accountability Act (HIPAA), as leis europeias e muitos outros regulamentos requerem recursos de auditoria abrangentes. Uma vez que as nuvens públicas são, por definição, uma caixa preta, os assinantes em potencial podem não ter como controlar a conformidade: (uma nuvem híbrida ou privada, por outro lado, pode ser configurada para atender tais requisitos).

Além disso, os provedores algumas vezes são requisitados para apoiar auditoria de terceiros, e seus clientes podem ser direcionados para suporte e-Discovery e investigações forenses quando suspeita-se de uma brecha. Esse requisito adiciona ainda mais importância ao manter a visibilidade adequada na nuvem.

No geral, as organizações costumam citar também a necessidade de acordos de nível de serviço flexíveis (SLAs) que possam ser adaptados a situações específicas, alavancando as experiências com os serviços terceirizados gerenciados tradicionais.

Pessoas e identidade

As organizações precisam garantir que usuários autorizados por todas as empresas e cadeias de suprimentos tenham acesso aos dados e ferramentas necessárias, no momento que precisam, enquanto bloqueiam aqueles que não possuem autorização para acesso. Normalmente, ambientes de nuvem oferecem suporte a uma grande variedade de comunidades de usuários, então esses controles são muito importantes. Além disso, as nuvens apresentam uma nova camada de usuários com privilégios: os administradores que trabalham para o provedor da nuvem. O monitoramento de usuário com privilégios, que inclui as atividades de registro, se tornou uma importante necessidade. Esse tipo de monitoramento deve incluir verificações de monitoramento físico e verificação de segundo plano.

A identificação de federações e recursos de ambientação rápidos deve estar disponível para coordenar a autenticação e autorização em sistemas de terceiros ou de back-end da empresa. É necessário um recurso de conexão única com base em padrões para simplificar o login de usuários em aplicativos hospedados internamente e na nuvem. Isso permite uma otimização simples e rápida dos serviços de nuvem.

Dados e informações

Muitas organizações mencionam que a proteção de dados é a questão de segurança mais importante. As preocupações típicas incluem a maneira que os dados são armazenados e acessados, os requisitos de conformidade e auditoria, as questões de negócios que envolvem o custo das violações de dados, os requisitos de notificação e os danos ao valor da marca. Todos os dados confidenciais ou regulamentados precisam ser devidamente separados na infraestrutura de armazenamento de nuvem, incluindo os dados arquivados.

A criptografia e o gerenciamento de chaves de criptografia de dados que estão sendo transferidos para a nuvem ou dados armazenados no datacenter do provedor de serviço são essenciais para proteger a privacidade dos dados e o gerenciamento de autorizações de conformidade. A criptografia de mídia móvel e a capacidade de compartilhar de forma segura as chaves de criptografia entre o provedor de serviços de nuvem e do cliente é importante, mas muitas vezes é esquecida. A forma de mover grandes volumes de dados de forma rápida e econômica pela Internet ainda não é exatamente prática. Em muitas situações, as organizações precisam enviar mídias móveis como uma fita de arquivamento para o provedor da nuvem. É essencial que os dados sejam criptografados e apenas o provedor da nuvem e o cliente tenham acesso às chaves de criptografia.

Restrições importantes relacionadas à localização dos dados podem surgir com a computação em nuvem, dependendo do local da organização, do tipo de dados que ela gerencia e da natureza de seus negócios. Vários estados que fazem parte da União Europeia (UE), por exemplo, proíbem expressamente que informações confidenciais de seus cidadãos sejam divulgados em outros países.

Além disso, a implementação da nuvem pode levantar polêmicas sobre violação de leis de exportação relativas à informações criptografadas e à propriedade intelectual. A assessoria jurídica da organização deve revisar todos os requisitos antes da implementação da nuvem e certificar-se de que a empresa é capaz de controlar a localização geográfica dos dados na infraestrutura do provedor.

As indústrias como as de serviços públicos e financeiros possuem variados tipos de usuários e dados classificados em diferentes níveis de e precisam manter essa classificação de dados na nuvem para poder regulamentar os acessos, a forma como os dados são criptografados e arquivados e também como as tecnologias são utilizadas para evitar a perda de dados.

Aplicativos e processos

Normalmente, os clientes consideram os requisitos de segurança de aplicações de nuvem em termos de segurança de imagem. Todos os requisitos de segurança de aplicativo típicos servem para aqueles aplicativos que se encontram na nuvem, mas também se aplicam para as imagens que hospedam os aplicativos. O provedor da nuvem precisa acompanhar e oferecer suporte a um processo de desenvolvimento seguro. Além disso, os usuários da nuvem precisam de suporte para a gerar as imagens, licenciamento e controle de uso. A suspensão e destruição das imagens devem ser executadas com cuidado, assegurando que os dados confidenciais das mesmas não sejam expostos.

Definir, verificar e manter o nível de segurança das imagens de acordo com as políticas de segurança específicas do cliente é um requisito importante, principalmente nos setores mais regulamentados.

As empresas precisam garantir que os serviços da Web que elas publicam na nuvem sejam compatíveis com os níveis de segurança exigidos e atendam às políticas de negócios. Desenvolver melhores práticas de segurança é um requisito fundamental.

Rede, Servidor e Terminal

No ambiente de nuvem compartilhada, os clientes querem garantir que todos os domínios arrendatários estejam devidamente isolados e que não exista a possibilidade de dados ou transações vazarem de um domínio para o outro. Para ajudar a alcançar isso, os clientes precisam ter a possibilidade de configurar domínios virtuais de confiança ou zonas de segurança com base em políticas.

Conforme os dados saem do controle dos clientes, eles esperam que o ambiente possua recursos como detecção de invasão e sistemas de prevenção. A preocupação não se limita às invasões em domínios virtuais de clientes, mas também ao possível vazamento e roubo de dados além do mau uso dos domínios para ataque de terceiros. Ao passar a responsabilidade pelos dados para prestadores de serviços externos, aumenta a preocupação sobre os ataques de negação de serviço com base em Internet (DoS) e negação de serviço distribuída (DDoS).

Em ambientes compartilhados, todas as partes devem estar de acordo com suas responsabilidades para revisar regularmente os dados. A empresa deve assumir a responsabilidade em termos de gerenciamento de contratos referentes a avaliações de risco ou eventual implementação de controles.

Nos locais em que os catálogos de imagens são fornecidos pelo provedor de nuvem, os clientes precisam que essas imagens estejam seguras e devidamente protegidas contra corrupção e irregularidades. Em muitos casos, os clientes esperam ainda que estas imagens sejam autorizadas e protegidas por criptografada.

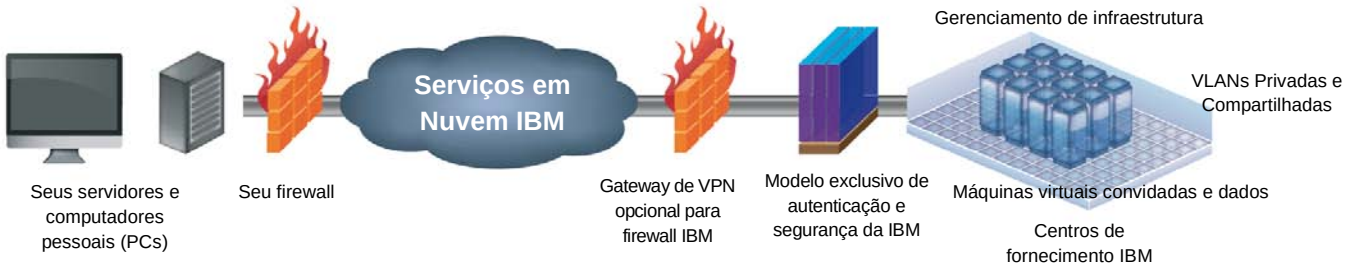

Figura 3. Uma visão conceitual da oferta do IBM SmartCloud Enterprise

Infraestrutura física

A infraestrutura da nuvem, juntamente com servidores, roteadores, dispositivos de armazenamento, fontes de alimentação e outros componentes que oferecem suporte às operações, devem ser protegidos também fisicamente. Essa proteção inclui o controle adequado e o monitoramento de acesso físico utilizando medidas de controle de acesso biométrico e monitoramento de circuito fechado de televisão (CCTV). Os provedores precisam expor claramente como o acesso físico para os servidores que hospedam as cargas de trabalho ou oferecem suporte de dados ao cliente são gerenciados.

IBM SmartCloud Enterprise

A oferta do IBM SmartCloud Enterprise é uma solução IaaS em nuvem projetada para fornecer acesso ágil e rápido aos recursos de TI em a uma base "pay-per-use", com características e funções desenvolvidas especialmente para atender as necessidades dos clientes corporativos. Estas necessidades incluem recursos com capacidade reservada, funções de administração de conta, rapidez de imagem e conectividade VPN para recursos de nuvem. Um amplo portfólio de produtos e serviços on demand ajuda a atender às mais diversas exigências dos clientes como, por exemplo, disponibilidade, segurança e com um sistema de gerenciamento de serviços integrados na nuvem para fornecer visibilidade, controle e automação.

O acesso ao portal de autoatendimento de infraestrutura e à interface de programação de aplicativos (API) é restrito a usuários que possuem uma IBM Web Identity. A infraestrutura está em conformidade com as políticas de segurança da IBM, incluindo varreduras de segurança regulares além de ações e operações administrativas controladas. Nos centros de distribuição da IBM, os dados do cliente e as máquinas virtuais são mantidos no datacenter, onde a segurança física é a mesma dos datacenters internos da IBM. A opção VPN da IBM permite que os clientes isolem seus ambientes no IBM SmartCloud Enterprise em uma rede local virtual (VLAN) que pode ser acessada somente pelos clientes. Veja a Figura 3 para obter uma visão conceitual da oferta.

Provedores de computação em nuvem e você: uma responsabilidade compartilhada

Conforme mencionado acima, os acordos de negócio de computação em nuvem dependem de uma responsabilidade compartilhada no que se refere a operações e medidas de segurança. As responsabilidades da IBM se baseiam em modelos operacionais de segurança complexos que foram projetados de forma a incluir a segurança física e o gerenciamento de hardware no hypervisor. Entre as responsabilidades do cliente estão o gerenciamento do controle adequado de acessos ao portal web da nuvem, a operação segura e o fortalecimento dos sistemas operacionais adotados, a escolha de uma implementação segura para uma rede privada virtual e a implementação dos mecanismos adequados para o controle de dados. A Figura 4 ilustra essas responsabilidades de maneira detalhada.

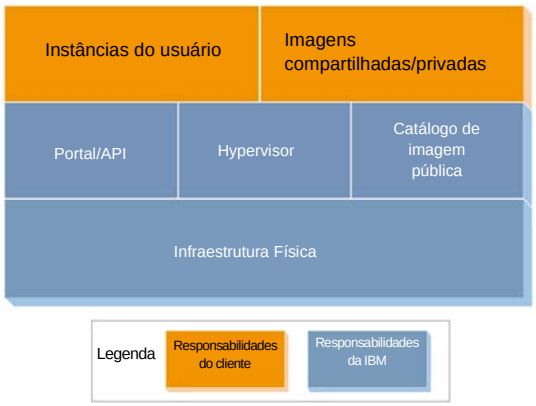

Figura 4. Abordagem de responsabilidade compartilhada

Primeiro, veremos as responsabilidades da IBM

Como mencionado acima, a IBM possui a responsabilidade pela infraestrutura física que compõe o ambiente SmartCloud Enterprise, o hypervisor e os componentes relacionados.

- **A segurança física dos componentes de nuvem IBM**
  A IBM possui um importante histórico de datacenters e negócios de hospedagem, em diversos localidades, pelo mundo todo. Hoje, a oferta do IBM SmartCloud Enterprise trabalha com os sites dos Estados Unidos, Canadá, Alemanha, Japão e Singapura, aproveitando a experiência, as ferramentas e as abordagens que a IBM já possui para a segurança física. Os exemplos incluem, mas não se limitam a:
  - Circuito fechado de televisão digital (CCTV) no datacenter, que registra imagens o tempo todo ou é acionado em determinados eventos (ativado por movimento). Os dados de vigilância CCTV costumam ser mantidos por pelo menos 30 dias.
  – Portas de acesso dos datacenters equipadas com alarmes sonoros locais.
  – Sistema de acesso baseado em computador (CAS) que usa leitores de cartões para restringir o acesso apenas àqueles com autorização para ter acesso às áreas controladas. Todas as entradas e saídas para essas áreas são monitoradas e registradas.
  – Segurança biométrica e por cartão estão presentes nos locais necessários. A função "anti-pass" (crachá), por exemplo, impede que vários usuários utilizem o mesmo cartão para entrar no datacenter central.
  – Projeto de instalações e proteção contra incêndios ajudam a prevenir falhas em cascata e de outros sistemas.
- **Gerenciamento de hardware e software no hypervisor**
  A IBM fornece gerenciamento e manutenção do ambiente de fornecimento, incluindo o hypervisor, a rede física e infraestrutura de hardware subjacente. Estes sistemas são gerenciados usando processos com base em Information Technology Infrastructure Library (ITIL). Os processos de gerenciamento de TI internos da IBM são rigorosamente aplicados e auditados internamente regularmente. Para gerenciar a infraestrurura, a IBM utiliza produtos e ferramentas internas disponíveis no mercado, incluindo ofertas de serviços como o IBM Managed Security Services para a proteção contra invasão e varreduras de vulnerabilidades. De acordo com o padrão adotado, a equipe da IBM e suas ferramentas não possuem acesso ou fazem a análise dos ambientes virtuais dos cliente, o que permite uma clara separação das funções entre a IBM e o cliente.
- **Segurança do portal de autoatendimento e APIs**
  Um usuário pode fornecer recursos para o ambiente do Enterprise SmartCloud de duas maneiras: por meio do portal de autoatendimento e das APIs do aplicativo. A infraestrutura usada para implementar esses pontos de entrada é instalada em locais da IBM segurados por meio de uma arquitetura com diversas camadas. Estes recursos estão sujeitos a rigorosos requisitos e processos de segurança internos da IBM que utilizam ofertas e produtos reconhecidos no mercado como o IBM Rational AppScan ®, para fazer a análise, monitoramento e gerenciamento dos aplicativos. A comunicação entre esses recursos e o cliente do consumidor (por exemplo, o navegador ou aplicativo personalizado integrado através das APIs) são protegidas por meio secure sockets layer (SSL) em protocolo de transporte de hipertexto (HTTP).

- **Catálogo de imagem pública**
  A IBM fornece um catálogo público de imagens de sistema operacional e de middleware. Estas imagens são criadas com a especificação dos nossos vendedores e empresas do IBM Software Group. O gerenciamento de patches das imagens fundamentais no catálogo é responsabilidade da IBM e adere aos padrões internos para implementação de correções relacionadas à segurança. Estas imagens são atualizadas regularmente e conforme surge a necessidade de correções importantes. Assim que o cliente fornece uma instância do catálogo do IBM SmartCloud Enterprise, ele se torna responsável por todo o gerenciamento de patches dessa instância em execução e por quaisquer imagens criadas a partir dessa instância.

Como parte do modelo de responsabilidade compartilhada entre a oferta IBM Enterprise SmartCloud, o cliente é esponsável por todos os aspectos de segurança dos recursos fornecidos no ambiente de nuvem. As seções abaixo demonstram esses recursos de forma mais detalhada.

- **Gerenciamento de identidade e controle de acesso**
  Para gerenciamento de identidade, o IBM SmartCloud Enterprise possui um sistema padrão Web Identity que a IBM desenvolveu e implementou para todos os usuários de sistemas ibm.com. Este sistema permite que os usuários criem e gerenciem IDs e incluam ferramentas para a manutenção de senhas.
  Uma vez que um cliente se inscreve para o serviço SmartCloud IBM Enterprise, o ID especificado durante o processo de assinatura é atribuído como o administrador da conta da empresa. Através do portal de autoatendimento do IBM SmartCloud Enterprise, o administrador pode adicionar, excluir e modificar IDs de usuários que podem ser utilizados para fornecer recursos de nuvem (instâncias, imagens, armazenamento etc). É responsabilidade do cliente gerenciar todos os IDs de usuário da conta com base em seus próprios requisitos (por exemplo, processo de aprovação para adicionar um ID, revalidação de IDs etc).

- **Sistema operacional convidado**
  O IBM SmartCloud Enterprise fornece um ambiente de autoatendimento para fornecimento de recursos em nuvem. A IBM usa uma política "sem contato" em todos os recursos fornecidos pelo cliente o que significa que, uma vez que um cliente fornece um recurso para a nuvem, ele passa a ser responsável pela segurança. Quando um cliente fornece uma instância (máquina virtual) no ambiente de nuvem do IBM SmartCloud Enterprise, ele recebe privilégios "root" ou "administrador" do sistema operacional convidado. Com esses privilégios, o cliente pode assegurar recursos fornecidos com base em suas necessidades internas ou padrões.

A lista a seguir contém as tarefas que cada cliente deve incluir no gerenciamento dos recursos provisionados. (Observação: esta lista não é universal e os clientes devem gerenciar seus recursos do sistema operacional em nuvem como fazem com os recursos contidos em seus próprios laboratórios).

- Gerenciamento de patches e correções de segurança: vendedores de sistemas operacionais atualizam seus produtos regularmente para se proteger de novas ameaças. O cliente controla o momento e o nível para a aplicação desses patches. A IBM sugere que os clientes monitorem regularmente os boletins de segurança dos fornecedores de sistemas operacionais, as atualizações e as correções para melhor atender às suas necessidades.
- Software adicional seguro: durante a instalação, configuração e gerenciamento de qualquer software no sistema operacional convidado, o cliente deve ter proteger adequadamente o software e quaisquer acessos ao sistema
- Criação e implementação de políticas de segurança no sistema operacional convidado, por exemplo:
  - Políticas de firewall do sistema operacional convidado
  - Proteção e distribuição de chaves de secure shell (SSH) do sistema operacional convidado
  - Criptografia de dados do sistema operacional
  - Escolha de software antivírus quando necessário
  - Remoção de pacotes e serviços que não são considerados necessários

- **Acesso à rede**
  Por padrão, cada instância (máquina virtual) fornecida no IBM SmartCloud Enterprise é atribuída a um ou mais endereços IP que podem ser roteados publicamente e acessados através da Internet. Como oferta opcional do IBM SmartCloud Enterprise, possuímos um serviço VPN. Cada VPN opcional fornece um túnel VPN com base em Internet Protocol Security (IPSec) entre um gateway que fornece suporte a IPSec de cliente e um datacenter IBM SmartCloud Enterprise. Com a opção VPN, o cliente recebe uma Rede de Área Local Virtual (VLAN) privada. Com essa opção, quando ele fornece uma instância, pode escolher entre fornecê-la na VLAN pública ou privada. A opção VPN provê ao cliente uma comunicação criptografada de dados na Internet e um nível adicional de isolamento com a rede virtual do SmartCloud IBM Enterprise. Desta forma, um cliente pode fornecer uma instância que abrange tanto a VLAN pública quanto a privada, o que possibilita maior flexibilidade na criação de arquiteturas de implementação em camadas na nuvem. Esta capacidade deve ser protegida usando firewalls de software (ou aqueles que são fornecidos com o sistema operacional e por terceiros) para limitar o acesso tanto do host quanto de porta.
- **Controle de dados**
  Como dito anteriormente, o acesso padrão ao sistema operacional da máquina virtual fornece todos os privilégios para os clientes. Como resultado, os clientes têm total controle sobre como os dados são tratados em seus ambientes de nuvem. Os clientes podem implementar qualquer ferramenta de software para mover dados e são responsáveis pela manutenção dessa ferramenta e administração de quaisquer controles de acesso. Os clientes podem considerar medidas adicionais de segurança para seus dados, como criptografia de sistema de arquivos. Como política, a IBM não move ou migra recursos fornecidos por um cliente de um datacenter para outro (por exemplo, imagens, armazenamento persistente etc). Quando os clientes fornecem um recurso, eles escolhem para qual datacenter ele será colocado. Esta política pode ser importante para os clientes que têm problemas de segurança com dados que circulam fora de determinadas localidades.
- **Alta disponibilidade**
  Depois de fornecer o ambiente de servidor virtual, os clientes podem instalar e configurar a alta disponibilidade. A alta disponibilidade é uma capacidade chave para as organizações que estão entrando para a computação em nuvem. Para garantir uma aplicação de alta disponibilidade na nuvem, é necessário atender um número de recursos como vulnerabilidade da rede, redundância e falha de armazenamento. Porém, uma das áreas mais importantes é failover de IP. Utilizar endereços IP virtuais para as máquinas virtuais pode permitir que clientes eliminem pontos específicos de falhas e projetem uma infraestrutura de TI altamente disponível.

Fornecendo alta disponibilidade para ambientes de nuvem

A exigência de proteção dos sistemas de TI ou aplicações contra falhas de qualquer dimensão não é nova e já é abordada em muitos produtos de software. No entanto, estes produtos de software são, em geral, incompatíveis com muitas das ofertas de nuvem e a maior parte dos provedores públicos de nuvem nem sempre fornecem a funcionalidade necessária. Nesse sentido, os usuários precisam complementar as implementações de nuvem com a arquitetura da alta disponibilidade fora dela.

Para atender a essas necessidades e preocupações em torno da alta disponibilidade de uma forma rica em segurança e mais oportuna, a oferta do IBM SmartCloud Enterprise adicionou suporte para endereços IP virtuais (vIPs) em instâncias na nuvem. Além de um endereço IP *estático* regular (que nunca muda) obtido por cada máquina virtual no momento de sua configuração, uma máquina pode assumir dinamicamente um ou vários endereços IP *virtuais* adicionais. Como o código da aplicação controla a associação entre os vIPs e as instâncias, a topologia da aplicação pode ajustar as falhas muito rapidamente, normalmente em menos de um segundo. A instalação e configuração de alta disponibilidade para o IBM SmartCloud Enterprise podem ser realizadas exclusivamente no seu ambiente fornecido de máquina virtual.

Como exemplo, pegue um par de máquinas virtuais, a Máquina Virtual A e a Máquina Virtual B, como mostrado na Figura 5. Cada máquina tem um endereço IP estático. Ambas as máquinas virtuais também estão configuradas para permitir a atribuição dinâmica de um endereço IP virtual, além do estático já existente.

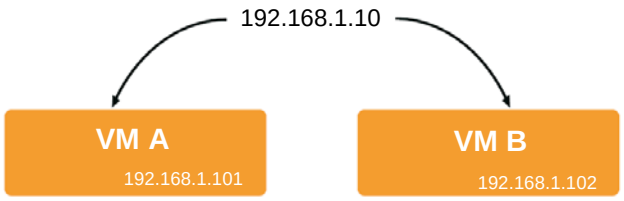

Figura 5. Além dos endereços IP estáticos as Máquinas Virtuais A e B podem aceitar o endereço IP virtual 192.168.1.10 durante o tempo de execução.

Os endereços IP estáticos são usados para administrar e manter as máquinas. O endereço IP virtual é aquele fornecido aos clientes, como o aplicativo publicado ou endereço IP do servidor.

Para começar, o endereço IP virtual é anexado à primeira máquina. Esta primeira máquina manipula todo o tráfego do serviço. A segunda máquina está em funcionamento e atua como espera média, como mostrado na Figura 6.

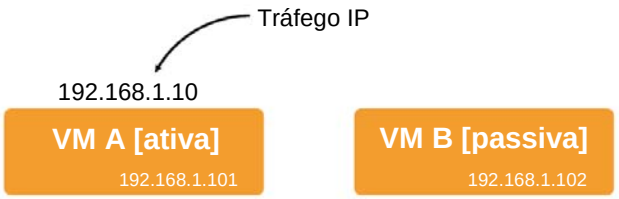

Figura 6. A configuração ativa/passiva: a Máquina Virtual A mantém o vIP e serviços de tráfego enquanto a Máquina Virtual B age como espera passiva.

Se a primeira máquina encontra um problema, lentidão ou falha, o endereço IP virtual é alternado para a segunda máquina. Agora, a segunda máquina atende todo o tráfego, enquanto a primeira máquina, uma vez reparada, se torna a próxima em espera, como mostrado na Figura 7.

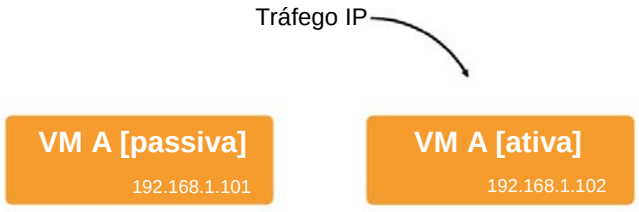

Figura 7. A configuração ativa/passiva: a Máquina Virtual VB assume o vIP e, agora, fornece todo o tráfego, enquanto a Máquina Virtual A age como espera.

O endereço publicado sendo o endereço estático significa que a falha e a alternação são praticamente imperceptíveis ao usuário final: a média é de alguns segundos até alguns minutos. Como o endereço IP virtual pode ser transferido entre diferentes máquinas muito rapidamente, com uma programação cuidadosa, é possível reduzir significativamente as interrupções não planejadas a partir da possibilidade do movimento do endereço IP no primeiro sinal de problemas.

Ao suportar IPs virtuais para máquinas virtuais, o IBM SmartCloud Enterprise pode ajudar a reduzir o tempo de inatividade do sistema em caso de falha da máquina virtual. Ao suportar IPs virtuais com máquina de backup virtual, o cliente pode ajudar a garantir que as interrupções sejam quase invisíveis para o usuário final.

Conclusão

Atualmente, a segurança é frequentemente listada como a preocupação número um dos clientes quando consideram a adoção da nuvem. As questões de segurança da nuvem lideram o ranking de preocupações dos clientes em relação à nuvem. Outros itens citados são a confiabilidade da nuvem, problemas de rede e preocupações com o retorno econômico do investimento. A segunda maior preocupação é a disponibilidade, um conceito que precisa ser trabalhado em quase todos os ambientes de TI.[1]

Para se beneficiar integralmente da computação em nuvem, os clientes devem garantir que os dados, aplicações e sistemas estejam devidamente protegidos, de forma que a infraestrutura de nuvem não exponha as organizações ao risco. A computação em nuvem vem com todos os requisitos habituais de disponibilidade e segurança de TI tradicionais, porém possui um nível adicional de risco e complexidade devido aos aspectos externos. Estes riscos demandam um quadro de segurança mais abrangente, que ajuda a garantir que todos os diferentes domínios de segurança trabalhem em conjunto de forma holística e sinérgica, em alinhamento com os objetivos de negócio globais.

A oferta IBM SmartCloud Enterprise é construída sobre competências, melhores práticas e ativos desenvolvidos por meio de anos de experiência no gerenciamento e operação de datacenters empresariais confiáveis e riquíssimos em segurança no mundo todo. A infraestrutura está em conformidade com as políticas de segurança da IBM, incluindo varreduras de segurança regulares e ações e operações administrativas controladas. Os dados do cliente e as máquinas virtuais são mantidos no datacenter de nossos centros de distribuição, onde são provisionados. A segurança física é a mesma aplicada nos datacenters internos da IBM.

O modelo IBM SmartCloud Enterprise não é uma solução padronizada, mas pode fornecer níveis adequados de segurança e disponibilidade para as necessidades específicas de cada organização na nuvem. Baseando-se em um amplo portfólio de serviços de consultoria, software, hardware e serviços de segurança gerenciados, o IBM SmartCloud Enterprise pode ajudá-lo a implementar com sucesso um ambiente de nuvem rico em segurança e com alta disponibilidade.

Para obter mais informações

Para saber mais sobre o IBM SmartCloud Enterprise ou sobre a implementação de um ambiente seguro na nuvem, entre em contato com um representante de marketing ou Parceiro de Negócios IBM ou acesse o site:
ibm.com/cloud/solutions/enterprise

Para saber mais sobre a implementação de um ambiente de nuvem seguro, consulte o IBM Red paper "Cloud Security Guidance - IBM Recommendations for Implementation of Cloud Security," REDP-4614, atibm.com/redbooks/abstracts/redp4614.html?Open

Para saber mais sobre a implementação de alta disponibilidade no ambiente do seu IBM Smart Cloud Enterprise, consulte o artigo do IBM developerWorks® “High availability apps in theIBMCloud” em **ibm.com/developerworks/cloud/library/cl-highavailabilitycloud.**

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produzido nos Estados Unidos da América
Junho de 2011

[1]"Cloud Computing Attitudes", IDC, Doc #223077, abril de 2010.

MSW03010-USEN-00