Segurança IBM
Liderança de Pensamento White Paper

Fevereiro de 2012

Gerenciamento de segurança consolidada para nuvens de mainframe

Alavancando o mainframe como um hub de segurança para ambientes de computação em nuvem

Índice

Introdução

As organizações atualmente enfrentam a expansão da computação distribuída, maior colaboração online, crescimento explosivo de dados e ambientes de TI heterogêneos – todas as questões que tornam a segurança da informação mais crítica e ainda mais complexa do que nunca. Mover dados para um ambiente virtualizado com base em nuvem pode ajudar a desenvolver e gerenciar uma infraestrutura mais flexível e 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 com maior eficiência e automação; escalar operações para atender à dinâmica do mercado e à estratégia de negócios; e praticamente eliminar o tempo de inatividade. A questão, portanto, não é migrar para a nuvem – é como fazê-lo ao mesmo tempo que dados críticos são protegidos. Não surpreende que o nível de segurança dos dados dependa muito de qual plataforma suporta o ambiente de nuvem.

O mainframe possui uma forte herança de ser uma plataforma extremamente segura para ambientes e cargas de trabalho virtuais e oferece uma alternativa atraente para ambientes intensamente expansíveis, muitas vezes implementados na nuvem - em particular no âmbito de segurança. Além disso, muitas organizações já estão utilizando um mainframe como seu hub de dados na execução dos principais aplicativos, proporcionando um ponto de aceleração natural na criação de um hub de segurança para toda a corporação.

Desde a automação até as tecnologias de virtualização avançada e padrões abertos do segmento, os mainframes IBM System z® ajudam a entregar uma base sólida e segura sobre a qual construir o ambiente virtual. Eles suportam ambientes de nuvem expansível com segurança líder de mercado, bem como disponibilidade, desempenho e baixo custo. Esses benefícios são particularmente valiosos no planeta mais inteligente de hoje, onde empresas equipadas, interconectadas e

inteligentes coletam, processam, utilizam e armazenam mais informações do que nunca.

Percepção dos benefícios de nuvens de mainframe

Além de muitas das razões tradicionais para escolher o mainframe ao invés de outras plataformas de hardware - segurança, confiabilidade e cargas de trabalho consolidadas, entre outras - a seguir estão alguns exemplos reais que demonstram por que as organizações implementam ambientes virtualizados em plataformas System z:

•• Uma organização já possuía um mainframe em seu datacenter executando cargas de trabalho de clientes. Ela desejava manter a base de habilidades do mainframe e migrar cargas de trabalho não mainframe para Linux em System z.

•• Outra organização queria oferecer software com base em nuvem como um serviço para seus clientes. Os cálculos da empresa revelaram que o custo de implementação de middleware IBM no mainframe seria menor do que outras plataformas.

•• A terceira organização desejava fornecer hosting de carga de trabalho de clientes em uma nuvem com base em mainframe. Sendo já um usuário de mainframe, queria proteger a sua base de hosting de carga de trabalho, oferecendo um ambiente de nuvem em System z.

Abordagem de questões de segurança na nuvem

Mais do que nunca, as organizações são confrontadas com a necessidade de proteger dados críticos em ambientes de multiplataforma distribuídos e colaborativos. Embora os benefícios operacionais e econômicos da computação em nuvem sejam claros, assim também é a necessidade de desenvolver a segurança adequada para implementações de nuvem. É uma preocupação justificável. De acordo com o IBM X-FORCE® Research & Development, os ataques estão cada vez mais sofisticados e comuns. No meio de 2011, a X-Force relatou que o número de vulnerabilidades críticas já havia ultrapassado o total para todo o ano de 2010.[1]

As mesmas características que tornam o mainframe ideal para a execução de aplicativos críticos – hardware robusto, sistemas operacionais confiáveis, recursos de gerenciamento de sistemas de dimensões industriais e segurança confiável – podem ser utilizadas para habilitá-lo como um hub de segurança corporativo. Estes recursos se estendem para os ambientes virtualizados.

A segurança é construída em cada nível da estrutura do System z, a partir de seu processador, hypervisor e sistema operacional até as suas comunicações, armazenamento e aplicativos. O hosting de cargas de trabalho virtuais e os ambientes de nuvem em um mainframe System z que executa soluções de software IBM pode oferecer muito mais benefícios do que riscos e aborda cada uma das seguintes questões de segurança:

Controle

Muitas organizações não se sentem confortáveis com a ideia de nuvens públicas porque suas informações residem em sistemas que elas não controlam. No entanto, ambientes típicos de nuvem de mainframe permitem que os usuários

implementem sua própria "nuvem privada", o que oferece mais controle. Além disso, esses ambientes podem oferecer um alto grau de transparência de segurança, o que ajuda os usuários a obterem uma melhor visão de toda a corporação e os deixa mais à vontade.

Usuários externos
Solicitante de serviço
Aplicativos
Fornecedor de serviço
Firewall
Servidor de aplicativos front-end
Nuvem privada
Sistemas e armazenamento
Rede virtual
Usuários internos

Figura 1: As implementações de nuvem necessitam de segurança igual ou superior às tradicionais.

Migração

Enquanto a migração de cargas de trabalho para a rede compartilhada e a infraestrutura de computação de nuvem pública forem capazes de aumentar o potencial de exposição não autorizada, a migração para ambientes de nuvem de mainframe pode oferecer autenticação crítica e acesso a tecnologias para proteger dados. O gerenciamento de acesso e de identidade é essencial para a segurança na nuvem, uma vez que limita o acesso a dados e aplicativos apenas para usuários autorizados e apropriados. Ao limitar quem pode visualizar e manipular dados ajuda a garantir que estes não são mal utilizados.

Confiabilidade

Alta disponibilidade é, compreensivelmente, uma questão importante para os departamentos de TI, a qual deve impedir perda ou degradação dos serviços em caso de interrupção. Além disso, aplicativos importantes não podem ser executados na nuvem sem fortes garantias de disponibilidade. Uma das marcas dos mainframes é a sua alta disponibilidade, tornando os ambientes de nuvem de mainframe plataformas extremamente estáveis e seguras. Isso pode ajudar os clientes a utilizar o mainframe como uma plataforma de hosting altamente escalável e confiável para suportar cargas de trabalho de múltiplos clientes simultaneamente.

Fácil de gerenciar

Os ambientes de nuvem de mainframe podem oferecer controles visuais fáceis de gerenciar o firewall, as configurações de segurança para aplicativos e os ambientes de tempo de execução na nuvem. Isso pode diminuir os custos de gerenciamento de TI e, ao mesmo tempo, economizar dinheiro a longo prazo. Um estudo interno da IBM descobriu que, ao longo de três anos, o custo total de propriedade (TCO) para uma nuvem privada com base em sistemas IBM

zEnterprise™ foi 76% menor do que o de uma nuvem pública de um provedor de serviço terceirizado. Isto ocorre devido a cargas de trabalho consolidadas e virtualizadas, bem como uma área de cobertura menor que equivale a menos custos de hardware e de software.

Conformidade

Manter a conformidade com o SOX (Sarbanes-Oxley Act), HIPAA (Health Insurance Portability and Accountability Act) e outros regulamentos pode limitar ou mesmo proibir o uso de nuvens para alguns aplicativos. Felizmente, os ambientes de nuvem de mainframe são capazes de fornecer recursos abrangentes de auditoria para compensar este risco.

O System z possui recursos de segurança projetados especificamente para ajudar os usuários a cumprirem requisitos regulamentadores relacionados à segurança, incluindo: gerenciamento de identidade e de acesso; criptografia de hardware e software; recursos de segurança de comunicação; e extensos registros e relatórios de eventos de segurança.

Benefícios gerais dos ambientes de nuvem de mainframe

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

O System z fornece até 100% de utilização da CPU, bem como uma arquitetura de "compartilhamento total" que pode hospedar milhares de cargas de trabalho mistas. O System z pode também ativar um datacenter mais eficiente, uma vez que utiliza menos energia e resfriamento, ocupa menos espaço e possui um número menor de componentes para gerenciar. Há também a vantagem de preços atraentes. Os clientes IBM já economizaram até 70% em gastos adicionais com auditoria, até 30% com a redução nos chamados de help desk e obtiveram até 52% de custos administrativos mais baixos utilizando o System z como a plataforma para o seu ambiente de nuvem.

O System z fornece todos os componentes necessários para entregar a nuvem hoje, incluindo:

- **Gerenciamento de carga de trabalho – Gerenciar requisitos relacionados à capacidade de infraestrutura de nuvem de acordo com as políticas de negócios.**
- **Processamento de transações – Suportar a integração de nuvem com aplicativos de processamento em transações online críticas.**
- **Escalabilidade - Escalar verticalmente com o IBM z/OS® e partições lógicas (LPARs) e, horizontalmente, com o Linux em System z e IBM z/VM® aliado ao IBM Workload Manager.**
- **Disponibilidade e fornecimento – Utilizar automação para implementar máquinas virtuais e aplicativos de recuperação.**
- **Auditoria e métricas - Contabilidade e medição com base em carga de trabalho suportam o planejamento de capacidade e o reembolso para a linha de negócios.**

Além disso, o mainframe apoia os padrões de segurança do segmento que ajudam a garantir a interoperabilidade, tais como Public Key Infrastructure, OASIS eXtensible Access Control Markup Language, OASIS Key Management Interoperability Protocol e muitos outros.

Otimização – e proteção – das plataformas virtualizadas

O suporte do mainframe para ambientes virtualizados de multiarquitetura permite aos clientes executar uma ampla gama de cargas de trabalho. Isso significa que os usuários podem adicionar processadores, blades e muito mais, de maneira rápida e fácil, e automatizar configurações de rede e hypervisor a fim de reduzir o tempo manual necessário para obter um ambiente de servidor virtual instalado e em funcionamento. Assim que a plataforma virtual é otimizada, é mais fácil consolidar cargas de trabalho devido a: área de cobertura reduzida; sistema menor; menos taxas de licenciamento; e recursos de consolidação de dados.

A escolha da segurança IBM para a computação em nuvem de mainframe

Para otimizar a segurança da empresa, é necessário que haja um alto nível de planejamento e avaliação para identificar riscos nas principais áreas de negócios. Esta estrutura de segurança inclui pessoas, processos, dados e tecnologia ao longo de toda a continuidade dos negócios. Esta abordagem holística pode facilitar um blueprint de segurança mais voltado aos negócios e uma estratégia que pode agir como um escudo eficaz de defesa para toda a organização.

A IBM pode ajudar. Nossas soluções de segurança oferecem recursos de segurança abrangentes, integrados de ponta a ponta aos mainframes, permitindo que as corporações consolidem seu gerenciamento de segurança e alavanquem o mainframe assim como o hub de segurança de sua corporação.

(imagem)
Figura 2: Alavancar um ambiente de mainframe para otimização de TI, consolidação de carga de trabalho e computação em nuvem.

(imagem)
Figura 3: Abordar a segurança de maneira holística com o IBM Security Framework.

IBM Resource Access Control Facility

O IBM Resource Access Control Facility (RACF®) é o principal produto para a proteção dos dados corporativos mais valiosos. Ao trabalhar em estreita colaboração com o sistema operacional, o programa licenciado líder do segmento da IBM é capaz de melhorar a segurança dos dados ao proteger recursos vitais do sistema, além de controlar o que os usuários podem fazer no sistema operacional. O RACF concede acesso apenas a usuários autorizados procedentes dos recursos protegidos. Após a identificação e autenticação do usuário, ele controla a interação entre o usuário, recursos do sistema, recursos de comunicações, programas e aplicativos. Ele também fornece recursos administrativos e de

auditoria detalhados.

Conjunto IBM Security zSecure

O conjunto IBM Security zSecure™ proporciona administração de segurança de baixo custo, melhora os serviços por meio da detecção de ameaças e reduz os riscos com auditoria automatizada e relatórios de conformidade. As ferramentas a seguir, em particular, podem aprimorar os ambientes de nuvem de mainframe:

•• **Security zSecure Audit –** Solução de conformidade e auditoria permite aos usuários analisar e efetuar relatórios sobre eventos de segurança de modo automático e detectar exposições de segurança
•• **Security zSecure Admin –** Permite uma administração de RACF mais eficiente e eficaz, utilizando significativamente menos recursos
•• **zSecure Manager para RACF z/VM –** Fornece serviços combinados de auditoria e administração para RACF no ambiente de máquina virtual (VM)

Tivoli Federated Identity Manager (para Linux em System z)

O IBM Tivoli® Federated Identity Manager é uma solução com base em padrões e controle de acesso para conexão única federada, gerenciamento de confiança em serviços da web e ambientes de arquitetura orientada a serviços (SOA). Ele lida com todas as informações de configuração de uma federação – incluindo as relações com parceiros, mapeamento de identidade, gerenciamento de token de identidade e muito mais.

Tivoli Identity Manager (para Linux em System z)

O IBM Tivoli Identity Manager é uma solução automatizada com base em políticas que gerenciam o acesso do usuário em todos os ambientes de TI, seja em um ambiente corporativo fechado ou em uma empresa virtual ou estendida. Por meio da utilização de funções, contas e permissões de acesso, ele ajuda a automatizar a criação, modificação e finalização de privilégios de usuários por todo o ciclo de vida do usuário.

Tivoli Access Manager para e-business (para Linux em System z)

O software Tivoli Access Manager para e-business é uma solução de autenticação altamente escalável, autorização e de SSO para usuários da web com o propósito de cumprir políticas de segurança entre uma vasta gama de recursos de aplicativos e da web. Ela centraliza o gerenciamento de acesso do usuário ao portal online e às 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, simplificando a implementação e a manutenção da disponibilidade de dados nativamente em repouso em ambientes de mainframe do System z. Além disso, simplifica relatórios importantes de gerenciamento e de conformidade para proteger a privacidade dos dados e cumprir os regulamentos de segurança.

IBM InfoSphere Guardium Database Security

O IBM InfoSphere® Guardium® Database Activity Monitor oferece uma solução simples e robusta para acompanhar continuamente o acesso a banco de dados e à automatização de controles de conformidade em corporações heterogêneas. A solução evita atividades não autorizadas por parte de informantes privilegiados ou hackers enquanto monitora os usuários finais para identificar fraudes sem quaisquer alterações nos bancos de dados, aplicativos ou prejuízo para o desempenho. Utilize esta solução para implementar controles centralizados e padronizados para segurança e monitoramento de banco de dados em tempo real, auditoria de banco de dados de baixa granularidade, relatórios de conformidade automatizados, controle de acesso de nível de dados, gerenciamento de vulnerabilidade do banco de dados e autodescoberta de dados sensíveis.

IBM Proventia Server Intrusion Prevention System (para Linux em System z)

O IBM Proventia® Server Intrusion Prevention System para Linux utiliza firewall de host e inspeção detalhada de pacotes de rede para identificar e bloquear milhares de ameaças conhecidas e emergentes, ao mesmo tempo que visa vulnerabilidades por todos os sistemas operacionais, aplicativos de cliente e da web – tudo isso enquanto fornece, em tempo real, conhecimento sobre a situação e inteligência para os administradores de segurança.

Conclusão

À medida que questões econômicas direcionam o foco para a redução de custos operacionais, e conforme surgem necessidades de segurança, a oportunidade de alavancar o mainframe para entregar eficiências operacionais em conjunto com excelente segurança é clara. Isto é particularmente verdadeiro em ambientes virtualizados, onde mainframes provaram possuir bases fortes e seguras sobre as quais infraestruturas de nuvem são construídas.

O System z é capaz de ajudar a proteger dados essenciais e aplicativos críticos, permitindo que os usuários virtualizem e compartilhem esses componentes em um ambiente flexível e seguro. Tire proveito da eficiência inerente do System z para implementar um ambiente virtualizado, utilizável e escalável que pode proporcionar maior disponibilidade, desempenho e economia.

Para mais informações

Para saber mais sobre a computação em nuvem IBM System z, entre em contato com seu representante IBM 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 IBM fornece a inteligência de segurança para ajudar as organizações a protegerem de holisticamente seu pessoal, infraestrutura, dados e aplicativos. A IBM oferece soluções para gerenciamento de identidade e acesso, segurança de banco de dados, desenvolvimento de aplicativos, gerenciamento de riscos, gerenciamento de terminal, segurança de rede e muito mais.

A IBM opera a maior organização de pesquisa do mundo, desenvolvimento e entrega de segurança do mundo.
Esta abrange nove centros de operações de segurança, nove centros de pesquisa IBM, 11 laboratórios de desenvolvimento de segurança de software e um Institute for Advanced Security com filiais nos Estados Unidos, Europa e Ásia-Pacífico. A IBM monitora 13 bilhões de eventos de segurança por dia em mais de 130 países e retém 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

são garantidos de acordo com os termos e condições dos acordos sob os quais foram fornecidos.

O cliente é responsável por garantir o cumprimento das leis e regulamentos que lhe são aplicáveis. A IBM não fornece orientação ou representação legal ou garante que seus serviços ou produtos irão garantir que o cliente esteja em conformidade com quaisquer leis ou requisitos. Quaisquer instruções sobre a direção ou intenção futura da IBM estão sujeitas à alteração ou à retirada sem aviso prévio e somente representam as metas e objetivos.

[1] Relatório Executivo de Soluções de Segurança IBM, “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&htmlfd=WGL03009USEN&attachment=WGL03009USEN.PDF

Por favor, recicle

TIW14125-BRPT-00