Riscos e Custos Ocultos da Compactação ZIP no z/OS

Este artigo aborda pontos inerentes a soluções legadas de compactação ZIP, que impactam negativamente assuntos relativos a utilização, regras de MLC e SLAs, e ainda a segurança de dados e suas conformidades regulatórias

White Paper by

David Kennedy
Data 21, Inc.
VP of Technical Sales

Introdução

Apesar da crescente capacidade de armazenamento dos computadores e da velocidade das redes, a compactação de dados continua sendo uma ferramenta essencial para armazenar e transmitir volumes cada vez maiores de dados. O formato .zip foi desenvolvido para uso em múltiplas plataformas e para o armazenamento eficiente de dados; combinando entre 85% e 95% em compactação média de dados, gerenciamento de arquivos e criptografia de dados.

A disponibilidade de utilitários e processos compatíveis com o formato .zip, em praticamente todas as plataformas de computação, aliada a facilidade de uso por usuários de todos os níveis de conhecimento técnico tornam os arquivos .zip uma solução simples, eficiente e segura no tráfego de informações dentro e fora da empresa. Reduzindo a complexidade de infraestruturas de rede na transferência de arquivos e até mesmo a necessidade de software de segurança, durante o tráfego de dados, os utilitários .ZIP servem ainda como uma metodologia de armazenamento de arquivos bastante eficiente e segura. Provê, com facilidade, arquivos compactados, criptografados, gerenciáveis e altamente transportáveis, de qualquer tamanho e com qualquer número de arquivos.

Pelas razões anteriores, a maioria das operações no z/OS emprega compactação .zip há anos. No entanto, é importante reconhecer que os ambientes têm sofrido mudanças significativas desde que essas soluções começaram a ser implementadas. Atualmente, a maioria dos produtos legados em operação não conta com as tecnologias necessárias e atualizadas no apoio a negócios estratégicos e nos ‘compliances’ regulatórios (LGPD), que proporcionam redução de custos do mainframe, garantia e conformidade sobre a privacidade de dados, impostas ao gerenciamento de mainframe e ao negócio, de forma geral.

E quais seriam essas novas tecnologias tão necessárias a atualização de todo esse processo?

***Criptografia AES Forte**

***(zEDC) zEnterprise® Data Compression**

***IBM® z Integrated Information Processor (zIIP)**

Uma vez que sua solução atual de compactação .zip para z/OS não atenda TODOS OS TRÊS requisitos, é bem provável que sua empresa esteja pagando muito por ele. Contudo, saiba como reduzir esse custo, além de se beneficiar das modernas e eficientes funcionalidades de um software de última geração, entrando em contato com a Workers Informática.

Conheça nosso plano de Substituição do Legado.

Criptografia AES Forte

O formato Zip fornece um recurso de criptografia de dados persistente e de fácil implementação, conhecido como ***Password Protection***. A inclusão de poucos parâmetros é suficiente para eliminar praticamente a ameaça de acesso não autorizado aos dados, em trânsito e armazenado.

> O formato de criptografia Zip 2.0 é conhecido por ser relativamente fraco e não fornecer a proteção adequada, caso seja acessado por ferramentas especializadas de recuperação de senha.
>
> - WINZIP COMPUTING

Praticamente todos os produtos Zip, em todas as plataformas, oferecem suporte à criptografia Zip AES; e por um bom motivo. A maioria das soluções .ZIP para o z/OS fornece apenas uma forma antiga (e fraca) de criptografia de senha, conhecida como criptografia Zip 2.0. Não se pode esperar que essa criptografia proteja informações confidenciais. Além de não estar em conformidade com as regulamentações de segurança atuais, não tira proveito do hardware criptográfico do mainframe, tornando-o muito lento e caro. Para serem considerados completamente seguros, os arquivos .ZIP requerem duas coisas: frases secretas bem construídas, difíceis de decifrar, e também uma criptografia forte (de preferência 256 bits). Se os dados confidenciais são compartilhados através de arquivos zip com criptografia fraca ou mesmo não criptografados, a empresa pode estar sujeita aos seguintes riscos:

Violação de Dados

O estudo dos custos envolvidos na violação de dados, levantado pela IBM em 2018, considera essa violação como "um evento em que o nome de um indivíduo, um registro médico, ou um registro financeiro de cartão de

débito/crédito são potencialmente colocados em risco – seja em formato eletrônico ou papel".

De acordo com essas informações, essas violações estão mais caras e resultam em mais registros perdidos/roubados, ano após ano

Identificando as três principais causas: ataque malicioso ou criminoso, falha do sistema ou erro humano. Os custos da violação de dados variam de acordo com a causa e as proteções disponíveis no momento da violação. O estudo descobriu que as médias do custo total dessa violação, do custo de cada registro perdido ou roubado (custo per capita) e do montante de violações aumentaram além das médias do relatório de 2017.

- Custo total médio da violação de dados: $ 3,86 milhões
- Aumento de custo médio total em um ano: 6,4%
- Custo médio por registro perdido ou roubado: $ 148
- Aumento anual no custo per capita: 4,8%
- Probabilidade de recorrência nos próximos dois anos: 27,9%
- Aumento médio no tamanho dos dados violados: 2,2%

Outros resultados de pesquisas recentes mostram que cerca de 60% das empresas sujeitas a essas ocorrências não criptografaram seus dados. Portanto, é altamente recomendado criptografar dados armazenados e trafegados

De acordo com o estudo, 48% desses incidentes envolveram ataques maliciosos ou criminosos, 27% foram causados por negligência de funcionários ou contratados (fator humano) e 25% envolveram falhas no sistema e de processos de negócios. O estudo descobriu ainda que o uso extensivo de criptografia é o segundo fator mais eficaz na redução do custo per capita.

Não Conformidade

Os custos do não conformidade podem ser extremamente elevados. Pesquisas recentes indicam que a não conformidade se tornou mais caro do que nunca para as empresas, excedendo em muito os custos de investimentos na implementação das conformidades exigidas.

Com base em um relatório recente da Ponemon Institute e da GlobalScape, o custo anual de não conformidade para as empresas é, em média, $ 14,8 milhões, um aumento de 45% desde 2011.

Esse intervalo pode ir de $ 2,2 milhões a $ 39,2 milhões.

As penalidades decorrentes da não conformidade, conforme o relatório do Ponemon, são 2,71 vezes o custo de estar em conformidade.

Praticamente, todas as regulamentações de proteção de dados, como HIPAA, GDPR e PCI-DSS requerem a criptografia de dados regulamentados. Por exemplo, a criptografia é especificamente referenciada no GDPR. O Artigo 32 (1) (a) das diretrizes exige a criptografia de dados pessoais.

O HIPAA exige que as empresas utilizem tecnologia de criptografia de dados na proteção das informações confidenciais do paciente. O PCI-DSS requer criptografia dos dados transmitidos do 'titular do cartão' em redes públicas abertas e da proteção dos dados armazenados. Em outras palavras, essas informações devem ser criptografadas sempre que armazenadas ou transmitidas. Os custos da não conformidade são provenientes de despesas associadas à interrupção de negócios, perdas de produtividade, multas, penalidades e custos de liquidação, entre outros. A mais óbvia e direta maneira de se proteger contra acesso não autorizado e seus riscos associados é a aplicação da criptografia persistente.

Infelizmente, a criptografia não é um recurso comum para dados armazenados entre os provedores de nuvem.

De acordo com a Skyhigh Networks, embora 81,8% dos provedores de nuvem criptografem dados em trânsito, apenas 9,4% criptografam dados armazenados em seus servidores.
Portanto, é responsabilidade do 'dono' dos dados garantir essa proteção.

Atualmente, a maioria das empresas reconhece que proteger apenas os dados necessários para atingir a conformidade é o mínimo necessário e que a mudança da criptografia seletiva (protegendo apenas tipos específicos de dados) para a criptografia generalizada (criptografando todos os dados) é necessária. Recente levantamento da Data21 com clientes z/OS revelou que a maioria dos entrevistados faz o zip rotineiro de dados confidenciais para transferência entre servidores localizados dentro e/ou fora da empresa.
Por conta da natureza e do volume de dados corporativos e processados no

Mainframe, isso não se mostrou surpreendente. Surpreendente foi constatar que, na maioria dos casos, esses arquivos não estão sendo criptografados por senha. Dada a facilidade de implementação e os benefícios obtidos, a pergunta é: Por quê?

Um fato é que muitas empresas se concentram em proteger o processo de transmissão de dados (em trânsito), em detrimento a proteção dos dados. O fato é que os dados são mais vulneráveis ao acesso não autorizado quando armazenados em um servidor, do que durante a sua transmissão.

Apesar de eficiente, o uso do FTP Seguro (SFTP) e das redes privadas virtuais (VPN), a proteção de dados ocorre apenas na transferência de arquivos, não garantindo a completa privacidade, quando comparada a criptografia .Zip AES - que protege os dados confidenciais durante a transmissão e também quando armazenados.

O fato é que os dados são mais vulneráveis ao acesso não autorizado quando armazenados em um servidor do que durante uma transferência

Outro motivo que pode levar as empresas de não utilizarem a proteção adequada pode ser o tempo e o custo da compactação e da criptografia. Discutiremos esse assunto, a seguir.

.

Custos Adicionais Ocultos

A redução do uso de Processadores Gerais (GP's) oferece uma economia imediata. A BMC, em 2019, revelou que a capacidade dos mainframes continua aumentando. Os MIPS continuam crescendo, colocando mais pressão sobre os orçamentos das empresas que dependem do mainframe. Mais de 61% dos entrevistados afirmam que a redução de custos do mainframe é um desafio. Portanto, é importante que as soluções implementadas suportem as tecnologias zSeries mais atuais, no atendimento a essa questão.

Compactação de Dados zEnterprise® (zEDC)

A compactação de dados zEDC oferece redução na CPU de até 118X e melhora do throughput de até 24X. O novo recurso zEDC “on chip”, da plataforma IBM z15, substituiu os custos extras dos antigos cartões zEDC,

tornando o zEDC disponível gratuitamente para todas as soluções de compactação zip no mainframe. Uma vez que sua máquina ofereça suporte ao zEDC, e sua solução zip não, há de ser considerada a substituição do software legado por uma solução que ofereça esse suporte com vantagens operacionais e benefícios financeiros claros.

.

O custo de CPU é reduzido em até 80%, se comparado com a compactação de soluções que não ofereçam o suporte zEDC.

O custo de compactação, significativamente menor, e a incrível velocidade de compactação do zEDC não servem apenas para melhorar todas as métricas do processamento zip do mainframe, mas também permitem um uso mais abrangente da compactação nativa do mainframe.

IBM® z Integrated Information Processor (zIIP)

Caso o zEDC não esteja disponível em seu ambiente, o zIIP é a segunda melhor opção para a redução dos custos da compactação. Conforme levantamento do setor, os custos de hardware mais software para um processador zIIP é de $ 150 a $ 200 por MIPS, se comparado aos $ 2.200 até $ 3.400 para um processador de uso geral.

À medida que os processos avançam, a compactação de dados se torna, cada vez mais, um dos usos mais importantes da CPU.

Reduzir os ciclos de compactação para os zIIPs, de baixo custo, é a segunda melhor opção a ser escolhida.

O zIIP reduz cargas MLC associadas ao processo de compactação de dados, liberando os GPs desse

Além disso, nos casos em que os GPs estejam limitados (kneecapped), o tempo de compactação também poderá ser reduzido. Uma vez que a maioria das instalações disponibilizem zIIPs, o simples fato de se manter uma solução que não ofereça esta facilidade representa um custo extra considerável em relação àqueles que já realizam.

.

A Solução ZIP/390 MP

O **ZIP/390 MP** é uma solução totalmente aderente a compactação ZIP para o z/OS e o USS, oferecendo custo bastante atraente e uma completa cobertura das principais tecnologias apresentadas neste White Paper, entre outras funções.

Com recursos operacionais superiores aos concorrentes e ofertas comerciais agressivas e competitivas, sua empresa ainda conta com o **plano de substituição do produto legado**, o **ZIP/390 MP torna-se a solução de software ideal para substituir as soluções mais caras e/ou com menos recursos tecnológicos**.

Acesse nossa página exclusiva do ZIP/390 para mais informações.

Sobre a Workers Informática

A **Workers Informática** atua há quase 30 anos nas principais empresas do país, oferecendo um compromisso diário de qualidade aos seus usuários e clientes. Nossa equipe técnica é formada por profissionais especializados. Nosso diferencial é fornecer um atendimento com soluções de acordo com as necessidades de cada um de nossos clientes e autonomia para avaliar e indicar essas soluções com isenção.

Sobre a Data 21

A Data 21, Inc. se especializou no desenvolvimento contínuo e no suporte de soluções de software para Mainframe, desde 1980. O compromisso da Data 21 é implementar em seus produtos os avanços relevantes do hardware e software zSeries da IBM, combinado com uma grande competitividade comercial, resultando em produtos superiores com o melhor desempenho e menores custos.