Fevereiro de 2012

Gerenciamento consolidado de segurança para nuvens no mainframe

Aproveitando o mainframe como hub de segurança para ambientes de computação em nuvem

IBM

Índice

Introdução

As organizações de hoje lutam com a expansão da computação distribuída, o aumento da colaboração online, o crescimento explosivo dos dados e ambientes de TI heterogêneos – problemas que tornam a segurança da informação mais crítica e mais complexa do que nunca. A movimentação de dados para um ambiente virtualizado e com base em nuvem pode ajudar a desenvolver e gerenciar uma infraestrutura mais flexível, bem como a reduzir os custos operacionais e o custo total de propriedade. Além disso, um ambiente virtualizado pode ajudar a acelerar o prazo de lançamento no mercado por meio de maior eficiência e automação; escalar operações para atender à dinâmica do mercado e às estratégias de negócios; e praticamente eliminar o tempo de inatividade. A dúvida não é, portanto, se a nuvem deve ser movida – mas sim como movê-la protegendo os dados críticos. Não surpreende o fato de que o nível de segurança dos dados depende principalmente da plataforma que oferece suporte ao ambiente de nuvem.

O mainframe tem um legado forte, pois é uma plataforma extremamente segura para ambientes e cargas de trabalho virtuais, além de oferecer uma alternativa atraente aos ambientes com extensão horizontal extensa muitas vezes implementados na nuvem – especialmente no domínio da segurança.

Ademais, muitas organizações já estão utilizando um mainframe como hub de dados para executar os principais aplicativos, o que proporciona um ponto de partida natural para criar um hub de segurança para a empresa inteira.

Desde a automação até tecnologias de virtualização avançada e padrões abertos de segmento de mercado, os mainframes IBM System z® ajudam a fornecer uma base sólida e segura para o desenvolvimento do ambiente virtual. Eles dão suporte a ambientes de nuvem expansíveis com segurança líder no segmento de mercado, além de disponibilidade, desempenho e custo reduzido. Tais benefícios são especialmente valiosos no planeta mais inteligente atual, onde negócios instrumentados, interconectados e inteligentes coletam, processam, utilizam e armazenam mais informações do que nunca.

Percebendo os benefícios das nuvens no mainframe

Além de muitos motivos tradicionais para escolher o mainframe em detrimento de outras plataformas de hardware – entre eles, segurança, confiabilidade e cargas de trabalho consolidadas –, há exemplos reais que demonstram por que as organizações implementam ambientes virtualizados em plataformas System z:

- Uma organização já tinha um mainframe em seu datacenter para executar cargas de trabalho de clientes. Queria manter a base com habilidades de mainframe e migrar cargas de trabalho de fora do mainframe para Linux no System z.
- Outra organização desejava oferecer software com base em nuvem como serviço a seus clientes. Seus cálculos revelaram que o custo de implementar o middleware IBM no mainframe seria inferior em relação a outras plataformas.
- Uma terceira organização queria fornecer hosting para cargas de trabalho de clientes em uma nuvem com base em mainframe. Como já utilizava mainframe, desejava proteger sua base de hosting para cargas de trabalho mediante a oferta de um ambiente de nuvem no System z.

Abordando preocupações de segurança na nuvem

Mais do que nunca, as organizações estão lidando com a necessidade de proteger dados críticos em ambientes distribuídos, colaborativos e de multiplataformas. Embora os benefícios operacionais e de capital da computação em nuvem sejam claros, também é evidente a necessidade de desenvolver uma segurança adequada para as implementações de nuvem. Trata-se de uma preocupação justificável. Segundo a IBM X-FORCE® Research & Development, os ataques estão se tornando mais sofisticados e mais comuns. Em meados de 2011, a X-Force relatou que o úmero de vulnerabilidades críticas já havia excedido o total para o ano de 2010.[1]

As mesmas características que tornam o mainframe ideal para a execução de aplicativos críticos – hardwares robustos, sistemas operacionais confiáveis, recursos de gerenciamento de sistemas com força de segmento de mercado e segurança de confiança – podem ser usadas para ativá-lo como um hub de segurança c orporativo. Tais recursos se estendem a ambientes virtualizados.

A segurança é criada em todos os níveis da estrutura do System z, desde o processador, hypervisor e sistema operacional até a c omunicação, armazenamento e aplicativos. O hosting de cargas de trabalho virtuais e ambientes de nuvem em um mainframe System z que executa soluções de software IBM pode abordar cada uma das preocupações de segurança a seguir, além de oferecer muito mais benefícios que riscos:

Controle

Muitas organizações não se sentem confortáveis com a ideia de nuvens públicas, pois suas informações residem em sistemas que não controlam. Entretanto, ambientes mainframe de nuvem típicos permitem aos usuários implementar sua própria "nuvem privada", o que proporciona mais controle. Ademais, esses ambientes podem oferecer um grau elevado de transparência na segurança, ajudando os usuários a ter uma visão melhor da empresa e deixando-os mais tranquilos.

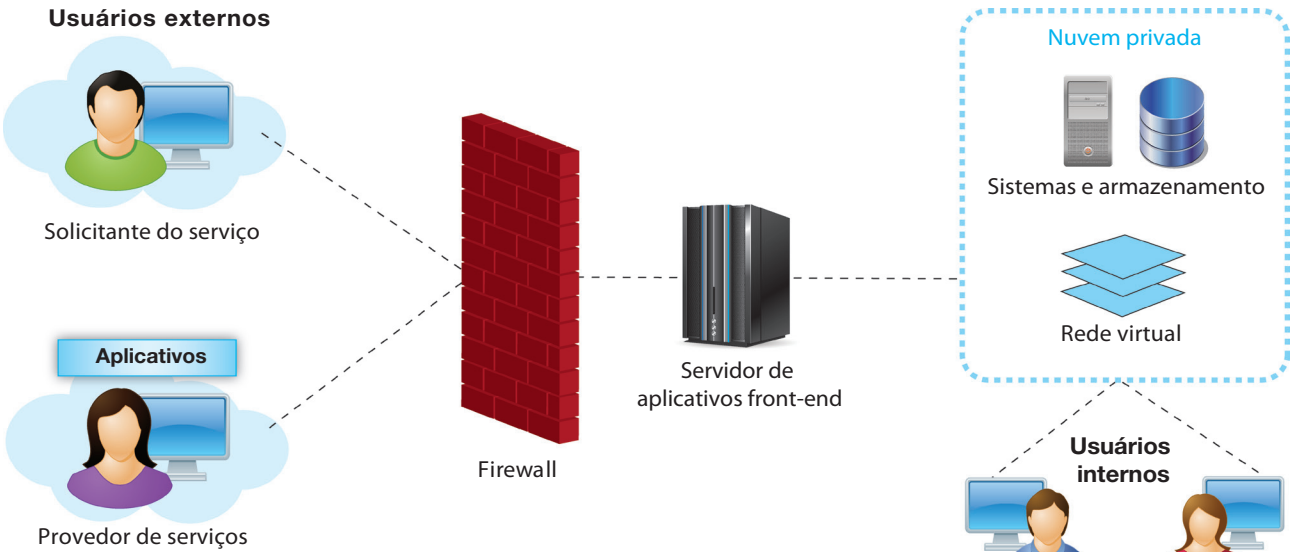

Figure 1: Implementações de nuvem precisam de segurança igual ou melhor que a de implementações tradicionais.

Migração

Enquanto migrar cargas de trabalho para a rede compartilhada e a infraestrutura de cálculo de uma nuvem pública pode aumentar a possibilidade de exposição não autorizada, a migração para ambientes mainframe de nuvem é capaz de fornecer tecnologias críticas de autenticação e acesso para proteger os dados. O gerenciamento de acesso e de identidade é fundamental para a segurança da nuvem, uma vez que limita o acesso a dados e aplicativos somente a usuários autorizados e apropriados. Limitar quem pode visualizar e manipular os dados ajuda a assegurar que não sejam manipulados incorretamente.

Confiabilidade

A alta disponibilidade é, compreensivelmente, uma questão importante para os departamentos de TI, que precisam prevenir a perda ou degradação de serviços em caso de indisponibilidade. Além disso, aplicativos críticos não podem ser executados na nuvem sem fortes garantias de disponibilidade. Uma das características dos mainframes é sua alta disponibilidade, que transforma os ambientes mainframe de nuvem em plataformas extremamente estáveis e seguras. Isso pode ajudar os clientes a utilizarem o mainframe como uma plataforma de hosting bastante escalável e confiável para dar suporte a diversas cargas de trabalho de clientes simultaneamente.

Gerenciamento fácil

Ambientes mainframe de nuvem podem oferecer controles visuais fáceis para gerenciar as configurações de firewall e segurança em aplicativos e ambientes de execução na nuvem. Isso pode reduzir os custos de gerenciamento de TI, economizando dinheiro no longo prazo. Um estudo interno da IBM constatou que o custo total de propriedade (TCO) geral ao longo de três anos para uma nuvem privada com base em sistemas IBM zEnterprise era 76% menor em relação à nuvem pública de um provedor de serviços terceiro. Isso se deve às cargas de trabalho consolidadas e virtualizadas, bem como a uma área de cobertura menor, que equivale a menos custos com hardware e software.

Conformidade

A conformidade com a Lei Sarbanes-Oxley (SOX), a Lei da Portabilidade e Prestação de Contas em Seguro-Saúde (HIPPA) e outros regulamentos pode limitar ou até mesmo proibir o uso de nuvens em alguns aplicativos. Felizmente, ambientes mainframe de nuvem podem fornecer recursos abrangentes de auditoria para compensar esse risco.

O System z tem recursos de segurança desenvolvidos especificamente para ajudar os usuários a se manterem em conformidade com requisitos regulamentares associados à segurança, incluindo gerenciamento de identidade e acesso; criptografia de hardware e software; recursos de segurança da comunicação; e criação extensiva de log e relatórios de eventos de segurança.

Benefícios gerais para ambientes mainframe em nuvem

Além dos benefícios de segurança, existem muitas outras razões para considerar a implementação de ambientes virtuais em servidores maiores e com expansão vertical, como o System z.

O System z oferece até 100% de utilização da CPU, além de uma arquitetura "com tudo compartilhado" que pode servir de host para milhares de cargas de trabalho mistas. Ele também pode ativar um datacenter mais eficiente, pois consome menos energia e precisa de menos refrigeração, ocupa menos espaço físico e tem menos peças para gerenciar.

Ademais, existem vantagens de preço atraentes. Clientes IBM economizaram até 70% em despesas de auditoria e até 30% com a redução de chamadas no help desk; além disso, tiveram custos administrativos 52% menores ao usarem o System z como plataforma para seu ambiente de nuvem.

O System z oferece todos os componentes necessários para fornecer a nuvem hoje, incluindo:

- Gerenciamento da carga de trabalho – Gerencie os requisitos de capacidade da infraestrutura de nuvem de maneira consistente com as políticas de negócios.
- Processamento de transações – Dê suporte à integração da nuvem com aplicativos críticos online para o processamento de transações.
- Escalabilidade – Escale verticalmente com o IBM z/OS® e partições lógicas (LPARs) e horizontalmente com Linux no System z e IBM z/VM® acoplado com o IBM Workload Manager.
- Disponibilidade e fornecimento – Use a automação para implementar máquinas virtuais e aplicativos de recuperação.
- Auditoria e métricas – A prestação de contas e a medição com base na carga de trabalho oferecem suporte ao planejamento de capacidade e ao estorno na linha de negócios.

Além disso, o mainframe dá suporte a padrões de segurança de segmento de mercado que ajudam a assegurar a interoperabilidade; estes incluem Infraestrutura de Chave Pública, Linguagem de Marcação Extensível para Controle de Acesso OASIS, Protocolo de Interoperabilidade para Gerenciamento de Chaves OASIS e muito mais.

Otimizando – e protegendo – plataformas virtualizadas

O suporte do mainframe para ambientes virtualizados multiarquiteturais permite que os clientes executem uma grande variedade de cargas de trabalho. Isso significa que os usuários podem incluir processadores, blades e muito mais de maneira rápida e fácil, além de automatizar configurações de hypervisor e rede a fim de reduzir o tempo manual necessário para colocar um ambiente de servidor virtual em operação. Depois de otimizar a plataforma virtual, fica mais fácil consolidar as cargas de trabalho devido à área de cobertura menor; ao sistema menor; às taxas de licenciamento mais baixas; e aos recursos de consolidação de dados.

Figure 2: Aproveite um ambiente mainframe para otimização de TI, consolidação de carga de trabalho e computação em nuvem.

Escolhendo a segurança IBM para computação mainframe em nuvem

Para otimizar a segurança corporativa, precisa haver um alto nível de planejamento e avaliação com o objetivo de identificar os riscos nas principais áreas de negócios. Essa estrutura de segurança inclui pessoas, processos, dados e tecnologias por toda a sequência contínua de negócios. Tal abordagem holística pode facilitar uma blueprint e uma estratégia de segurança acionadas por negócios que funcionem como uma defesa efetiva para a organização inteira.

A IBM pode ajudar. Nossas soluções de segurança fornecem recursos de segurança abrangentes, integrados e de ponta a ponta nos mainframes, o que permite que as empresas consolidem seu gerenciamento de segurança e aproveitem o mainframe como seu hub de segurança corporativo.

Figure 3: Trate a segurança de forma holística usando o IBM Security Framework.

IBM Resource Access Control Facility

O IBM Resource Access Control Facility (RACF®) é um produto de ponta para proteger os dados corporativos mais valiosos. Trabalhando junto com o sistema operacional, esse programa IBM licenciado que é líder no segmento de mercado pode aumentar a segurança dos dados ao proteger recursos vitais dos sistemas e controlar o que os usuários podem fazer no sistema operacional. O RACF concede acesso aos recursos protegidos somente para usuários autorizados. Depois de identificar e autenticar o usuário, ele controla a interação entre o usuário, recursos do sistema, recursos de comunicação, programas e aplicativos. Também fornece recursos administrativos e de auditoria detalhados.

Conjunto IBM Security zSecure

O conjunto IBM Security zSecure oferece administração de segurança com custo reduzido, melhora os serviços mediante a detecção de ameaças e reduz os riscos com relatórios automatizados de auditoria e conformidade. As ferramentas a seguir, em especial, conseguem aprimorar os ambientes mainframe de nuvem:

- **Security zSecure Audit** – Esta solução de conformidade e auditoria permite aos usuários analisar e relatar automaticamente eventos de segurança, além de detectar exposições de segurança
- **Security zSecure Admin** – Permite a administração mais efetiva do RACF, utilizando uma quantidade significativamente menor de recursos
- **zSecure Manager para RACF z/VM** – Oferece auditoria e administração combinadas para o RACF no ambiente da máquina virtual (VM)

Tivoli Federated Identity Manager (para Linux no System z)

O IBM Tivoli® Federated Identity Manager é uma solução de controle de acesso baseada em padrões para conexão única federada e gerenciamento de confiança em serviços da web e ambientes de arquitetura orientada a serviços (SOA). Manipula todas as informações de segurança para uma federação – incluindo relações de parceiros, mapeamento de identidade e gerenciamento de token de identidade, entre outros.

Tivoli Identity Manager (para Linux no System z)

O IBM Tivoli Identity Manager é uma solução automatizada com base em políticas que gerencia o acesso do usuário em ambientes e TI, seja em um ambiente corporativo fechado ou em uma empresa virtual ou estendida. Por meio do uso de funções, contas e permissões de acesso, ajuda a automatizar a criação, modificação e rescisão dos privilégios de usuário em todo o ciclo de vida do usuário.

Tivoli Access Manager para e-business (para Linux no System z)

O software Tivoli Access Manager para e-business é uma solução extremamente escalável de autenticação de usuário, autorização e SSO na web que permite impingir políticas de segurança sobre uma grande variedade de recursos da web e aplicativos. Centraliza o gerenciamento do acesso de usuários para portal online e iniciativas de negócios.

IBM Security Key Lifecycle Manager (para z/OS)

O IBM Security Key Lifecycle Manager para z/OS gerencia chaves de criptografia para armazenamento, simplificação da implementação e manutenção da disponibilidade para dados em repouso de forma nativa, em ambientes mainframe do System z. Além disso, simplifica o gerenciamento de chaves e a geração de relatórios de segurança com o objetivo de proteger a privacidade dos dados e cumprir com os regulamentos de segurança.

IBM InfoSphere Guardium Database Security

O IBM InfoSphere® Guardium® Database Activity Monitor oferece uma solução simples e robusta para monitorar continuamente o acesso a bancos de dados e automatizar os controles de conformidade em empresas heterogêneas. A solução impede atividades não autorizadas por parte de pessoas com acesso a informações privilegiadas ou hackers, ao mesmo tempo em que monitora usuários finais para identificar fraudes sem quaisquer mudanças em bancos de dados, aplicativos ou desempenho impactante. Use esta solução para implementar controles centralizados e padronizados visando segurança e monitoramento de banco de dados em tempo real, auditoria de baixa granularidade de bancos de dados, geração automatizada de relatórios de conformidade, controle de acesso no nível dos dados, gerenciamento da vulnerabilidade dos bancos de dados e autodescoberta de dados sensíveis.

IBM Proventia Server Intrusion Prevention System (para Linux no System z)

O IBM Proventia® Server Intrusion Prevention System para Linux utiliza criação de firewalls para hosts e inspeção profunda de pacotes de rede para identificar e bloquear milhares de ameaças conhecidas e emergentes, focando em vulnerabilidades nos sistemas operacionais, aplicativos de clientes e aplicativos da web – tudo isso enquanto proporciona reconhecimento situacional em tempo real e inteligência aos administradores de segurança.

Conclusão

À medida que os problemas econômicos dão mais importância à redução dos custos operacionais e as necessidades de segurança aumentam, fica evidente a oportunidade de aproveitar o mainframe para proporcionar eficiências operacionais, assim como uma segurança excelente. Isso é verdadeiro especialmente em ambientes virtualizados, nos quais os mainframes mostraram que são bases fortes e seguras para a criação de infraestruturas de nuvem.

O System z pode ajudar a proteger os dados principais e aplicativos críticos essenciais, ao mesmo tempo em que permitem que os usuários virtualizem e compartilhem tais componentes em um ambiente seguro e flexível. Tire proveito das eficiências inerentes ao System z para implementar um ambiente virtualizado utilizável e escalável que possa oferecer disponibilidade, desempenho e r edução de custos superiores.

Para mais informações

Para saber mais sobre a computação em nuvem no IBM System z, entre em contato com seu representante ou Parceiro de Negócios IBM ou visite http://event.on24.com/r.htm?e=322059&s=1&k=42285CDCC0D5EA69BC2C885FB5F2C394 para acessar o webcast "Consolidated Security Management for Mainframe Clouds".

Sobre a Segurança IBM

O portfólio de segurança da IBM proporciona a inteligência de segurança necessária para ajudar as organizações a protegerem de forma holística seu pessoal, infraestruturas, dados e aplicativos. A IBM oferece soluções para gerenciamento de identidade e acesso, segurança de banco de dados, desenvolvimento de aplicativos, gerenciamento de risco, gerenciamento de terminal e segurança de rede, entre outros. A IBM administra a maior organização de pesquisa e desenvolvimento e a maior organização de fornecimento do mundo. Isso inclui nove centros de operações de segurança, nove centros de Pesquisa IBM, 11 laboratórios de desenvolvimento de segurança para softwares e um Instituto de Segurança Avançada, com escritórios nos Estados Unidos, Europa e Ásia-Pacífico. A IBM monitora 13 bilhões de eventos de segurança por dia em mais de 130 países e possui mais de 3.000 patentes de segurança.

Para mais informações sobre a segurança IBM, visite:
ibm.com /security

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produzido nos Estados Unidos da América
Fevereiro de 2012

[1] IBM Security Solutions Executive Summary, “IBM X-Force 2011 Mid-year Trend and Risk Report: CIO Security Priorities”. Setembro de 2011. O relatório completo pode ser acessado aqui: http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGL03009USEN&attachment=WGL03009USEN.PDF

Recicle

TIW14125-USEN-00