Marc Staimer, Dragon Slayer

ARTIGO

Acha que todas as distribuições oferecem o melhor ambiente de DevSecOps no Linux?

Pense melhor!

Introdução

O DevOps está mudando. O desenvolvimento de código com segurança adicional posterior é uma estratégia perigosamente falha. Quando essa segurança adicional não consegue corrigir vulnerabilidades de código exploráveis, ela coloca toda a organização em risco. Para muitos que trabalham com DevOps, a segurança geralmente era apenas algo com o que eles se preocupavam depois. Era comum supor que as múltiplas camadas sistêmicas de medidas e dispositivos de segurança da organização de TI protegeriam qualquer novo código contra malware ou violações. Além disso, o desenvolvimento de código com segurança integrada adiciona tarefas e etapas ao tempo de desenvolvimento e teste. Mais tarefas e etapas atrasam o prazo de lançamento no mercado. As nuvens multilocatário mudaram radicalmente o mercado. Em um mundo com um número cada vez maior de ataques cibernéticos, qualquer vulnerabilidade pode colocar em risco os dados de milhões de usuários.

Essas atitudes herdadas do DevOps são inseguras. Elas são potencialmente muito caras no ambiente atual. Lembre-se de que quase todos os países desenvolvidos e a maioria dos países em desenvolvimento promulgaram leis e regulamentos para proteger informações de identificação pessoal, ou PII[1]. As PII são incrivelmente valiosas para os cibercriminosos. O roubo de PII permite que eles cometam muitos crimes cibernéticos, incluindo o roubo cibernético de identidades, finanças, propriedade intelectual, privilégios de administrador e muito mais. As PII também podem ser vendidas na web. A finalidade dessas leis e regulamentos de PII é forçar as organizações de TI a proteger as PII. O não cumprimento dessas leis e regulamentos geralmente acarreta sanções financeiras punitivas.

A prática de adicionar segurança ao DevOps após o desenvolvimento deveria ser aposentada. Contudo, ela ainda é a regra em vez da exceção. Lembre-se de que as vulnerabilidades de código exploratório talvez não sejam específicas do código desenvolvido, mas dos sistemas operacionais, compiladores ou ferramentas subjacentes utilizados no desenvolvimento do código. Com frequência, o código de DevOps desacelera o desenvolvimento. Prazos deixam de ser cumpridos. Muitas organizações de TI fazem o cálculo frio de deixar as atividades de segurança para o fim de seus ciclos de desenvolvimento. Isso está se tornando cada vez mais precário. Basta uma vulnerabilidade explorada para arruinar o dia dos executivos, acionistas, funcionários e, especialmente, dos desenvolvedores. Quando isso acontece, começa o alvoroço. Todo o mundo larga o que está fazendo para resolver a situação o mais rápido possível.

O problema do crime cibernético está piorando, não melhorando. O surgimento do ransomware acelerou essa tendência. A cada 14 segundos, mais uma organização é vítima de ransomware[2]; 1,5 milhão de sites de phishing são criados todos os meses[2]; e os ataques de ransomware aumentaram mais de 97% nos últimos dois anos[2]. É um problema que cresce rapidamente. O ransomware tem como alvo vulnerabilidades de sistema e software e as explora assim que se tornam de conhecimento público. Elas se tornam publicamente conhecidas assim que um patch de vulnerabilidade é liberado.

No momento em que uma correção de vulnerabilidade do sistema operacional (SO) é lançada, o relógio começa a correr. O ônus de implementá-la ou não antes que os cibercriminosos possam explorá-la recai sobre os administradores de TI. Isso aumenta o estresse e é uma das razões pelas quais o DevOps se tornou mais consciente da segurança, transformando-o no DevSecOps.

O DevSecOps integra operações e práticas de segurança ao software conforme ele é desenvolvido. A meta é fornecer rapidamente produtos de alta qualidade e alta segurança. O foco do DevSecOps é garantir a segurança integrada ao processo de desenvolvimento desde o início. A equipe de desenvolvimento está assumindo a responsabilidade de fornecer serviços e código mais seguros em vez de confiar em outras pessoas para garantir a segurança do seu trabalho após a conclusão. O sucesso depende do alinhamento estreito entre o desenvolvimento de aplicativos, com melhorias significativas nos resultados de monitoramento, alerta, automação, aplicação de correções, atualização e implantação.

A Oracle trata o DevSecOps como questão de alta prioridade, o que fica evidente em todos os bancos de dados, aplicativos e middleware da Oracle, e especialmente na distribuição Oracle Linux. Este documento demonstra como a ênfase da Oracle na segurança torna sua distribuição Linux a líder e mais adequada para o DevSecOps.

[1] No setor de saúde, são chamadas de informações privadas de saúde (PHI) ou PHI eletrônicas (EPHI)
[2] Estatísticas sobre ransomware e Comparitech

Índice

Problemas conhecidos de segurança do Linux e as respostas do Oracle Linux

O Linux de software livre se tornou rapidamente o SO predominante derivado do UNIX. Agora, ele já ultrapassou em muito[3] as implantações de servidores Microsoft Windows. Essa popularidade o tornou um alvo para cibercriminosos de todos os tipos. Não se engane, porque definitivamente existem vulnerabilidades exploráveis no Linux. A comunidade de software livre está comprometida com a correção dessas vulnerabilidades. O problema é que a aplicação de correções no Linux para essas vulnerabilidades não é um processo trivial.

O problema de correção de vulnerabilidades do Linux

O motivo pelo qual a correção das vulnerabilidades do Linux não é trivial é porque normalmente ela é disruptiva. Processos disruptivos exigem agendamento. Poucos aplicativos conseguem tolerar uma interrupção durante o horário comercial. A maioria das organizações de TI agenda processos disruptivos, como a correção de vulnerabilidades do Linux, para um fim de semana dentro de 90 a 120 dias. O NopSec.com relata que a organização média de TI leva mais de 103 dias (mais de três meses) para aplicar correções de vulnerabilidade, aumentando para 176 dias no caso de instituições financeiras. Em outras palavras, a correção fica atrasada. É adiada para que diferentes partes interessadas, aplicativos, servidores, hipervisores, armazenamento, rede etc. tenham tempo para coordenar seus esforços. Quando esse fim de semana agendado acontece (e supondo que não seja adiado, o que é muito comum), nas primeiras 24 horas é quando todos os processos de correção disruptivos são implementados. As próximas 24 horas são reservadas para recuperar as correções que não funcionaram ou causaram problemas. Esses processos são trabalhosos e propensos a erros.

De acordo com os serviços de nuvem de TI do Ponemon Institute e da ServiceNow, entrevistas com mais de 3.000 profissionais de segurança cibernética em todo o mundo[4] determinaram que 48%[3] sofreram no mínimo uma e possivelmente mais violações de dados em um período de dois anos, e 57% dos entrevistados atribuíram as violações a vulnerabilidades para as quais havia uma correção que não tinha sido aplicada.

Quando uma correção de vulnerabilidade do Linux é liberada, ela documenta todas as vulnerabilidades e falhas de segurança que foram corrigidas. Isso inicia a corrida entre aqueles que implementam a correção e aqueles que tentam explorar a vulnerabilidade. A documentação de liberação da correção informou os cibercriminosos onde atacar. Eles sabem que têm uma janela de oportunidade para explorar as vulnerabilidades antes que a correção seja implementada.

Os cibercriminosos fazem engenharia reversa dessas vulnerabilidades em semanas ou até dias. Eles presumem que a maioria das organizações de TI leva meses, geralmente muitos meses, para aplicar a correção. O Relatório de Investigações da Violação de Dados da Verizon de 2019 valida essa suposição. Ele descobriu que a correção tende a não ser feita em tempo hábil e geralmente é incompleta. Sua pesquisa mostrou que as organizações de TI corrigem, em média, menos de 40% dos sistemas vulneráveis afetados no prazo de 30 dias após a divulgação da vulnerabilidade. Suas pesquisas confirmaram que a correção é um processo disruptivo, que exige ampla coordenação de vários departamentos e muita mão de obra em tarefas manuais. O relatório do Ponemon Institute e da ServiceNow também descobriu o seguinte:

- 55% gastaram mais tempo com processos manuais do que respondendo rapidamente a vulnerabilidades;
- 61% se sentiram frustrados com a dependência de processos manuais ao corrigir vulnerabilidades;
- 12 dias foi o tempo médio perdido coordenando manualmente as equipes para cada vulnerabilidade corrigida;
- 65% relataram dificuldades em identificar quais vulnerabilidades corrigir primeiro e quais podiam esperar.

A correção de vulnerabilidades do Linux é um enorme problema de segurança que precisa urgentemente de correção.

Como o Oracle Linux resolve as correções problemáticas de vulnerabilidades do Linux

Para resolver essas correções de vulnerabilidade de segurança do Linux que são desmoralizantes, problemáticas e tão comuns, é preciso transformar a aplicação de correções do SO Linux em algo "não

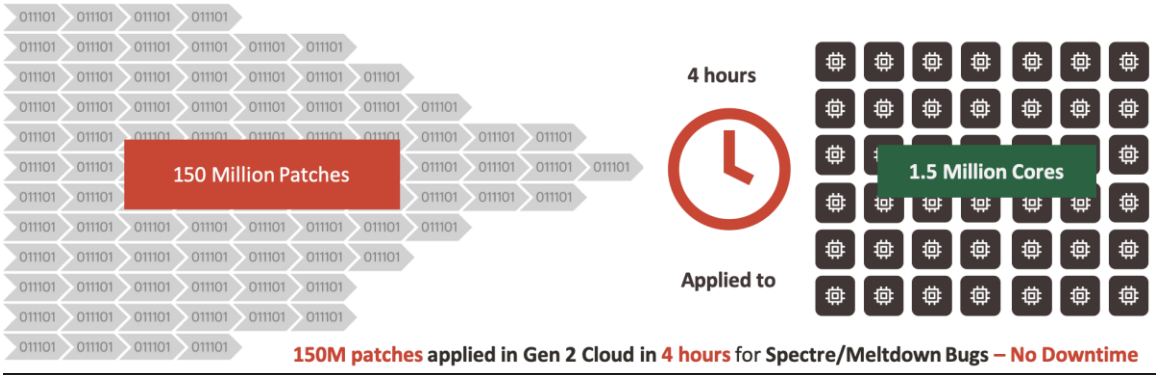
[3] *Relatório da IDC sobre participação de mercado mundial dos sistemas operacionais e subsistemas* referente a 2017; o Linux tinha 68% do mercado. Sua participação só aumentou desde então. Desenvolvedor da Microsoft revela que o Linux agora é mais usado em Azure do que o Windows Server: https://www.zdnet.com/article/microsoft-developer-reveals-linux-is-now-more-used-on-azure-than-windows-server/

[4] Today's State of Vulnerability Response: Patch Work Demands Attention

disruptivo" e online. E é exatamente isso que a Oracle faz com o Ksplice. A tecnologia e o serviço Ksplice exclusivos da Oracle[5] atualizam os kernels, os hipervisores e as bibliotecas críticas de espaço do usuário sem exigir reinicialização ou interrupção. Assim, sempre que quaisquer correções do SO Linux são liberadas, incluindo correções para vulnerabilidades exploráveis, o Ksplice permite que elas sejam implementadas rapidamente, em tempo hábil, sem precisar de agendamento ou coordenação com ninguém. Sem interrupções, sem tempo de inatividade, sem agendamento, sem coordenação e sem amplas janelas de vulnerabilidades exploráveis conhecidas. Em outras palavras, um Linux mais seguro.

O Ksplice do Oracle Linux adiciona outro nível de segurança ao alertar após as correções de segurança serem implementadas com "Detecção de exploits conhecidos" nas escalações de privilégio. Os administradores podem restringir os alertas a tentativas específicas de escalação de privilégio. Ele permite exclusivamente auditar e alertar sobre escalações de privilégio conhecidas.

Nenhuma outra distribuição Linux, nem IBM Red Hat, nem SUSE, nem Ubuntu, resolveu esse problema de segurança. O Oracle Linux é a primeira distribuição Linux que realmente resolve as correções problemáticas de vulnerabilidades do Linux.



Comprovação de correção não disruptiva de Spectre/Meltdown na Oracle Gen2 Cloud

Outra comprovação vem de uma companhia aérea muito grande que utiliza o Oracle Linux e o Ksplice. O Ksplice permitiu que ela cumprisse requisitos rigorosos de segurança sem ter que "passar por um processo demorado de gerenciamento de mudanças. Esse processo demorado de gerenciamento de mudanças geralmente adiciona uma tonelada de despesas operacionais" ao processo. O tempo do administrador do sistema diminuiu de 54 para 7 horas por ciclo, enquanto os servidores atualizados ou corrigidos continuaram a operar sem reinicialização. O Ksplice também permitiu que os administradores do sistema revertessem correções ou atualizações a partir de qualquer ponto em microssegundos com um comando simples.

Mas não existem pessoas que afirmam que hipervisores com Live Migration ou vMotion conseguem gerenciar esse problema com correções incrementais? A resposta direta é que eles não conseguem. O processo de correção incremental corrige ou atualiza uma máquina virtual (VM) com SO Linux e aplicativo, migra os usuários para a VM corrigida, passa a corrigir a VM sem correção e depois faz o failback dos usuários para a VM corrigida. O processo reinicia e se repete. Esse processo ainda é disruptivo e precisa de tempo de inatividade agendado. Ainda é manual, trabalhoso, repetitivo e sujeito a erros humanos frequentes. Ele não aumenta a segurança do DevOps.

Os testes de regressão de atualização e correção da Oracle foram projetados para evitar impactos negativos nos ambientes existentes. No entanto, isso não isenta as organizações de TI da responsabilidade de fazer seus próprios testes de regressão. As melhores práticas ainda exigem que esses testes sejam executados em seus ambientes de teste antes de aplicar as correções em seus ambientes de produção. A reversão de correções é outra tarefa consistentemente sujeita a erros. Não com o Ksplice. E, como os clientes do Oracle Linux descobriram, o Ksplice reverte as correções tão facilmente quanto as aplica, mais uma vez de forma não disruptiva, sem reiniciar a máquina.

[5] A Red Hat tem o Kpatch e a SUSE, o kGraft, que são similares ao Ksplice, mas servem apenas para o kernel e um pequeno subconjunto de correções. O Ksplice possui uma variedade muito maior de correções, incluindo a capacidade de corrigir hipervisores e bits críticos de espaço do usuário de forma não disruptiva.

O problema de déficit do ecossistema de segurança do DevSecOps

Para ser verdadeiramente DevSecOps, é preciso um ecossistema Linux muito seguro. O padrão recomendado pelo setor e pelos governos é o Common Criteria (CC), de acordo com o Perfil de Proteção do Sistema Operacional de Uso Geral (OSPP) da Parceria Nacional de Garantia da Informação (NIAP), dos EUA.[6] Ele se tornou o padrão do setor.

Outro problema da distribuição Linux com DevSecOps é a criptografia. É claro que todo o mundo tem criptografia. Mas sua criptografia raramente é validada de acordo com a FIPS 140-2 do Instituto Nacional de Padrões (NIST), dos EUA. Muitos fornecedores afirmam ter conformidade com a HIPAA/HITECH, mas não foram validados. A FIPS 140-2 não é um algoritmo de criptografia. É um processo de validação por terceiros contratados pelo NIST. Isso é extremamente importante para os mercados de serviços de saúde e governo federal dos EUA. A HIPAA/HITECH exige que todos os módulos criptográficos sejam validados pelo NIST. A FIPS 140-2 é o único processo de validação aprovado.

A validação não é trivial nem barata. Se a aplicação de criptografia não for validada pela FIPS 140-2, de acordo com a HIPAA/HITECH,[7] as informações privadas de saúde eletrônicas (EPHI) armazenadas não estarão em conformidade. Muitas agências do governo dos EUA, governos estaduais e municipais também exigem a validação FIPS 140-2 para criptografia.

O próximo problema de segurança do DevSecOps no Linux que frequentemente é esquecido é o acompanhamento dos mais recentes avanços de segurança de software livre e hardware. A segurança é um alvo sempre em movimento. É um jogo de ataque e defesa. O crime cibernético é um negócio lucrativo que arrecada bilhões de dólares[8] todos os anos, com muitos lucros sendo investidos em P&D. O crime cibernético é organizado e, às vezes, patrocinado por governos. Por exemplo, o crime cibernético da Coreia do Norte captura quantias significativas em moeda estrangeira para a notória nação eremita.[9]

Nunca haverá segurança perfeita. A melhor prática de segurança é que as organizações de TI dificultem o máximo possível a vida dos cibercriminosos, incentivando-os a buscar alvos mais fáceis. É por isso que os profissionais de segurança enfatizam a defesa profunda em camadas. É a mesma estratégia necessária para o DevSecOps. Quem consegue aproveitar os aprimoramentos mais recentes de segurança de hardware, como o EPYC Secure Memory Encryption (SME) da AMD, dificulta o trabalho dos cibercriminosos. Garantir que a distribuição Linux esteja utilizando os aprimoramentos mais recentes de segurança em software livre (como as funções de segurança Kata Containers, libvirt, QEMU e Kubernetes, e tokens de OpenID Connect baseados em OAuth 2.0) dificulta muito a violação da segurança.

Estranhamente, quase todas as distribuições Linux suportam de forma desordenada os avanços na segurança de hardware e, mais importante ainda, de software livre. Assim como a correção disruptiva, isso abre possíveis vulnerabilidades que podem ser exploradas.

Como o Oracle Linux resolve o problema do déficit do ecossistema de segurança do DevSecOps

A Oracle é totalmente focada em segurança. Por isso, ela assumiu uma abordagem muito proativa na adoção e no suporte ao hardware mais recente da AMD, Intel e ARM. A Oracle também está firmemente comprometida em oferecer suporte ao mais recente software livre de segurança Linux, incluindo KATA Containers, libvirt, QEMU e tokens de OpenID Connect baseados em OAuth 2.0. Além disso, a Oracle fornece inicialização segura e criptografia de dados em trânsito e em repouso.

A Oracle vai além de apenas apoiar os avanços de software livre do Linux, ela também contribui para eles. A Oracle é uma das principais colaboradoras contínuas da comunidade de software livre de desenvolvimento do Linux. Um exemplo dessas contribuições é o amplamente aclamado Oracle Clustered File System 2 (OCFS2). O OCFS2 é um sistema de arquivos em cluster de uso geral, baseado em extensão, desenvolvido pela Oracle e contribuído para a comunidade Linux. É uma alternativa de software livre de categoria corporativa altamente eficaz para sistemas proprietários de arquivos em cluster, oferecendo alta

---

[6] Parceria Nacional de Garantia da Informação

[7] PHI eletrônicas ("EPHI") foram criptografadas conforme especificado na Regra de Segurança da HIPAA pelo "uso de um processo algorítmico para transformar dados em um formato em que há baixa probabilidade de atribuir significado sem o uso de um processo ou chave confidencial" (45 CFR § 164.304, definição de criptografia) e se esse processo ou chave confidencial que pode permitir a descriptografia não tiver sido violado. Para evitar violação do processo ou da chave confidencial, essas ferramentas de descriptografia devem ser armazenadas em um dispositivo ou em um local separado dos dados que são usados para criptografar ou descriptografar. O processo de criptografia identificado abaixo foi testado pelo NIST e considerado em conformidade com essa norma.
Os processos de criptografia válidos para dados em repouso são consistentes com a Publicação Especial 800-111 do NIST, "Guide to Storage Encryption Technologies for End User Devices."

[8] Estatísticas sobre ransomware e Comparitech

[9] How Cybercrime Funds North Korea's Nuclear Program

performance e alta disponibilidade. Outro é o DTrace. O DTrace é uma estrutura abrangente de rastreio dinâmico que fornece uma infraestrutura poderosa, permitindo que administradores, desenvolvedores e equipe de serviços respondam de forma concisa a perguntas arbitrárias sobre o comportamento do SO Linux e dos programas de usuário em tempo real. Ele simplifica bastante a análise de causa-raiz, que é extremamente importante para o DevSecOps durante o testdev, para solucionar problemas com rapidez e precisão. Essas são apenas algumas das contribuições da Oracle. A Oracle fornece código pré-lançamento no GitHub.

O Oracle Linux tem validação FIPS 140-2. E atualmente o Oracle Linux é a única distribuição Linux na Lista de produtos conformes da NIAP[10].

Impacto conhecido na performance do DevSecOps no Linux e as respostas do Oracle Linux

Quando o SO Linux subjacente faz o trabalho pesado na performance, os processos e aplicativos do DevSecOps precisam fazer muito menos. Alguns talvez questionem: Como a otimização de performance é um problema de segurança do DevSecOps? Segurança e performance andam de mãos dadas. Os processos de segurança frequentemente consomem muitos recursos. Maior performance permite que mais dessa performance seja alocada à segurança integrada sem reduzir a performance aceitável do aplicativo. A experiência de 40 anos da Oracle como banco de dados dominante no mundo lhe proporcionou conhecimento privilegiado e uma perspectiva única sobre como otimizar a segurança e a performance de cargas de trabalho críticas.

O Oracle Database é uma infraestrutura de software subjacente fundamental. Sua performance afeta e é afetada pela segurança. Tornar o banco de dados mais eficiente e otimizar a performance permite mais funções de segurança sem afetar a performance do aplicativo de banco de dados. O SO Oracle Linux também é uma infraestrutura de software subjacente fundamental. A Oracle está aplicando essa experiência comprovada de 40 anos de produção ao cenário de performance do Linux.

Limitações de otimização de performance do DevSecOps no Linux

As distribuições Linux da Red Hat, SUSE e Ubuntu não têm as décadas de experiência em otimização de segurança e performance de banco de dados da Oracle. Elas não podem aproveitar o conhecimento que não possuem. Assim, elas deixam que os desenvolvedores de aplicativos otimizem a performance. Isso representa mais trabalho para os desenvolvedores. E frequentemente retarda o DevSecOps. E, como afirmado anteriormente, a segurança costuma afetar negativamente a performance do aplicativo, o que, por sua vez, retarda ainda mais o tempo de conclusão do DevSecOps. Todas as distribuições Linux aproveitam os aprimoramentos de performance de software livre. Poucas distribuições enfatizam a otimização da performance do aplicativo/banco de dados.

Como o Oracle Linux otimiza a performance para DevSecOps

A Oracle enfatiza especificamente a otimização de performance. O Oracle Linux é o padrão de desenvolvimento da Oracle. Hoje, é a base para todos os produtos e serviços da Oracle. A nuvem pública Oracle é construída com base no Oracle Linux. Os sistemas projetados pela Oracle, incluindo Exadata, Exadata Cloud at Customer (ECC), Private Cloud Appliance (PCA), Private Cloud at Customer (PCC), Oracle Database Appliance (ODA), Oracle Zero Data Loss Recovery Appliance (ZDLRA) e Oracle Big Data Appliance (BDA) são todos construídos com base no Oracle Linux. A maioria dos aplicativos da Oracle é desenvolvida com base no Oracle Linux. Portanto, a Oracle se beneficia muito de ter a otimização de performance integrada ao Oracle Linux. E a otimização de performance do Linux é um dos principais focos da Oracle.

O Oracle Linux tem muitas otimizações de performance disponíveis, incluindo:

- Performance aprimorada de memória. O Oracle Linux procura localizar melhor os processos próximos à memória dele e colocar melhor as cargas de trabalho que não cabem em um único nó NUMA.

[10] Oracle Linux certified under Common Criteria and FIPS 140-2

- A otimização de performance Java de referência SPECjbb®[11] oferece uma melhoria de performance até 3,6 vezes, que ajuda a eliminar a contenção de bloqueio.
- Acelera a performance de dispositivos de bloco mais lentos com o bcache, que simplifica o uso de SSDs como cache de bloco. Isso fornece milhões de IOPS na memória de classe de armazenamento (SCM) e SSDs flash NVMe com um novo subsistema de camadas de blocos com filas múltiplas em escala.
- As equipes de engenharia do Oracle Database e do Oracle Linux colaboram continuamente em melhorias e otimizações para reforçar a performance dos aplicativos de banco de dados. Alguns exemplos incluem:
    - Os mecanismos tradicionais de comunicação interprocessos (IPC) tendem a exibir problemas de estabilidade quando sujeitos a cargas pesadas. A Oracle foi pioneira em uma nova abordagem chamada Reliable Datagram Sockets (RDS). O RDS é um protocolo sem conexão de baixa latência para entregar datagramas de maneira confiável a milhares de terminais. O RDS resulta em significativamente menos retransmissões. Isso é especialmente útil durante os períodos de pico de processamento, porque melhora muito a performance do banco de dados no Linux. A Oracle contribuiu com o código RDS para a comunidade de software livre. Agora ele faz parte do kernel do Linux.
    - A Oracle aproveitou o RDS Linux, simplificando o código do Oracle Database. Ela removeu o código de usuário, agora desnecessário, que havia resolvido os problemas de instabilidade antes do RDS. Isso reduziu o consumo de CPU do banco de dados, acelerando a performance.
    - Extensas melhorias de performance e escalabilidade para o planejador de processos, gerenciamento de memória, sistemas de arquivos e aplicação de rede. Ele foi ajustado para ter uma performance melhor e mais rápida nas configurações x86 com vários núcleos de CPU e grandes quantidades de memória principal.
    - Bibliotecas e chamadas de sistema otimizadas melhoram a performance das consultas ao Oracle Database.
    - Foi desenvolvido o Database Smart Flash Cache para Oracle Linux a fim de acelerar IOs para cargas de trabalho de banco de dados com leitura intensiva. O Database Smart Flash Cache permite que o cache de buffer do banco de dados se expanda além da área global do sistema (SGA) na memória principal para o cache de segundo nível que reside em um dispositivo flash ou SCM. Como a SCM tem leituras de três a cinco vezes mais rápida[12] do que SSDs flash, os quais estão, por sua vez, em uma ordem de magnitude mais rápida do que a dos discos rígidos, o Database Smart Flash Cache acelera significativamente a performance do banco de dados. Isso é feito apenas pelo custo da SCM ou do SSD flash.
    - Como discutido anteriormente, a Oracle contribui com todas as melhorias do sistema operacional Linux a montante para a comunidade Linux de software livre. Dessa forma, cargas de trabalho de aplicativos não Oracle e o DevSecOps também podem aproveitar essas otimizações.

As otimizações de performance do Oracle Linux são perfeitas e transparentes para o DevSecOps, economizando etapas, testes e, o mais importante, tempo.

Limitações de otimização de desempenho do banco de dados do DevSecOps no Linux

A maioria dos aplicativos e microsserviços tira proveito de um banco de dados. Escolher o banco de dados correto pode significar o sucesso ou o fracasso do projeto de DevSecOps. Muito poucos bancos de dados aproveitam as otimizações de desempenho do Linux. Menos ainda aproveitam as otimizações de desempenho de hardware da Intel ou AMD. Isso geralmente é bastante frustrante para os desenvolvedores, pois os força a tentar obter mais desempenho do código do aplicativo ou da infraestrutura geral. Fazer isso aumenta o tempo para a conclusão e, com frequência, os custos de infraestrutura.

[11] Notas sobre a liberação para UEK Release 4

[12] A SCM deveria ter latência 10 vezes menor que os SSDs flash NVMe, porque o 3D XPOINT tem latência 10 vezes menor que o Flash MLC NAND. Os resultados do mundo real obtidos por fornecedores de armazenamento (Pure Storage, Dell e NetApp) mostraram que o controlador de SCM na unidade reduz as diferenças gerais de latência em 50% a 70%, o que equivale a latência de 3-5 vezes mais baixa.

Como o Oracle Linux melhora a performance do Oracle Database para DevSecOps

O banco de dados mais essencial nas últimas quatro décadas foi o Oracle Database. É o primeiro banco de dados abrangente do mundo[13] que oferece suporte à grande maioria das metodologias populares de análise, incluindo: relacional, valor da chave, série temporal, JSON, XML, objeto, documento, espacial, gráfico e aprendizado de máquina de IA. Os Oracle Databases não fornecem apenas ferramentas de máquina de IA. Está disponível um amplo conjunto de algoritmos plug-and-play, o que significa que não é necessário nenhum cientista de programação ou de dados para aproveitar o aprendizado de máquina de IA da Oracle. E todos os diferentes recursos de análise podem ter acesso aos mesmos dados. Os bancos de dados conectáveis (PDBs) e os bancos de dados de contêineres (CDBs) multilocatários da Oracle permitem que vários tipos de banco de dados utilizem uma cópia física de dados, reduzindo a infraestrutura de armazenamento. Menos infraestrutura de armazenamento se traduz em tarefas e cargas de trabalho muito reduzidas.

A Oracle e a Intel trabalharam em estreita colaboração para otimizar e dimensionar a performance dos aplicativos do Oracle Database em execução no Oracle Linux. Por exemplo:

- A Intel otimizou os algoritmos de threading de CPU que permitem ao Oracle Database melhorar a escalabilidade de NUMA, aproveitando as instruções SIMD e AVX da Intel.
- A Oracle modificou o Oracle Database para tirar proveito da biblioteca multi-threaded Intel® IPP (Intel® Integrated Performance Primitives). Isso acelera a compactação/descompactação colunar, bem como as operações de criptografia.
- Os Oracle Databases usam a Oracle Hybrid Columnar Compression (HCC) com o Oracle Linux. A HCC obtém uma redução de dados de 10 a 15 vezes ou mais[14]. Os melhores algoritmos de redução de dados por deduplicação e compactação obtêm uma redução de dados de apenas 2 a 5 vezes nos Oracle Databases[15]. Isso permite que o Oracle Database seja executado mais rapidamente e consuma menos armazenamento caro.
- Os aplicativos Oracle Database compilados no Oracle Linux podem obter a melhor performance dos aplicativos Linux utilizando o compilador otimizado da Intel.

Isso significa que aplicativos baseados no Oracle Database em execução no Oracle Linux obterão a melhor performance em comparação com qualquer outra distribuição. E, como mencionado anteriormente, performance e segurança andam de mãos dadas. Uma companhia de seguros muito grande descobriu isso quando testou o Oracle Database 11G em Red Hat e em Oracle Linux. A infraestrutura de hardware era idêntica em ambos os casos. Eles descobriram uma performance de taxa de transferência não trivial de 15% a 20% maior no Oracle Linux seguro[16].

Gargalos conhecidos na implantação do DevSecOps no Linux e as respostas do Oracle Linux

Poucas pessoas gostam de reescrever ou modificar códigos sem necessidade. Mas, com muita frequência, o código deve ser modificado antes de ser colocado em produção. Uma das principais razões para isso é que o ambiente do DevSecOps é diferente do ambiente de produção. As nuvens públicas podem estar em uma versão diferente do SO Linux de outras nuvens públicas ou de versões locais. Cada ambiente pode estar em um nível diferente de correção de segurança implementada ou ter uma distribuição Linux completamente diferente. Embora as distribuições Linux sejam geralmente compatíveis, pode haver e há mesmo diferenças significativas.

Problemas de implantação de aplicativos do DevSecOps no Linux

Se o ambiente de desenvolvimento do DevSecOps for diferente dos ambientes de produção, o código e os processos precisarão ser alterados para produção e teste, retardando as implantações finais. Fica mais

[13] Classificação de mecanismo de banco de dados. A pesquisa em cada banco de dados deixa claro que a Oracle fornece atualmente o único banco de dados que suporta OLTP, OLAP, data warehousing, séries temporais, documento, valor da chave, objeto, JSON, XML, espacial e gráfico no mesmo banco de dados, tornando-o o primeiro banco de dados abrangente.

[14] De acordo com a documentação do Oracle Database, Exadata e ZFS, a HCC pode atingir até 50 vezes de redução de dados para dados de arquivo. Para a maioria dos data warehouses, normalmente os engenheiros de sistema da Oracle obtêm uma redução de 10 a 15 vezes, conforme relatado pela Dragon Slayer Consulting em 2019.

[15] De acordo com a Dell EMC, HPE, Pure Storage, Hitachi, NetApp e vários outros fornecedores de armazenamento, a deduplicação de Oracle Databases atinge seu ponto máximo, na melhor das hipóteses, em 5 vezes, embora tipicamente esteja mais próxima de 2,5 vezes, conforme relatado pela Dragon Slayer Consulting em 2019.

[16] Estudo de caso da Oracle

complicado em ambientes híbridos, especialmente quando as distribuições Linux talvez não sejam completamente compatíveis. Os aplicativos talvez não correspondam às expectativas ou aos acordos de nível de serviço ou talvez não funcionem. É apenas mais um problema do DevSecOps.

Como o Oracle Linux simplifica as implantações de produção de aplicativo no DevSecOps

Como mencionado anteriormente, a Oracle construiu todo o seu negócio com base no Oracle Linux. Todos os aplicativos desenvolvidos no Oracle Linux também serão executados sem modificação no Oracle Exadata, Oracle Exadata Cloud at Customer, Oracle Database Appliance, Oracle Private Cloud Appliance, Oracle Private Cloud at Customer e na nuvem pública da Oracle. Desenvolva uma vez e execute em qualquer lugar.

Quanto à compatibilidade entre o Oracle Linux e o Red Hat Linux, a Oracle trata toda e qualquer incompatibilidade como se fosse um erro. Nos 13 anos em que a Oracle distribui o Oracle Linux, nunca foi aberto um chamado de incompatibilidade[17].

Outras vantagens do DevSecOps no Oracle Linux

A Oracle é a primeira a entregar operações autônomas de Linux na nuvem com o Oracle Autonomous Linux:

- Provisionamento automático
- Ajuste de escala automático
- Ajuste automático
- Atualização e correção online automáticas
- Monitoramento e correção de segurança automáticos

Atualmente, o Autonomous Linux está disponível apenas na Oracle Cloud. Contudo, alguns desses recursos autônomos podem ser replicados utilizando ferramentas padrão no Oracle Linux.

Conclusão

O DevSecOps está navegando em um território novo, construindo a segurança desde o início. Fazer isso sem comprometer a performance ou modificar o código na implantação de produção é complicado e difícil. O Oracle Linux simplifica tudo.

Não resta dúvida de que a melhor distribuição Linux para o DevSecOps é o Oracle Linux.

Para obter mais informações sobre o DevSecOps no Oracle Linux

Acesse: Oracle Linux

Artigo patrocinado pela Oracle. **Sobre a Dragon Slayer Consulting:** Marc Staimer, como Presidente e CDS da Dragon Slayer Consulting, uma empresa de 22 anos de atuação de Beaverton, OR, EUA, é conhecido por seu entendimento profundo e aguçado dos problemas dos usuários, especialmente com armazenamento, rede, aplicativos, serviços em nuvem, proteção de dados e virtualização. Marc publicou milhares de artigos e dicas de tecnologia da perspectiva do usuário para publicações online de renome internacional, incluindo muitos dos sites Searchxxx.com da TechTarget, Network Computing e GigaOM. Além disso, Marc também apresentou centenas de artigos, webinars e seminários a muitos gigantes conhecidos do setor, como: Brocade, Cisco, DELL, EMC, Emulex (Avago), HDS, HPE, LSI (Avago), Mellanox, NEC, NetApp, Oracle, QLogic, SanDisk e Western Digital. Ele também prestou serviços semelhantes a fornecedores/startups menores e menos conhecidos, incluindo: Asigra, Cloudtenna, Clustrix, Condusiv, DH2i, Diablo, FalconStor, Gridstore, ioFABRIC, Nexenta, Neuxpower, NetEx, NoviFlow, Pavilion Data, Permabit, Qumulo, SBDS, StorONE, Tegile e muitos outros. Suas apresentações como palestrante costumam ter casa cheia, por causa das informações pragmáticas e imediatamente úteis fornecidas. Você pode entrar em contato com Marc pelos seguintes meios: marcstaimer@me.com, (503)-312-2167, em Beaverton OR, 97007.

[17] Oracle OpenWorld, setembro de 2019, palestra principal de Larry Ellison na marca de 15:50