# Abordagem de segurança em camadas para Kubernetes e containers

Como proteger containers na compilação, implantação e execução

## Sumário




facebook.com/redhatinc
@redhatbr
linkedin.com/company/red-hat-brasil

## Introdução

Os containers têm chamado muita atenção porque conseguem empacotar uma aplicação e suas respectivas dependências em apenas uma imagem. Essa imagem pode ser utilizada durantes as fases de desenvolvimento, teste e produção. Com os containers, é mais fácil assegurar a consistência em todos os ambientes e em vários destinos de implantação, como servidores físicos, máquinas virtuais e nuvens públicas ou privadas. Eles ajudam as equipes a desenvolver e gerenciar com mais facilidade as aplicações que aumentam a agilidade dos negócios.

- **Aplicações:** com os containers, os desenvolvedores têm mais facilidade para criar e utilizar uma aplicação e suas dependências como uma unidade. É possível implantá-los em poucos segundos. Em um ambiente containerizado, o processo de compilação do software é o estágio do ciclo de vida em que o código da aplicação é integrado às bibliotecas do ambiente de execução necessárias.
- **Infraestrutura:** os containers representam os processos da aplicação em área restrita em um kernel do sistema operacional Linux® compartilhado. Eles são mais compactos, mais leves e menos complexos do que as máquinas virtuais. Os containers também são portáteis em diferentes ambientes, como on-premise e plataformas de nuvem pública.

O Kubernetes é a melhor plataforma de orquestração de containers para as empresas. Proteger os containers se tornou uma tarefa ainda mais importante, já que muitas organizações agora executam seus serviços essenciais neles. Neste documento, você verá a descrição dos principais elementos da segurança de aplicações containerizadas.

## Segurança completa para containers e Kubernetes: camadas e ciclo de vida

A proteção de containers é muito semelhante à de qualquer outro processo em execução no Linux. Antes de implantar e executar o container, é preciso pensar na segurança em todas as camadas do stack da solução, bem como em todo o ciclo de vida da aplicação e do container. É importante observar que a segurança precisa ser um processo contínuo também integrado a todo o ciclo de vida da TI. Além disso, a segurança deve ter a capacidade de se ampliar para responder a novas ameaças e soluções à medida que elas aparecem. Veja na Figura 1 uma abordagem completa de segurança de containers.

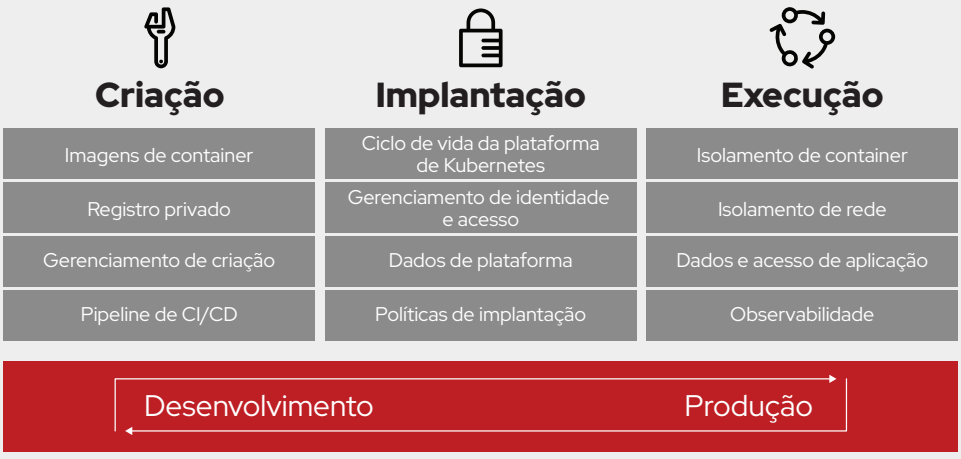


Figura 1. A segurança completa dos containers engloba a proteção da compilação, implantação e do ambiente de execução, além de ampliar esse processo com ferramentas avançadas quando apropriado.

Com os containers, os desenvolvedores têm mais facilidade para criar e utilizar uma aplicação e suas dependências como uma unidade. Os containers também simplificam o uso máximo dos servidores, habilitando as implantações de aplicações multitenant em um host compartilhado. É possível implantar várias aplicações em um único host inicializando e encerrando containers individuais conforme necessário. Ao contrário da virtualização tradicional, você não precisa de um hipervisor para gerenciar sistemas operacionais guest em cada máquina virtual. Com os containers, você virtualiza os processos da aplicação, e não o hardware.

Naturalmente, é muito difícil que as aplicações sejam entregues em um único container. Até mesmo as mais simples costumam ter um front-end, um back-end e um banco de dados. E implantar aplicações avançadas baseadas em microsserviços nos containers significa implantar vários deles. Às vezes, isso é feito no mesmo host ou distribuído entre vários hosts ou nós, como mostra a Figura 2.

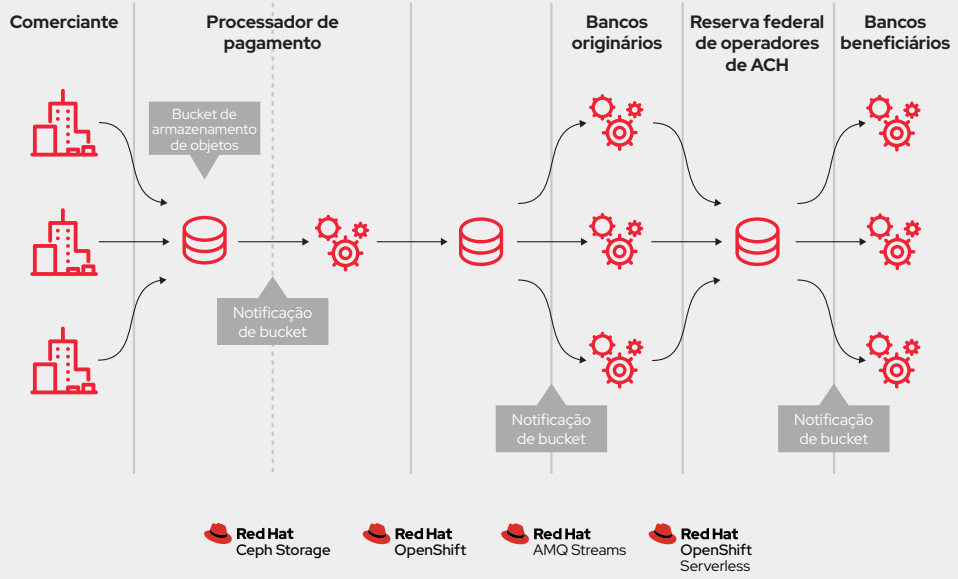


Figura 2. Os ambientes de containers podem ser complexos e distribuídos por vários nós.

Ao gerenciar a implantação de um container em escala, considere o seguinte:

- Quais containers devem ser implantados em quais hosts?
- Qual host tem mais capacidade?
- Quais containers precisam acessar uns aos outros e como eles se descobrirão?
- Como controlar o acesso a recursos compartilhados (rede e armazenamento, por exemplo) e como gerenciá-los?
- Como monitorar a integridade do container?
- Como escalar automaticamente a capacidade das aplicações para atender à demanda?
- Como habilitar o autosserviço do desenvolvedor e atender aos requisitos de segurança?

É possível criar o próprio ambiente de gerenciamento de containers. Para isso, você precisa de tempo para integrar e gerenciar cada componente. Também é possível implantar uma plataforma de aplicações em container com recursos integrados de segurança e gerenciamento. Usando essa abordagem, sua equipe se concentra na criação de aplicações que agregam valor aos negócios, em vez de reformular a infraestrutura.

O Red Hat® OpenShift® Container Platform oferece uma plataforma Kubernetes empresarial e consistente em nuvem híbrida para a criação e a escala de aplicações containerizadas. A utilização do Kubernetes em toda a empresa requer a adoção de mais recursos para integrar a segurança às aplicações, proteger o ambiente de execução dos containers e automatizar as políticas que permitem gerenciar a proteção da implantação deles.

## Integre a segurança às aplicações

É importante integrar a segurança às aplicações nas implantações nativas em nuvem. Para proteger as aplicações containerizadas, você precisa:

1. Incluir conteúdo de confiança nos containers.
2. Usar um registro de container empresarial.
3. Controlar e automatizar os containers de compilação.
4. Integrar a segurança ao pipeline da aplicação.

### 1. Use conteúdo de confiança nos containers

Ao gerenciar a segurança, você precisa considerar o que está dentro do container. Atualmente, as aplicações e as infraestruturas são formadas por componentes com disponibilidade imediata. Muitos deles são pacotes open source, como ocorre com o sistema operacional Linux, o Apache Web Server, o Red Hat JBoss® Enterprise Application Platform, o PostgreSQL e o Node.js. As versões containerizadas desses pacotes também estão disponíveis para você não precisar criá-los. No entanto, como acontece com qualquer código vindo de uma fonte externa, é necessário saber a origem dos pacotes, quem os criou e se há códigos maliciosos neles. Pergunte a si mesmo:

- O conteúdo do container pode danificar minha infraestrutura?
- Há vulnerabilidades conhecidas na camada da aplicação?
- As camadas do sistema operacional e do ambiente de execução no container estão atualizadas?
- Com que frequência o container será atualizado? E como saberei quando ele está atualizado?

Há muitos anos, a Red Hat empacota e entrega conteúdo Linux confiável no Red Hat Enterprise Linux e em todo o nosso portfólio de soluções. Agora, a Red Hat oferece o mesmo conteúdo confiável empacotado como containers Linux. Com a criação do Red Hat Universal Base Images, você pode usar as imagens de container da Red Hat e ter maior confiabilidade, segurança e desempenho em todos os ambientes onde os containers Linux compatíveis com o Open Container Initiative (OCI) são executados. Ou seja, é possível criar uma aplicação containerizada no Red Hat Universal Base Image, enviá-la para o registro do container que quiser e compartilhá-la.

E, com o Red Hat Ecosystem Catalog, você aproveita uma grande quantidade de operadores e imagens certificadas para vários ambientes de execução de linguagem, middleware, bancos de dados e muito mais. Os operadores e containers certificados da Red Hat funcionam em qualquer ambiente em que o Red Hat Enterprise Linux é executado, como bare-metal, máquinas virtuais e nuvem, além de receber o suporte da nossa empresa e parceiros.

A Red Hat sempre monitora a integridade das imagens que entrega. Com o Container Health Index, classificamos o "grau" de cada imagem de container, detalhando como elas devem ser selecionadas, consumidas e avaliadas para atender às necessidades dos sistemas de produção. Parte da classificação tem como base a maturidade e o impacto da errata de segurança não aplicada em todos os componentes de um container. Isso oferece uma classificação agregada do grau de segurança do container, que tanto os especialistas de segurança quanto os leigos conseguem entender.

A Red Hat também recompila as imagens de container e as envia ao registro público quando lança atualizações de segurança. Por exemplo, as correções CVE-2019-5736 no runc, CVE-2019-11091 no MDS e CVE-2019-14835 no VHOST-NET. Por meio do Red Hat Security Advisories, enviamos alertas sobre qualquer problema detectado nas imagens de container certificadas e direcionamos você para a versão que foi atualizada. Assim, você atualiza todas as aplicações que usam essa imagem.

Haverá casos em que você precisará de um conteúdo que a Red Hat não oferece. Recomendamos a adoção de ferramentas de verificação de containers que usam bancos de dados de vulnerabilidade atualizados com frequência. Dessa forma, você sempre tem as informações mais recentes sobre as vulnerabilidades conhecidas ao usar imagens de container de outras fontes. A lista de vulnerabilidades conhecidas está em constante evolução. Por isso, quando fizer o primeiro download das imagens de container, verifique o conteúdo delas e acompanhe sempre o status de vulnerabilidade de todas as imagens aprovadas e implantadas. É isso que a Red Hat faz com suas próprias imagens de container.

### 2. Use um registro de container empresarial para aumentar a segurança do acesso às imagens

Naturalmente, suas equipes estão criando containers que acrescentam conteúdo às imagens de container públicas que você faz download. É preciso gerenciar o acesso e utilização dessas imagens de container, bem como daquelas criadas internamente, da mesma forma que você gerencia outros tipos de binários. Há vários registros privados que oferecem suporte ao armazenamento de imagens de container. Recomendamos que você escolha aquele que ajude a automatizar as políticas de uso das imagens de container armazenadas no registro.

O Red Hat OpenShift inclui um registro privado com funcionalidades básicas para gerenciar as imagens de container. Ele oferece controle de acesso baseado em função (RBAC) para você determinar quem pode extrair e enviar imagens de container específicas. O Red Hat OpenShift também é compatível com a integração de outros registros privados que talvez já estejam em uso na sua empresa, como o Artifactory da JFrog e o Sonatype Nexus.

O Red Hat Quay está disponível como um registro empresarial independente. Ele oferece muitos outros recursos como replicação geográfica e acionadores de imagens de compilação.

O verificador de segurança do Red Hat Quay é baseado na plataforma open source do projeto Clair para detectar vulnerabilidades em todas as imagens nessa solução. É possível integrar o Red Hat OpenShift Container Security Operator ao Red Hat Quay para ver em todo o cluster, usando o console do OpenShift, as vulnerabilidades conhecidas encontradas nas imagens implantadas.

### 3. Controle e automatize as imagens de containers de compilação

Gerenciar esse processo de compilação é fundamental para proteger o stack de software. Ao aderir a filosofia de "compilar uma vez, implantar em qualquer ambiente", você assegura que o resultado desse processo de compilação seja exatamente o que foi implantado na produção. Também é importante preservar a imutabilidade dos containers. Em outras palavras, evite aplicar patches nos containers em execução e prefira recompilá-los e reimplantá-los.

O Red Hat OpenShift oferece vários recursos para automatizar compilações de acordo com eventos externos, o que aumenta a segurança das imagens personalizadas.

- Os acionadores do Red Hat Quay oferecem um mecanismo para gerar uma compilação de repositório de um Dockerfile com base em um evento externo, como um webhook ou envios do GitHub, BitBucket e GitLab.
- O Source-to-image (S2I) é um framework open source para combinar código-fonte e imagens base (Figura 3). Com ele, as equipes de desenvolvimento e operações têm facilidade para colaborar em um ambiente de compilação reproduzível. Quando um desenvolvedor atualiza o código com o git, no S2I, o Red Hat OpenShift pode:
  - Acionar a montagem automática de uma nova imagem a partir de artefatos disponíveis, incluindo a imagem base do S2I e o código recém-atualizado. Isso é feito com webhooks no repositório do código ou algum outro processo de integração contínua (CI) automatizada.
  - Implantar automaticamente a imagem recém-criada para testes.
  - Colocar a imagem testada no status de produção e implantar a nova imagem automaticamente usando o processo de implantação e integração contínuas (CI/CD).

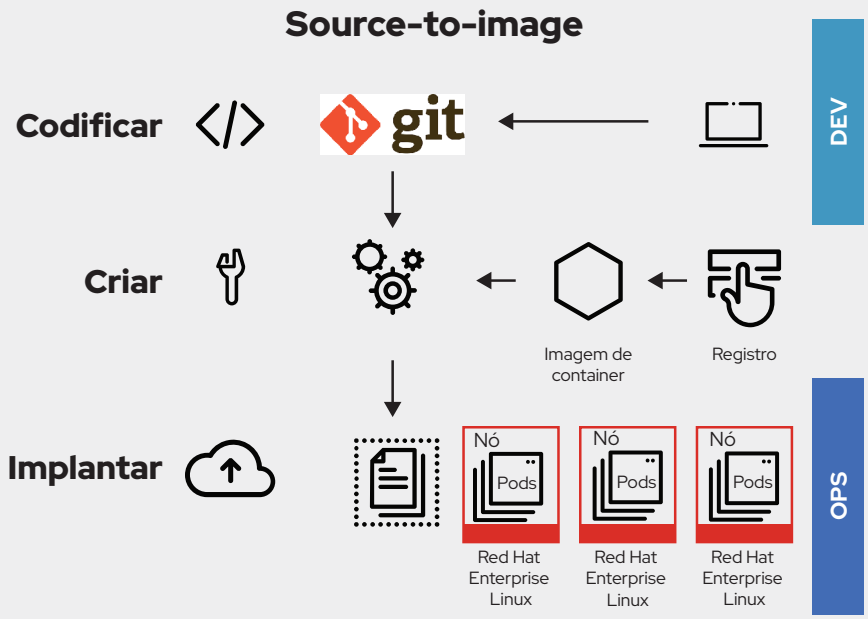


Figura 3. O S2I é um fluxo de trabalho e kit de ferramentas para criar imagens de container reproduzíveis e prontas para execução a partir do código-fonte.

- Use os fluxos de imagens do Red Hat OpenShift para vigiar as mudanças nas imagens externas implantadas no cluster. Esses fluxos são compatíveis com todos os recursos nativos do Red Hat OpenShift, como compilações e implantações, tarefas, controladores de replicação e conjuntos de réplicas. Ao vigiar os fluxos, as compilações e as implantações são notificadas quando há a inclusão ou modificação de novas imagens e respondem com o lançamento automático de uma compilação ou implantação, respectivamente.

  Por exemplo, imagine uma aplicação criada com três camadas de imagens de container: base, middleware e aplicação. Um problema é descoberto na imagem base, que é recompilada pelo Red Hat e enviada ao Red Hat Ecosystem Catalog. Com o fluxo de imagens habilitado, o Red Hat OpenShift detecta que a imagem foi alterada. No caso das compilações que dependem dessa imagem e que têm acionadores definidos, o Red Hat OpenShift fará automaticamente a recompilação da imagem da aplicação incorporando a imagem base corrigida.

  Depois de concluir a compilação, a imagem personalizada atualizada é enviada para o registro interno do Red Hat OpenShift. O Red Hat OpenShift detecta de imediato as alterações nas imagens no registro interno e, no caso das aplicações com acionadores definidos, implanta automaticamente a imagem atualizada. Assim, o código executado em produção é sempre igual ao da imagem atualizada mais recentemente. Todos esses mecanismos funcionam em conjunto para integrar os recursos de segurança ao pipeline e processo de CI/CD.

### 4. Integre a segurança ao pipeline da aplicação

O Red Hat OpenShift conta com instâncias integradas do Tekton e do Jenkins para CI: esse é um pipeline Kubernetes de CI/CD de próxima geração compatível com os containers (incluindo a funcionalidade serverless). A solução também oferece APIs RESTful avançadas que você pode usar para integrar a própria compilação ou ferramentas de CI/CD, incluindo um registro privado de imagens.

Uma prática recomendada de proteção de aplicações é integrar os testes de segurança automatizados ao pipeline, incluindo o registro, o ambiente de desenvolvimento integrado (IDE) e as ferramentas de CI/CD.

**Registro:** você precisa verificar as imagens de container no seu registro privado. Use o Red Hat Quay com o verificador de segurança do Clair para enviar aos desenvolvedores notificações sobre as vulnerabilidades descobertas. É possível integrar o OpenShift Container Security Operator ao Red Hat Quay para ver em todo o cluster, usando o console do OpenShift, as vulnerabilidades conhecidas encontradas nas imagens implantadas. Se preferir, o Red Hat Ecosystem Catalog conta com várias soluções externas certificadas para realizar a verificação de containers.

**IDE:** usando os plugins do ambiente de desenvolvimento integrado (IDE) do Red Hat Dependency Analytics, você recebe avisos de vulnerabilidade e dicas de correção nas dependências do projeto assim que o código chega ao IDE.

**CI/CD:** integre os verificadores à CI para analisar as vulnerabilidades conhecidas em tempo real. Assim, é possível catalogar os pacotes open source no container, ver notificações sobre qualquer vulnerabilidade conhecida e receber informações quando novas vulnerabilidades forem descobertas em pacotes verificados anteriormente.

Além disso, inclua no processo de CI as políticas que sinalizam as compilações com problemas detectados por verificações de segurança. Dessa forma, sua equipe pode tomar as medidas adequadas para resolver esses problemas o mais rápido possível.

Por fim, recomendamos que você assine os containers personalizados para ter certeza de que eles não serão adulterados entre a compilação e a implantação.

## Como gerenciar a configuração, segurança e conformidade da implantação

A segurança eficaz da implantação inclui a automação das suas políticas e a proteção da plataforma Kubernetes. O Red Hat OpenShift oferece os seguintes recursos prontos para uso:

1. Gerenciamento do ciclo de vida e configuração da plataforma.
2. Gerenciamento de identidade e acesso.
3. Proteção do armazenamento anexado e dos dados da plataforma.
4. Políticas de implantação.

### 5. Gerenciamento do ciclo de vida e configuração da plataforma

Publicado no terceiro trimestre de 2019, o artigo Cloud Native Computing Foundation (CNCF) Kubernetes Security Audit revelou que a principal ameaça à segurança do Kubernetes é a complexidade gerada ao configurar e reforçar os componentes dele. O Red Hat OpenShift ajuda você a superar esse desafio com os operadores Kubernetes.

Os operadores são um método de empacotar, implantar e gerenciar aplicações nativas do Kubernetes. Eles funcionam como um controlador personalizado que amplia a interface de programação de aplicações (API) do Kubernetes com a lógica específica exigida para gerenciar a aplicação. Todos os componentes da plataforma do Red Hat OpenShift são empacotados em um operador, o que oferece gerenciamento, monitoramento e configuração automatizados. Os operadores individuais configuram diretamente componentes como o servidor da API e a rede definida por software (SDN). Já o operador na versão do cluster gerencia diversos outros deles em toda a plataforma. Com os operadores, é possível automatizar o gerenciamento do cluster, incluindo as atualizações, do kernel aos serviços mais superiores no stack.

Um dos principais benefícios da plataforma de aplicações em containers é habilitar o autosserviço do desenvolvedor. Assim, as equipes de desenvolvimento têm mais rapidez e facilidade para entregar aplicações criadas em camadas aprovadas. Com um portal de autosserviço, você oferece controle suficiente às equipes para promover a colaboração sem deixar de proporcionar segurança. O Operator Lifecycle Manager (OLM) oferece aos usuários do cluster do Red Hat OpenShift o framework para encontrar e usar operadores na implantação dos serviços necessários para habilitar as aplicações. Com o OLM, os usuários podem instalar, atualizar a atribuir controles de acesso baseados em função aos operadores disponíveis.

Para ajudar na conformidade, o Red Hat OpenShift inclui o Compliance Operator para você automatizar a conformidade da plataforma com os controles técnicos exigidos pelos frameworks correspondentes. Com o Compliance Operator, os administradores do Red Hat OpenShift descrevem o estado de conformidade desejado de um cluster, têm uma visão geral das falhas e descobrem maneiras de corrigi-las. O Compliance Operator avalia a conformidade de todas as camadas da plataforma, incluindo os nós que executam o cluster. O File Integrity Operator também está disponível para você realizar verificações de integridade frequentes nos arquivos nos nós do cluster.

### 6. Gerenciamento de identidade e acesso

Como o Kubernetes inclui uma grande variedade de recursos para os desenvolvedores e administradores, o RBAC e o gerenciamento de identidades reforçado são essenciais para a plataforma de aplicações em container. As APIs do Kubernetes são fundamentais para automatizar o gerenciamento de containers em escala. Por exemplo, as APIs são usadas para iniciar e validar solicitações, incluindo a configuração e implantação de pods e serviços.

A autorização e autenticação da API são essenciais para proteger a plataforma de aplicações em container. O servidor da API é um ponto central de acesso e precisa receber o mais alto nível de análise de segurança. O painel de controle do Red Hat OpenShift conta com autenticação

integrada, oferecida pelo operador Cluster Authentication. Os desenvolvedores, administradores e contas de serviço recebem tokens de acesso ao OAuth para se autenticarem na API. Como administrador, você pode possível configurar o provedor de identidades que quiser no cluster para que os usuários façam a autenticação antes de receber um token. Aceitamos nove provedores de identidade, incluindo os diretórios do Lightweight Directory Access Protocol (LDAP).

O RBAC de alta granularidade é habilitado por padrão no Red Hat OpenShift. Os objetos desse recurso determinam se um usuário tem permissão para executar uma determinada ação em um cluster. Os administradores do cluster podem usar funções e vinculações para controlar os níveis de acesso ao cluster do OpenShift e aos projetos dentro dele.

### 7. Proteção dos dados da plataforma

O Red Hat OpenShift reforça o Kubernetes por padrão para proteger os dados em trânsito. Isso também inclui opções de proteção para os dados em repouso.

O Red Hat OpenShift protege os dados em trânsito da plataforma ao:

- Criptografá-los via https em todos os componentes da plataforma de aplicações em container que se comunicam entre si.
- Enviar todas as comunicações com o painel de controle pelo Transport Layer Security (TLS).
- Assegurar que o acesso ao servidor de API seja baseado em tokens ou em certificados X.509.
- Usar a cota do projeto para limitar os danos causados por um token não autorizado.
- Configurar o etcd com os próprios certificados e autoridades de certificação. (No Kubernetes, o etcd armazena o estado mestre persistente, enquanto os outros componentes vigiam as mudanças no etcd para entrar em um estado especificado.)
- Alterar os certificados da plataforma automaticamente.

O Red Hat OpenShift protege os dados em repouso da plataforma ao:

- Criptografar os discos do Red Hat Enterprise Linux CoreOS e o armazenamento de dados do etcd para aumentar a segurança (opcional).
- Disponibilizar os Padrões de processamento de informações federais (FIPS) para o Red Hat OpenShift. O FIPS 140-2 é um padrão de segurança do governo americano usado para aprovar módulos criptográficos. Quando o Red Hat Enterprise Linux CoreOS é iniciado no modo FIPS, os componentes da plataforma do Red Hat OpenShift chamam os módulos criptográficos do Red Hat Enterprise Linux.

Os containers são úteis para as aplicações stateless e stateful. O Red Hat OpenShift é compatível com o armazenamento persistente e temporário. A proteção do armazenamento anexado é um elemento importante dos serviços de segurança stateful. O Red Hat OpenShift é compatível com vários tipos de armazenamento, incluindo o sistema de arquivos de rede (NFS), Elastic Block Stores (EBS) da Amazon Web Services (AWS), discos persistentes do Google Compute Engine (GCE), Azure Disk, iSCSI e Cinder.

Além disso, o Red Hat OpenShift Container Storage é uma solução de armazenamento persistente definido por software integrado ao Red Hat OpenShift Container Platform e otimizado para ele. O OpenShift Container Storage oferece armazenamento persistente altamente escalável para aplicações nativas em nuvem que exigem recursos como criptografia, replicação e disponibilidade na multicloud híbrida.

- O **volume persistente (PV)** pode ser ativado em um host de qualquer forma compatível com o provedor de recursos. Os provedores oferecem recursos diferentes, e os modos de acesso de cada volume persistente são definidos para os modos específicos que recebem suporte de um volume específico. Por exemplo, o NFS pode dar suporte a vários clientes de leitura/gravação, mas o volume persistente de um NFS específico pode ser exportado no servidor como somente leitura. Cada volume persistente tem seu próprio conjunto de modos de acesso que descreve os próprios recursos específicos. Alguns exemplos são ReadWriteOnce, ReadOnlyMany e ReadWriteMany.
- Para o **armazenamento compartilhado** (por exemplo, NFS, Ceph e Gluster), o truque é fazer com que o volume persistente de armazenamento compartilhado registre sua ID de grupo (gid) como uma anotação no recurso do PV. Quando o PV é chamado pelo pod, a gid anotada é adicionada aos grupos complementares do pod e dá a ele acesso ao conteúdo do armazenamento compartilhado.
- Para o **armazenamento em blocos** (por exemplo, EBS, discos persistentes do GCE e iSCSI), as plataformas de aplicações em container podem usar os recursos do SELinux para proteger a raiz do volume ativado nos pods sem privilégio. Assim, o volume ativado fica sendo de propriedade do container ao qual está associado e só pode ser visualizado por esse container.

É claro que você pode aproveitar os recursos de segurança disponíveis na solução de armazenamento escolhida.

### 8. Automatize as implantações baseadas em políticas

A segurança reforçada inclui políticas automatizadas que podem ser usadas para gerenciar a implantação do container e do cluster do ponto de vista da segurança.

- Implantação de containers baseada em políticas

É possível configurar os clusters do Red Hat OpenShift para permitir ou proibir a extração de registros de imagens específicos. Uma prática recomendada para os clusters de produção é permitir apenas as imagens que serão implantadas a partir do registro privado.

Com o plugin controlador de admissões de restrições de contexto de segurança (SCCs) do Red Hat OpenShift, você define um conjunto de condições que um pod precisa executar para ser aceito no sistema. As **restrições de contexto de segurança** permitem a eliminação de privilégios por padrão: um recurso importante e recomendado. As restrições de contexto de segurança (SCCs) do Red Hat OpenShift, por padrão, asseguram que nenhum container com privilégios seja executado nos nós de trabalho do OpenShift. O acesso às IDs de processo e à rede do host é negado por padrão.

Os usuários que têm as permissões exigidas podem ajustar as políticas padrão de SCC para que elas sejam mais permissivas, se assim for desejado.

Com o Red Had Advanced Cluster Management for Kubernetes, você aproveita o **gerenciamento avançado do ciclo de vida de aplicações** usando padrões open source para implantar aplicações por meio de políticas de posicionamento integradas aos controles de governança e pipelines de CI/CD existentes.

- Gerenciamento de vários clusters baseado em políticas

Implantar vários clusters é uma maneira útil de ter alta disponibilidade nas aplicações em várias zonas. Isso também proporciona funcionalidades para o gerenciamento comum das implantações ou migrações em vários provedores de nuvem, como a Amazon Web Services (AWS), o Google Cloud e o Microsoft Azure. Ao gerenciar vários clusters, as ferramentas de orquestração precisam oferecer a segurança necessária nas diferentes instâncias implantadas. Como sempre, a configuração, autenticação e autorização são essenciais, assim como a capacidade de transmitir

dados com segurança para as aplicações, onde quer que elas sejam executadas, e gerenciar as políticas de aplicação nos clusters. O Red Had Advanced Cluster Management for Kubernetes oferece:

- **Gerenciamento do ciclo de vida de vários clusters** para você criar, atualizar e excluir clusters do Kubernetes em escala com confiança e consistência.
- **Gestão de governança, riscos e conformidade baseada em políticas** para você configurar e manter automaticamente a consistência dos controles de segurança de acordo com os padrões empresariais do setor. Também é possível especificar uma política de conformidade e aplicá-la a um ou mais clusters gerenciados.

## Proteja as aplicações em execução

Além da infraestrutura, manter a segurança das aplicações é essencial. Para proteger as aplicações containerizadas, você precisa de:

1. Isolamento de containers.
2. Isolamento de rede e aplicações.
3. Proteção no acesso às aplicações.
4. Observabilidade.

### 9. Isolamento de containers

Para aproveitar todos os benefícios da tecnologia de orquestração e do empacotamento de containers, a equipe de operações precisa do ambiente certo para executar os containers. Ou seja, um sistema operacional que proteja os containers nos seus limites: protegendo o kernel do host a partir de container escapes, além de protegê-los uns dos outros.

Os containers são processos Linux com isolamento e confinamento de recursos para você executar aplicações em área restrita em um kernel de host compartilhado. A abordagem adotada para a proteção dos containers precisa ser igual à de qualquer outro processo em execução no Linux.

A publicação NIST Special Publication 800-190 recomenda o uso de um sistema operacional otimizado para containers para aumentar a segurança. O Red Hat Enterprise Linux CoreOS é o sistema operacional base do Red Hat OpenShift. Ele diminui o ambiente do host e o ajusta de acordo com os containers para reduzir a superfície de ataque. O Red Hat Enterprise Linux CoreOS inclui apenas os pacotes necessários para executar o Red Hat OpenShift, e o espaço do usuário dessa solução é de somente leitura. O teste, o controle de versão e o envio da plataforma são feitos com o Red Hat OpenShift. Além disso, ela é gerenciada pelo cluster. A instalação e as atualizações do Red Hat Enterprise Linux CoreOS são automáticas e sempre compatíveis com o cluster. A solução também aceita a infraestrutura que você quiser usar, herdando boa parte do ecossistema do Red Hat Enterprise Linux.

Todos os containers Linux em execução na plataforma do Red Hat OpenShift são protegidos por recursos avançados de segurança do Red Hat Enterprise Linux (integrados aos nós do Red Hat OpenShift). Isso inclui namespaces do Linux, SELinux, cGroups, recursos de sistema operacional e modo de computação segura (seccomp).

- Os namespaces do Linux criam a base do isolamento do container. Eles indicam aos processos que eles têm suas próprias instâncias de recursos globais. Os namespaces criam uma abstração que dá a entender que a execução está acontecendo no próprio sistema operacional dentro de um container.

- O SELinux oferece uma camada extra de segurança para manter os containers isolados uns dos outros e do host. Com o SELinux, os administradores impõem controles de acesso obrigatórios (MAC) a todos os usuários, aplicações, processos e arquivos. Ele funciona como uma parede de tijolos que impede o rompimento da abstração do namespace (acidentalmente ou de propósito). O SELinux reduz as vulnerabilidades do ambiente de execução dos containers e evita que os processos dos containers saiam da contenção quando bem configurado.
- Os cGroups (grupos de controle) limitam, representam e isolam o uso de recursos (por exemplo, CPU, memória, E/S de disco e rede) de um conjunto de processos. Use-os para evitar que os recursos do container sejam suplantados por outro container no mesmo host. Outra atribuição dos cGroups é controlar dispositivos falsos, um vetor de ataque comum.
- Use os recursos do Linux para bloquear privilégios em um container. Os recursos são unidades de privilégio distintas que podem ser ativadas ou desativadas de forma independente. Com eles, é possível executar ações como envio de pacotes brutos de protocolo da internet (IP) ou a vinculação a portas abaixo de 1024. Durante a execução dos containers, é possível eliminar vários recursos sem impactar a grande maioria das aplicações containerizadas.
- Por fim, um perfil de modo de computação segura (seccomp) pode ser associado a um container para restringir as chamadas de sistema disponíveis.

### 10. Isolamento de rede e aplicações

A segurança multitenant é essencial para o uso do Kubernetes em escala empresarial. Com a multiloção, diferentes equipes podem usar o mesmo cluster e evitar o acesso não autorizado aos ambientes uns dos outros. O Red Hat OpenShift é compatível com multilocação usando uma combinação de namespaces do kernel e do Kubernetes (projeto), SELinux, RBAC e políticas de rede.

- **Projetos do Red Hat OpenShift** são namespaces do Kubernetes com anotações SELinux. Eles isolam aplicações em equipes, grupos e departamentos. As vinculações e funções locais são usadas para controlar quem tem acesso a projetos individuais.
- **Restrições de contexto de segurança** permitem a eliminação de privilégios por padrão: um recurso importante e recomendado. As restrições de contexto de segurança (SCCs) do Red Hat OpenShift, por padrão, asseguram que nenhum container com privilégios seja executado nos nós de trabalho do OpenShift. O acesso às IDs de processo e à rede do host é negado por padrão.

Em geral, implantar aplicações avançadas baseadas em microsserviços nos containers significa implantar vários deles distribuídos em diversos nós. Esses microsserviços precisam descobrir uns aos outros e se comunicar entre si. Pensando na proteção da rede, você precisa de uma plataforma de aplicações em container que adote um único cluster e segmente o tráfego para isolar usuários, equipes, aplicações e ambientes diferentes nesse cluster. Também são necessárias ferramentas para gerenciar o acesso externo ao cluster e o acesso dos serviços dele a componentes externos. Para isolar a rede, você precisa destes recursos importantes:

- **Controle de tráfego de entrada.** O Red Hat OpenShift conta com o CoreDNS para oferecer um serviço de resolução de nomes aos pods. O roteador da solução (HAProxy) do Red Hat OpenShift é compatível com entradas e rotas para oferecer acesso externo aos serviços em execução no cluster. Ambos esses componentes oferecem suporte a políticas de passagem e recriptografia: respectivamente, um faz a criptografia e descriptografia do tráfego HTTP durante o encaminhamento dele, e o outro transmite o tráfego sem encerrar o TLS.

- **Namespaces de rede.** A etapa inicial da proteção da rede são os namespaces. Cada conjunto de containers (conhecido como "pod") recebe o próprio endereço IP e intervalo de porta ao qual se vincular, isolando as redes de pod umas das outras no nó. Os endereços IP do pod não dependem da rede física a que os nós do Red Hat OpenShift são conectados.
- **Políticas de rede.** A SDN do Red Hat OpenShift usa políticas de rede para realizar o controle de alta granularidade das comunicações entre os pods. É possível controlar o tráfego de rede entre qualquer pod de origem e de destino em portas e direções específicas. Quando as políticas de rede são configuradas no modo multitenant, cada projeto recebe a própria ID de rede virtual, o que isola as redes umas das outras no nó. Nesse modo, por padrão, os pods do projeto podem se comunicar entre si. No entanto, os pods de diferentes namespaces não podem fazer o envio ou recebimento de pacotes de pods ou serviços de um projeto distinto.
- **Controle de tráfego de saída.** O Red Hat OpenShift também oferece a capacidade de controlar o tráfego de saída dos serviços em execução no cluster usando o roteador ou métodos de firewall. Por exemplo, é possível usar a lista de permissões de IPs para oferecer acesso a bancos de dados externos.

### 11. Proteção no acesso às aplicações

A segurança das aplicações inclui o gerenciamento dos usuários delas, bem como a autenticação e a autorização da API.

- **Controle do acesso dos usuários**

Os recursos de single sign-on (SSO) na web são parte essencial das aplicações atuais. As plataformas de aplicações em container podem incluir vários serviços containerizados para os desenvolvedores usarem na criação de aplicações. O Red Hat Single Sign-On é um serviço de federação, single sign-on na web e autenticação baseada em OpenID Connect ou Security Assertion Markup Language (SAML) 2.0. Essa solução tem suporte completo, é pronta para uso e baseada no projeto upstream Keycloak. O Red Hat Single Sign-On conta com adaptadores de cliente para o Red Hat Fuse e para o Red Hat JBoss Enterprise Application Platform. A solução possibilita a autenticação e o single sign-on na web para aplicações Node.js. Ela também pode ser integrada aos serviços de diretório baseados no LDAP, incluindo o Microsoft Active Directory e o Red Hat Enterprise Linux Identity Management. O Red Hat Single Sign-On também se integra a provedores com login por mídia social, como Facebook, Google e Twitter.

- **Controle do acesso de API**

As APIs são fundamentais para aplicações compostas de microsserviços. Essas aplicações têm vários serviços de API independentes. Isso gera a proliferação de endpoints de serviço que exigem ferramentas extras de governança. Recomendamos o uso de uma ferramenta de gerenciamento de APIs. O Red Hat 3scale API Management oferece uma variedade de opções padrão para autenticação e segurança de APIs, que podem ser usadas sozinhas ou combinadas para emitir credenciais e controle de acesso.

Os recursos de controle de acesso disponíveis no Red Hat 3scale API Management vão além da segurança e autenticação básicas. Os planos de conta e aplicação permitem que você restrinja o acesso a endpoints, métodos e serviços específicos, além de aplicar políticas de acesso a grupos de usuários. Com os planos de aplicação, é possível definir limites de taxa para o uso da API e o fluxo de controle de tráfego para grupos de desenvolvedores. Defina limites por período para chamadas de API recebidas para proteger sua infraestrutura e manter o tráfego fluindo sem problemas. Também é possível acionar automaticamente alertas de sobrecarga para aplicações que atinjam ou excedam limites de taxa e definir o comportamento para aplicações além do limite.

### Proteção do tráfego das aplicações

A proteção do tráfego das aplicações com opções de entrada e saída do cluster é um assunto abordado na seção 10 deste documento. No caso de aplicações baseadas em microsserviços, proteger o tráfego entre os serviços no cluster também é importante. É possível usar um service mesh para criar essa camada de gerenciamento. O termo "service mesh" (malha de serviços, em inglês) descreve a rede de microsserviços que compõem as aplicações em uma arquitetura distribuída desse tipo e as interações entre os microsserviços.

Baseado no projeto open source Istio, o Red Hat OpenShift Service Mesh inclui uma camada transparente nas aplicações distribuídas existentes para possibilitar o gerenciamento da comunicação entre os serviços, sem precisar alterar o código deles. A solução usa um operador multitenant para gerenciar o ciclo de vida do painel de controle, o que permite que ela seja usada de acordo com cada projeto. E mais: o OpenShift Service Mesh não requer recursos de RBAC no escopo do cluster.

O Red Hat OpenShift Service Mesh oferece recursos de descoberta, balanceamento de carga, chaves de segurança, criptografia e autenticação entre serviços, recuperação de falhas, métricas e monitoramento.

O 3scale Istio Adapter é um adaptador opcional para você rotular os serviços em execução no Red Hat OpenShift Service Mesh.

## 12. Observabilidade

A capacidade de monitorar e auditar os clusters do Red Hat OpenShift é importante na hora de proteger o cluster e os usuários deles contra uso incorreto. O Red Hat OpenShift inclui monitoramento e auditoria integrados, além de um stack de geração de logs opcional.

Os serviços do OpenShift Container Platform se conectam à solução integrada de monitoramento baseada no Prometheus e no respectivo ecossistema. Há um painel de alertas disponível. Os administradores do cluster podem habilitar o monitoramento de projetos definidos pelo usuário. É possível configurar as aplicações implantadas no Red Hat OpenShift para aproveitar os componentes de monitoramento do cluster.

Os eventos de auditoria são uma prática de segurança recomendada e costumam ser exigidos para assegurar a conformidade com os frameworks de regulamentação. Em sua essência, a auditoria do Red Hat OpenShift foi criada usando uma abordagem nativa em nuvem para oferecer centralização e resiliência. No Red Hat OpenShift, a auditoria de hosts e eventos são habilitados por padrão em todos os nós. Essa solução oferece muita flexibilidade para você configurar o gerenciamento e o acesso aos dados de auditoria. É possível controlar a quantidade de informações incluídas nos registros de auditoria do servidor da API escolhendo qual perfil de política de registros de auditoria será usado.

Os dados de registro, auditoria e monitoramento são protegidos por RBAC. Os administradores do projeto podem acessar os dados do projeto, e os do cluster ficam disponíveis para os administradores do cluster.

É recomendável configurar o cluster para encaminhar todos os eventos de registro e auditoria a um sistema de Gerenciamento de eventos e informações de segurança (SIEM), possibilitando a análise, a retenção e o gerenciamento da integridade. Os administradores do cluster do Red Hat OpenShift podem implantar a geração de logs no cluster para agregar todos os logs dessa solução, incluindo os de auditoria de APIs e hosts, de containers de aplicações e de infraestruturas. A geração de logs no cluster agrega os logs de todos os nós do cluster e os armazena em um local padrão. Há várias opções disponíveis para encaminhar registros ao SIEM que você quiser.

## Extensão da segurança com um ecossistema robusto

Para aprimorar ainda mais a segurança do Kubernetes e dos containers ou para atender às políticas existentes, você pode integrar ferramentas externas de proteção. A Red Hat conta com um amplo ecossistema de parceiros certificados que oferecem soluções como:

- Gerenciamento de acesso privilegiado.
- Autoridades de certificação externas.
- Soluções de gerenciamento de chaves e cofres externos.
- Ferramentas de gerenciamento de vulnerabilidades e verificadores de conteúdo de containers.
- Ferramentas de análise de ambientes de execução de containers.
- SIEM.

## Conclusão

A implantação de microsserviços e aplicações baseadas em containers vai muito além da segurança. A plataforma de aplicações em container precisa oferecer uma experiência válida para as equipes de desenvolvimento e de operações. Além disso, é necessária uma plataforma de aplicações de nível empresarial, segura e baseada em containers que impulsione o trabalho dessas equipes, sem comprometer as funções necessárias de cada uma. E essa plataforma também precisa aumentar a eficiência operacional e o uso da infraestrutura.

O Red Hat OpenShift tem como base containers Linux padrão e portáteis que oferecem recursos integrados de segurança, incluindo:

- Ferramentas de CI/CD e compilações integradas para possibilitar práticas seguras de DevOps.
- Kubernetes reforçado e empresarial com gerenciamento do ciclo de vida, conformidade e configuração da plataforma integrados.
- RBAC reforçado com integrações para os sistemas de autenticação empresariais.
- Opções para gerenciar a entrada e saída do cluster.
- SDN integrada e service mesh com suporte para a microssegmentação da rede.
- Suporte para a proteção de volumes de armazenamento remoto.
- Red Hat Enterprise Linux CoreOS, otimizado para a execução de containers em escala com forte isolamento.
- Políticas de implantação para automatizar a segurança dos ambientes de execução.
- Geração de logs, auditoria e monitoramento integrados.

O Red Hat OpenShift também oferece o maior conjunto de linguagens de programação, frameworks e serviços, todos com suporte (Figura 4). O Red Hat Advanced Cluster Management for Kubernetes oferece o gerenciamento fortemente integrado de vários clusters.

O Red Hat OpenShift pode ser executado no OpenStack, VMware, bare-metal, AWS, Google Cloud Platform (GCP), Azure, IBM Cloud e qualquer plataforma compatível com o Red Hat Enterprise Linux. A Red Hat também oferece o Red Hat OpenShift Dedicated na AWS e no GCP como um serviço de nuvem pública. O Azure Red Hat OpenShift é uma solução da Red Hat em parceria com a Microsoft. Já o Red Hat OpenShift Service on AWS é oferecido em parceria com a Amazon.

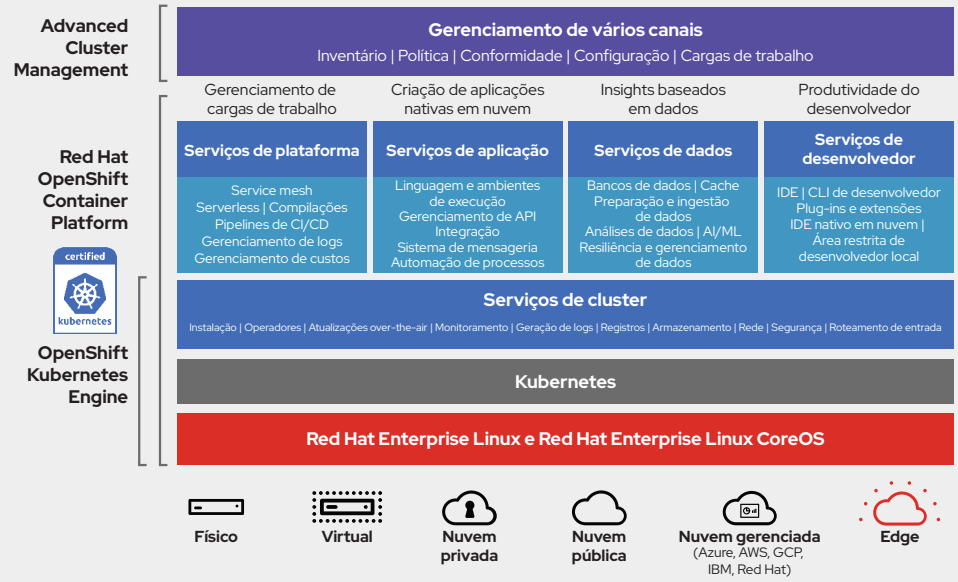


Figura 4. O Red Hat OpenShift oferece um stack de tecnologia com recursos completos nas nuvens públicas e privadas e nos ambientes virtuais e físicos.

Há mais de duas décadas, somos líderes de mercado na oferta de soluções open source confiáveis para os clientes. A Red Hat traz esse mesmo nível de confiança e segurança para os containers por meio de soluções, como o Red Hat OpenShift Container Platform, Red Hat Advanced Cluster Management for Kubernetes e nosso portfólio de soluções prontas para containers.

## SOBRE A RED HAT

A Red Hat é a líder mundial no fornecimento de soluções corporativas de software open source. Por meio da estreita parceria com as comunidades, a Red Hat oferece tecnologias confiáveis e de alto desempenho em Linux, cloud híbrida, containers e Kubernetes. A Red Hat ajuda os clientes a integrar aplicações de TI novas e existentes, desenvolver aplicações nativas em cloud e definir padrões com nosso sistema operacional líder do setor, além de automatizar, proteger e gerenciar ambientes complexos. Com serviços de consultoria, treinamento e suporte premiados, a Red Hat tem a confiança das empresas da Fortune 500. Como um parceiro estratégico para provedores de cloud, integradores de sistema, fornecedores de aplicações, clientes e comunidades open source, a Red Hat ajuda as organizações a se preparar para o futuro digital.

facebook.com/redhatinc
@redhatbr
linkedin.com/company/red-hat-brasil

**AMÉRICA LATINA**
+54 11 4329 7300
latammktg@redhat.com

**BRASIL**
+55 11 3629 6000
marketing-br@redhat.com

br.redhat.com
#F26463_1220

Copyright © 2020 Red Hat, Inc. Red Hat, o logotipo da Red Hat, OpenShift e JBoss são marcas comerciais ou registradas da Red Hat, Inc. e suas subsidiárias nos Estados Unidos e em outros países. Linux® é uma marca registrada da Linus Torvalds nos EUA e em outros países.