



BENEFÍCIOS DE SEGURANÇA DO RED HAT ENTERPRISE LINUX 5 NO IBM SYSTEM Z

Por Karl Wirth da Red Hat e Peter Spera da IBM Corp.

SUMÁRIO

Durante décadas, os mainframes IBM têm sido a plataforma de hardware preferencial para uma computação segura. O IBM System Z se baseia nesta tradição e a amplia. O Red Hat® Enterprise Linux® foi projetado por e para as organizações mais preocupadas com segurança do mundo.

O Red Hat Enterprise Linux 5 proporciona o melhor nível de segurança com um sistema operacional estável e de código-fonte aberto. Trabalhando em conjunto, IBM e Red Hat criaram uma solução atraente para a segurança - o Red Hat Enterprise Linux 5 no IBM System z.

Este documento explorará os benefícios de segurança do Red Hat Enterprise Linux 5 no IBM System z.



Benefícios de segurança do IBM System z

SEGURANÇA FÍSICA

A segurança física é um componente crítico de qualquer política de segurança e um benefício essencial de um mainframe. Centenas de servidores espalhados por toda a organização podem trazer risco e complexidade. A organização pode ser difícil de proteger, tanto física quanto logicamente. O System z fornece Particionamento Lógico (LPAR) e z/VM no mainframe para permitir que diversas imagens possam conviver lado a lado no ambiente de mainframe. Estas tecnologias proporcionam o isolamento exigido pelos clientes corporativos e do governo em um ambiente certificado Common Criteria. É muito mais simples proteger uma ou várias máquinas System z localizadas no data center principal.

As configurações de networking vulneráveis e expostas que são implementadas no ambiente distribuído podem ser duplicadas dentro do ambiente fisicamente seguro do mainframe, agregando o benefício de segurança física e a facilidade de auditar a implementação da rede.

VIRTUALIZAÇÃO

Os benefícios desta segurança física seriam de pouca utilidade se todas as aplicações consolidadas no mainframe fossem executadas em conjunto em uma única imagem lógica. Durante décadas, os mainframes da IBM têm fornecido funcionalidade de virtualização. No System z, a LPAR pode ser utilizada para dividir os recursos em massa do mainframe em partições que representem melhor os requisitos da carga de trabalho. Dentro de uma LPAR, o z/VM permite que um grande número de imagens de sistema operacional com aplicações diversificadas ou associadas possa rodar simultaneamente na mesma máquina, mantendo o isolamento de cada imagem. E utilizando os HiperSockets, o System z permite comunicação de alta velocidade e fisicamente segura entre as imagens que residem em LPARs separadas.

AUDITORIA

O Red Hat Enterprise Linux 5, juntamente com o IBM System z, fornecem o recurso de auditoria de alto nível requerido pelos clientes mais exigentes. A partir do recurso de auditoria integrado pela Red Hat aos recursos de auditoria do mainframe (inclusive LPAR, z/VM e conexões de rede), as organizações podem obter as informações de que necessitam para assegurar que sua política de segurança seja fortemente implementada.



Benefícios de Segurança do Red Hat Enterprise Linux 5

A segurança da plataforma deve ser uma parte predominante e fundamental da plataforma - não apenas um complemento. Ela deve ser analisada e mantida continuamente para garantir a integridade da plataforma. Deve incluir organicamente o ecossistema de parceiros e uma ampla comunidade de plataformas. Por estes motivos, o Red Hat Enterprise Linux 5 se destaca como uma opção de última geração, líder de mercado, para configurações nas quais a segurança realmente importa. Quatro valores definem a abordagem da Red Hat:

- **Inovação.** A Red Hat é um exemplo em termos de desenvolvimento de novas tecnologias de segurança para Linux, desde a certificação SELinux e EAL 4+ (ambas descritas na próxima seção) até a proteção contra ataques (detalhada abaixo), mais as muitas inovações adicionais descritas no centro de recursos do Red Hat Enterprise Linux: http://www.redhat.com/rhel/resource_center/
- **Transparência.** A disponibilidade do código fonte do Red Hat Enterprise Linux torna a solução uma alternativa melhor para criar sistemas seguros do que as de código proprietário. As inovações do Red Hat Enterprise Linux 5 se devem, em grande parte, ao poder do modelo de desenvolvimento open source, que combina a contribuição de clientes, parceiros, desenvolvedores, usuários finais e administradores.
- **Vigilância.** A Red Hat busca continuamente por potenciais exposições de segurança, certificando cada pacote e fornecendo atualizações de segurança testadas através da Red Hat Network. Os clientes podem fortalecer ainda mais suas infra-estruturas através do atendimento e suporte da Red Hat.
- **Inclusão.** A Red Hat trabalha em estreita colaboração com parceiros como a IBM para garantir que os clientes tenham opções ao criar um ambiente seguro e integrado.

O Red Hat Enterprise Linux 5 traz quatro inovações importantes que protegem os sistemas contra ataques, particularmente na área de buffer overflow e outros ataques dirigidos à memória. Estas novas funções são:

- **Fortify source.** Esta verificação agora é executada em todos os pacotes selecionados. Quando o compilador sabe o tamanho de um buffer, é possível garantir que este não estourará.
- **Proteção stack smashing (canary values).** O sistema colocará um canary value em um ponto aleatório acima da stack. Este valor é verificado durante a operação normal. Se a stack for esmagada, o canary value terá sido alterado, indicando que a stack realmente foi esmagada. Este método pode detectar buffer overflows com antecedência.
- **Pointer encryption.** Os ponteiros de função são criptografados com valores aleatórios exclusivos. Isto é feito para que se possa detectar uma alteração de um ponteiro na memória e evitar o subsequente redirecionamento da execução.
- **Proteção de memória SELinux.** Este aprimoramento pode evitar que qualquer memória que estava aberta à gravação se torne executável. Isto impede que um atacante possa gravar seu código na memória e então executá-lo.

Na Red Hat, os valores de inovação, transparência, vigilância e inclusão não são meras palavras, mas sim processos de negócios que produzem e mantêm o produto o mais seguro possível, fornecendo, ao mesmo tempo, o mais alto valor agregado para os clientes. É por isso que a Red Hat tem se mantido, por quatro anos consecutivos, no topo do ranking elaborado pela pesquisa realizada anualmente pela CIO Insight, que entrevista CIOs de empresas com atuação global.



Benefícios de Segurança do Red Hat Enterprise Linux 5 no IBM System z

A solução Red Hat Enterprise Linux 5 no System z traz para uma organização os seguintes benefícios adicionais de segurança:

UM ÚNICO LINUX EM TODA A EMPRESA, DE PONTA A PONTA

O compromisso da Red Hat com um código fonte unificado significa que ela usa o mesmo código para oferecer o Red Hat Enterprise Linux no IBM System z como o faz na plataforma x86. Este código Linux é convencional, estável, previsível para seu ambiente de mainframe e resolução mais rápida de vulnerabilidades de segurança. Os mesmos administradores de sistema podem executar o Red Hat Enterprise Linux no System z como fazem em outras plataformas. Sua expertise traz maior habilidade e precisão, tempo de resposta menor e maior segurança corporativa global.

SUPORTE PARA SECURITY ENHANCED LINUX

Exclusivamente no Red Hat Enterprise Linux, o Security Enhanced Linux (SELinux) oferece controle granular e baseado em políticas sobre o acesso de programas a dados e recursos do kernel, impedindo que um programa comprometido possa atuar fora de sua política.

O SELinux foi desenvolvido em coordenação com a comunidade open source e a National Security Agency (NSA) para proporcionar os mais altos níveis de segurança para o sistema operacional Linux. O SELinux não é uma distribuição ou ramificação separada do Linux. Pelo contrário, é uma feature do Red Hat Enterprise Linux.

Por default, mais de 200 serviços principais do sistema Red Hat Enterprise Linux 5 são protegidos por meio de políticas dirigidas. Portanto, as organizações podem se beneficiar rapidamente da segurança fornecida pelo SELinux.

Como um benefício adicional, o Red Hat Enterprise Linux 5 inclui também ferramentas aprimoradas de gestão do SELinux, que simplificam o processo de criação, personalização, gerenciamento e diagnóstico de suas políticas.

CERTIFICAÇÃO COMMON CRITERIA EAL4+ SOB CAPP, RBAC, LSPP EM SYSTEM Z

O Red Hat Enterprise Linux 5 é o primeiro sistema operacional Linux a ser lançado com suporte nativo à funcionalidade necessária para atender a Common Criteria for Trusted Operating Systems (Critérios Comuns para Sistemas Operacionais Confiáveis). Isto inclui toda a funcionalidade exigida pela certificação EAL 4+ sob os seguintes perfis de proteção: CAPP (Controlled Access Protection Profile), RBAC (Role Based Access Control), e LSPP (Labeled Security Protection Profile).

Além das certificações Common Criteria já disponíveis para clientes do System z, a IBM está patrocinando a certificação EAL 4+ do Red Hat Enterprise Linux 5 no System z. As certificações já existentes, que incluem LSPP no z/VM e no z/OS, combinadas com a certificação do Red Hat Enterprise Linux 5, proporcionarão um ambiente de plataforma seguro, capaz de satisfazer as exigências rigorosas das políticas de segurança dos setores público e privado.



Para clientes fora do âmbito do governo, isto garante que a plataforma foi projetada, analisada e testada pelos padrões de segurança mais rigorosos do governo.

Para clientes do setor governamental, que são obrigados a obedecer os Common Criteria for Trusted Operating Systems, o Red Hat Enterprise Linux 5 é uma solução open source que suporta, de forma nativa, a segurança em diversos níveis. Esta é uma opção convencional empolgante para clientes que percebem os benefícios do ambiente operacional open source e da consolidação no System z da IBM.

VIRTUALIZAÇÃO

O z/VM da IBM fornece os benefícios de segurança de um ambiente de virtualização de qualidade historicamente comprovada para o Red Hat Enterprise Linux no System z. Diversas imagens Linux podem rodar com segurança simultaneamente dentro do ambiente z/VM. Estas imagens podem ser completamente isoladas, ou parte de uma solução maior, end-to-end / multi-imagem. A comunicação em rede entre imagens pode ser implementada via LANs e switches virtuais para proporcionar a flexibilidade requisitada por qualquer solução end-to-end corporativa. Se for exigido um número pequeno de imagens, o LPAR poderá ser considerado como uma alternativa ao z/VM; porém, quando usados em conjunto, eles se tornam uma alternativa altamente configurável e extremamente flexível para rodar o Red Hat Enterprise Linux e suas cargas de trabalho.

ACELERAÇÃO CRIPTOGRÁFICA

As funções criptográficas necessárias para proteger dados, validar pontos finais ou assinar são vitais para a implementação de qualquer aplicação segura, mas podem consumir muita CPU quando implementadas em softwares. O System z contém instruções criptográficas, aceleradores de SSL e co-processadores criptográficos de hardware sensíveis e reativos a adulterações dos quais o Red Hat Enterprise Linux pode tirar proveito. Estas opções proporcionam às aplicações e empresas a segurança, a flexibilidade e a velocidade de que precisam para atender as demandas dos atuais requisitos abrangentes de segurança corporativa.

O IBM System z suporta duas abordagens de implementação de chaves: Secure Key e Clear Key. A Secure Key é uma chave criptografada sob outra chave dentro dos limites do ambiente de hardware seguro. Apesar da versão criptografada daquela Secure Key poder sair do ambiente de hardware, o valor claro daquela chave nunca está disponível fora do ambiente de hardware seguro. As chaves seguras e suas funções são geralmente usadas em aplicações bancárias e financeiras. A Clear Key é uma chave criptográfica similar, mas não é criptografada sob outra chave. Portanto, as funções criptográficas têm atuação mais rápida com uma Clear Key. O exemplo mais generalizado de criptografia Clear Key é a negociação que acontece para autorizar uma transação protegida por SSL. Os internautas utilizam seus navegadores Web para conectarem-se ao servidor de uma loja e solicitar produtos via transação protegida por SSL.

A execução do Red Hat Enterprise Linux no System z permitirá à sua organização aproveitar as seguintes funções de criptografia para incrementar a segurança e o desempenho:

1. Placas aceleradoras RSA Clear Key, bem como criptografia simétrica e funções hash baseadas em instruções de hardware embutidas para AES-128, DES, TDES, SHA-1 e SHA-256 estão disponíveis no RHEL 5



2. Funcionalidades de criptografia utilizando hardware estão planejadas e serão suportadas em um release futuro.

3. A utilização de Crypto API do kernel (cryptoki) faz com que o sistema permita que as chamadas crypto API do kernel possam, sem modificação, utilizar as instruções de hardware do System z para criptografia.

AUTENTICAÇÃO CENTRALIZADA

O Red Hat Enterprise Linux é totalmente compatível com LDAP, permitindo que este seja integrado perfeitamente a implementações RACF existentes. Como a Red Hat é uma empresa de padrões abertos, sabe-se que aplicações de terceiros como Tivoli Identity Manager, SUN One Director Server, Red Hat Directory Server e muitos outros sistemas LDAP e Kerberos funcionam sem problemas.

RESUMO

O Red Hat Enterprise Linux 5 no IBM System z oferece benefícios significativos de segurança para a empresa e organizações governamentais. O System z proporciona segurança física robusta, virtualização, aceleração criptográfica de hardware e recursos de auditoria. O Red Hat Enterprise Linux 5 combina uma abordagem criativa, transparente, alerta e abrangente de segurança, com uma grande variedade de funções que protegem os sistemas contra ataques, particularmente na área de buffer overflow e outros ataques dirigidos à memória. O Red Hat Enterprise Linux 5 no System z proporciona às organizações uma única arquitetura Linux para toda a empresa, suporte para Security Enhanced Linux (SELinux), uma certificação Common Criteria EAL4+ sob CAPP, RBAC e LSPP, aceleração criptográfica e autenticação centralizada.

© 2007 Red Hat, Inc. Todos os direitos reservados. Red Hat, Red Hat Enterprise Linux, os logotipos Shadowman e JBoss são marcas registradas da Red Hat, Inc. nos EUA e em outros países. Linux é uma marca registrada da Linus Torvalds. Todas as outras marcas registradas são de propriedade de seus respectivos donos.

RT#371420 5/07