

Automação da conformidade e segurança para o setor financeiro com a Red Hat

"As equipes ganham mais agilidade, trabalham juntas de forma mais eficiente e passam mais tempo inovando. Assim, cumprimos a promessa de sempre fazer o melhor para os clientes."¹

James Hixon
Diretor sênior,
Engenharia e Automação de Nuvem,
Ally Financial

Introdução

À medida que a adoção digital cresce, a complexidade da infraestrutura associada também aumenta. Isso acontece principalmente no setor de serviços financeiros, que costuma ter aversão aos riscos e resistência às mudanças por conta das restrições técnicas e regulatórias. As empresas de serviços financeiros precisam de recursos de automação para implantar aplicações e assegurar a consistência e a conformidade das arquiteturas distribuídas adotando a segurança exigida. As configurações e os patches inconsistentes são difíceis de gerenciar em um ambiente com sistemas operacionais Windows e Linux®, infraestruturas virtualizadas, containers e nuvens públicas e privadas.

Com o crescimento desse ambiente misto, os riscos aumentam enquanto a visibilidade e o controle se tornam mais reduzidos. Como resultado, o monitoramento manual da conformidade e da segurança fica cada vez mais difícil. Além disso, muitas vezes, há uma certa tensão nas relações entre as equipes de desenvolvimento, operações e segurança. Por isso, os profissionais de segurança são os últimos a saberem sobre problemas e alterações nas configurações.

Depois que as vulnerabilidades são identificadas, leva algum tempo até que os problemas sejam solucionados e as correções, automatizadas. E mais: os problemas persistentes costumam deixar as organizações em apuros. As vulnerabilidades identificadas são um desafio extra. Quando as correções são finalmente implementadas, as organizações têm dificuldades para documentar o problema remediado, incluindo informações como: quando aconteceu, quais problemas foram resolvidos e por quem. Os bancos, provedores de meios de pagamentos, seguradoras e outras empresas de serviço financeiro também precisam atender às normas de segurança, como o Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (PCI DSS) e o Regulamento Geral sobre a Proteção de Dados (GDPR). Isso exige um trabalho rigoroso de monitoramento, geração de relatórios e documentação para manter a conformidade.

Automação voltada à segurança e conformidade

Para lidar com as questões de conformidade e segurança, os provedores de serviços financeiros precisam se concentrar na automação dos processos de rede e TI orientados por dados em toda a organização. Isso inclui:

- Sistema operacional
 - Gerenciamento de pacote
 - Gerenciamento de patches
 - Proteção do sistema operacional para atender a conformidade básica de segurança, oferecendo o provisionamento de tempo necessário para se obter consistência e imutabilidade
- Infraestrutura e segurança como código
 - Capacidade de reprodução, compartilhamento e verificação, além de ajudar nas auditorias de segurança e conformidade
- Linguagens de programação e script que todos da organização possam entender, o que facilita a utilização



facebook.com/redhatinc
@redhatbr

linkedin.com/company/red-hat-brasil

¹ Caso de sucesso da Red Hat, "Ally Financial adota plataforma de nuvem e DevOps para acelerar o time to market", maio de 2019.

- Provisionamento do sistema
 - Integração com o gerenciamento de serviços de TI (ITSM)
 - Provisionamento de armazenamento
- Fluxos de trabalho
 - Gerenciamento simplificado de serviços
- Monitoramento e segurança contínua (Day 2 security operations)
 - Gerenciamento de patches
 - Identificação e gerenciamento de vulnerabilidades (por exemplo, verificações de integridade)
 - Governança proativa de políticas de conformidade, controle e segurança
 - Reparos: automação e geração de correções

Desafios da automação da segurança e conformidade

Garantir conformidade e segurança com a verificação manual de sistemas é problemático por diversas razões, incluindo:

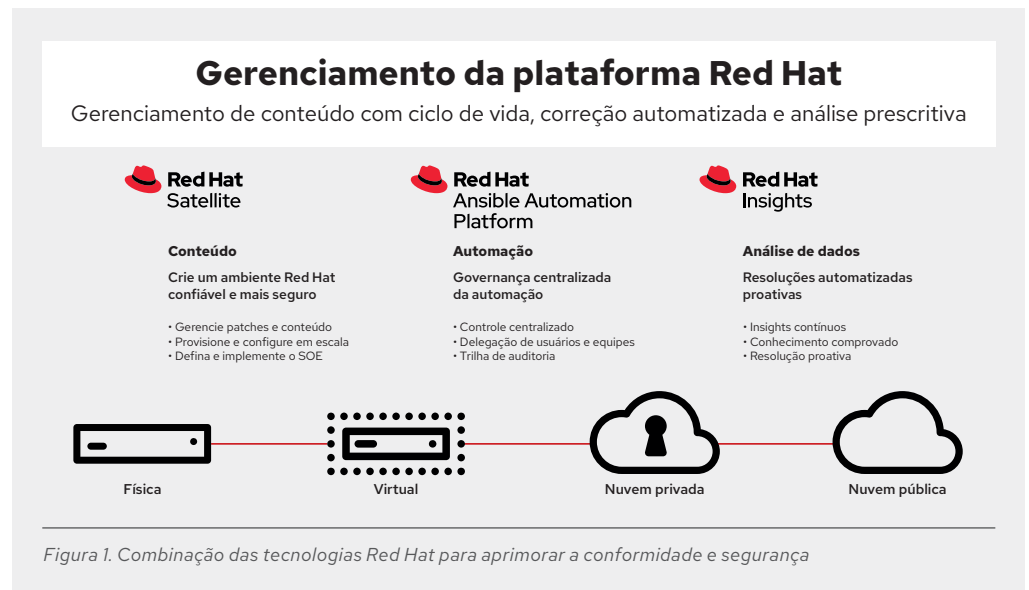
- Tarefas demoradas e monótonas
- Há a possibilidade falhas humanas
- A trilha de auditoria para ações inadequadas e alterações simples de configuração não é registrada corretamente
- Não tem capacidade de reprodução, compartilhamento ou verificação
- Dificuldade de receber aprovação em auditorias devido a informações inconsistentes e incompletas de changelog
- A comunicação entre as equipes de segurança e operações é ineficaz ou inexistente

As empresas de serviços e soluções financeiras precisam determinar onde as tarefas manuais serão executadas e a frequência desse trabalho para estabelecer uma estratégia de automação. É preciso ter como foco tecnologias de automação flexíveis para dar suporte às mudanças futuras nos requisitos. Escolher as tecnologias de automação certas é o segredo para acelerar a implementação e a expansão entre os serviços e dispositivos de rede.

Automação inteligente da segurança com a Red Hat

As tecnologias Red Hat® oferecem um stack de software completo para viabilizar sua estratégia de automação. Isso inclui softwares, sistemas operacionais com segurança reforçada e diversas integrações com fornecedores (AWS, Cisco, Juniper, VMware etc.), atendendo às necessidades tanto da automação da rede quanto da TI.

Você não precisa ter todas as tecnologias Red Hat. No entanto, a capacidade de automação da conformidade e da segurança é muito maior quando você associa as nossas soluções. Por exemplo, o Red Hat Enterprise Linux, o Red Hat Ansible® Automation Platform, o Red Hat Satellite e o Red Hat Insights formam uma poderosa combinação para a automação da conformidade e segurança.



Essas tecnologias trabalham juntas para proporcionar os seguintes benefícios extras:

Red Hat Enterprise Linux

O [Red Hat Enterprise Linux](#) oferece tecnologias de segurança para combater vulnerabilidades, proteger dados e atender à conformidade regulatória. Com ele, é possível automatizar conformidades regulatórias e correções de configurações de segurança no sistema e nos containers. Para isso, basta usar o OpenSCAP, ferramenta de análise da Red Hat com certificação do National Institute of Standards and Technology (NIST). Ela faz verificações e correções de configurações e vulnerabilidades tendo como parâmetro:

- PCI DSS.
- Guia de implementação técnica de segurança (STIG) da Agência americana de sistemas de informação de defesa (DISA).
- Política de segurança dos Serviços de informação da justiça criminal (CJIS).
- Serviços de nuvem empresariais (C2S).
- Lei de portabilidade e responsabilidade de seguros de saúde (HIPAA).
- NIST 800-171.
- Perfil de proteção do sistema operacional (OSPP) v4.2.
- Perfil empresarial da Red Hat para provedores de nuvem certificados.

Para atender melhor às várias necessidades de segurança da computação híbrida, o Red Hat Enterprise Linux aprimora a automação da segurança de software. Isso reduz os riscos por meio da integração do OpenSCAP com o Red Hat Ansible Automation Platform. Com essa integração, é possível aplicar os Ansible playbooks compatíveis e também aqueles pré-gerados da Red Hat para corrigir sistemas e manter a conformidade com os parâmetros de segurança. Além disso, a integração permite criar novos Ansible playbooks usando um perfil de segurança específico ou utilizando diretamente as verificações do OpenSCAP. Dessa forma, você implementa correções no ambiente híbrido da TI com mais rapidez e consistência.

As funções de sistema do Red Hat Enterprise Linux também ajudam a automatizar a segurança. Elas usam um conjunto de módulos e Ansible roles que proporcionam uma interface de configuração consistente e estável. Isso viabiliza o gerenciamento remoto do Red Hat Enterprise Linux 6.10 e versões superiores. Por exemplo, para configurar de maneira correta e consistente o Security-Enhanced Linux (SELinux) nos sistemas Red Hat Enterprise Linux, basta usar a função de sistema correspondente.

Ao automatizar tarefas comuns de gerenciamento, diminui o número de usuários que precisarão solicitar acesso direto como superusuário aos hosts, o que reduz a vulnerabilidade a ataques. Com o SELinux, é possível alocar privilégios específicos para tarefas de gerenciamento automatizadas, protegendo o sistema contra bugs de escalação.

Red Hat Ansible Automation Platform

O [Red Hat Ansible Automation Platform](#), que inclui o Red Hat Ansible Tower, é uma tecnologia de automação de TI sem agente, simples e poderosa. Essa solução oferece uma plataforma comum de automação para toda a organização, o que proporciona os seguintes benefícios de conformidade e segurança:

- Capacidade de reprodução e rastreamento para fins de conformidade
- Enorme redução do tempo gasto com tarefas repetitivas
- Redução do risco de períodos de downtime com a adoção de uma abordagem consistente de gerenciamento da infraestrutura
- Redução do risco de erros sistemáticos por meio de análises, detecções e soluções automatizadas
- Redução no tempo de retorno de receita ao disponibilizar a tecnologia mais rapidamente
- Redução de risco de falhas humanas
- Processos de TI mais rápidos (muitas vezes, passando de dias para minutos)
- Gerenciamento e configuração consistentes em um ambiente com vários fornecedores
- Automação de implantações, definições e gerenciamento do ciclo de vida de configurações, incluindo a aplicação de políticas e a atualização de sistemas e firewalls em toda a rede
- Replicação rápida de problemas de campo por meio de informações de configuração em catálogos de serviço
- Capacidade de incorporar o Ansible Automation Platform a processos e ferramentas de segurança por meio de interfaces de programação de aplicações de transferência de estado representacional (APIs RESTful)
- Solução de alta escalabilidade com controle de acesso, cofre de credenciais, programação de tarefas e fluxos de trabalho, integração da administração de fontes e auditoria com gerenciamento gráfico de inventário. Isso simplifica a representação de todos os componentes e oferece visibilidade de todas as atividades de automação

O Ansible Automation Platform inclui módulos e funções criadas especificamente para a integração com soluções e fornecedores de segurança. Por exemplo, Splunk (SIEM), Snort (prevenção e detecção de invasões) e Checkpoint (firewall empresarial).

Red Hat Satellite

O [Red Hat Satellite](#) oferece à TI informações sobre os sistemas Red Hat no ambiente, incluindo a identificação daqueles que estão desatualizados e que têm vulnerabilidades conhecidas. As organizações usam essa solução no gerenciamento de conteúdo e subscrições, provisionamento de hosts seguros, controle de configurações e gestão de patches. O Ansible Automation Platform trabalha com o Satellite para implantar e gerenciar automaticamente configurações de software, o que proporciona controle completo e automatizado de sistemas e aplicações durante o ciclo de vida. Assim, você mantém a segurança, a conformidade e a trilha de auditoria.

Com o Red Hat Satellite, você:

- Define e aplica um ambiente operacional padrão (SOE).
- Usa o Ansible Automation Platform para implantar funções de sistema do Red Hat Enterprise Linux e instalar o Red Hat Insights no SOE.
- Identifica desvios do SOE e usa o Ansible Automation Platform para corrigir esses problemas.
- Identifica os riscos à segurança, desempenho, estabilidade e disponibilidade por meio do Insights. Depois, gera Ansible playbooks de forma dinâmica para realizar a execução direta das correções de riscos no Satellite.
- Os sistemas provisionados pelo Satellite podem fazer retornos de chamadas ao Ansible Tower para garantir a execução de playbooks após o provisionamento.
- Usa o Ansible Automation Platform para importar e utilizar as funções de sistema do Red Hat Enterprise Linux.
- O Ansible Tower usa o Satellite como uma fonte de inventário dinâmico.
- Implanta o Insights usando o Ansible Automation Platform no Satellite.

Red Hat Insights

O [Red Hat Insights](#) está incluído no Red Hat Satellite e também funciona de maneira autônoma como um complemento do Red Hat Enterprise Linux. É possível realizar análises preditivas com as descobertas geradas pelo Insights. Além disso, quando essa solução é integrada ao Ansible Tower, ela pode ser configurada para gerar playbooks e executar correções automaticamente. O Ansible Tower usa a API do Insights para oferecer suporte a trabalhos de correção em toda a organização. Integre os recursos de detecção e correção do Insights a scripts e sistemas externos para proporcionar às equipes de operações a capacidade de escalar correções orientadas em toda a empresa.

O Ansible Tower pode ser configurado para se conectar à API do Insights e, assim, recuperar informações dele. Por exemplo, use o Ansible Tower para extrair os Ansible playbooks usados na versão de Portal do Cliente do Red Hat Insights. Além disso, é possível inicializá-los diretamente na solução para automatizar a correção de problemas.



Figura 2. Conformidade e segurança automatizadas com a Red Hat.

Caso de uso: gerenciamento automatizado de patches

Juntos, o Red Hat Satellite, o Red Hat Insights e o Red Hat Ansible Automation Platform detectam riscos nos hosts gerenciados pelo Red Hat Satellite de maneira otimizada. Eles também usam os playbooks do Red Hat Ansible Automation Platform para corrigir muitos desses problemas. Você pode criar um plano de correção replicável, colocá-lo em prática e fornecer um relatório para os auditores. O Insights pode ser configurado para controlar o tipo de informação enviado ao Satellite para que você veja e controle os dados encaminhados.

1. Use o Insights para identificar os sistemas que precisam de patch.
2. Crie um plano do Insights para os playbooks que você irá usar e os sistemas em que você quer executá-los.
3. Agende a execução do plano do Insights ou o ative manualmente.
4. Proceda de acordo com as informações fornecidas pelo plano do Insights. O Insights aprende e se aprimora a cada novo elemento de inteligência e dados obtidos. Ele descobre automaticamente insights relevantes, faz recomendações de próximas ações personalizadas e até mesmo automatiza as tarefas.
5. Forneça informações consolidadas para auditoria produzidas por meio da execução do plano do Insights, incluindo quem o executou, os horários de início e de término e a execução no nível da tarefa.

Resumo

As redes financeiras estão evoluindo em direção a uma maior capacidade de programação, e as aplicações estão ficando mais complexas. Por isso, é essencial ter uma solução de automação para gerenciar o ambiente de rede e de TI. A solução de conformidade e automação da Red Hat atende aos interesses dos provedores de serviços financeiros com a automação completa das redes e da TI.

O Red Hat Ansible Automation Platform oferece uma linguagem de automação comum e uma camada operacional que expõe as APIs necessárias para realizar uma automação completa. Isso se aplica quando você conecta o Red Hat Satellite para provisionar e configurar sistemas com segurança em conformidade, usa os dados do Red Hat Insights para corrigir problemas de segurança de forma proativa ou utiliza uma automação simples para implantar, gerenciar e fazer upgrade da nuvem. Essa abordagem é muito útil nas organizações que precisam de segurança total em dispositivos e aplicações específicos. O Red Hat Ansible Automation Platform assegura a automação em todo o ambiente do Red Hat Enterprise Linux, incluindo a descoberta de informações do ambiente, a adesão às políticas organizacionais e a aplicação de alterações de configuração relacionadas.

Todas as soluções Red Hat não dependem de fornecedor e dão suporte ao ambiente de TI sem a substituição de processos e aplicações legadas. Isso viabiliza a orquestração e integração dos processos e tarefas de segurança em dispositivos, plataformas e fornecedores. Enquanto os recursos internos se concentram na inovação, a Red Hat cuida da sua estratégia essencial de automação da segurança e simplifica o gerenciamento dos serviços.

Próximas etapas

- Para iniciar ou ampliar a automação da conformidade e da segurança, agende uma discovery session da Red Hat e aproveite para analisar seu ambiente em busca de oportunidades de automação. O Red Hat Services também oferece soluções mais abrangentes para a automação da segurança e dos fluxos de confiabilidade. Elas combinam o Red Hat Insights, o Red Hat Satellite e o Red Hat Ansible Tower para identificar falhas ou possíveis configurações

problemáticas de acordo com o Insights. Essa solução proporciona um framework escalável em que é possível usar e personalizar playbooks do Insights, além de utilizar e implantar playbooks do cliente para corrigir vulnerabilidades e ter uma trilha de auditoria no ambiente da TI.

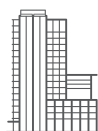
- Participe do webinar sobre segurança e conformidade para instituições de serviço financeiro e descubra como a tecnologia de gerenciamento de segurança da Red Hat reduz os riscos da infraestrutura na sua organização.

Conheça mais sobre as soluções Red Hat

O Red Hat Satellite, o Red Hat Insights e o Red Hat Ansible Automation Platform também oferecem mais controle e gerenciamento da segurança em todo o portfólio da Red Hat. Por exemplo, para clientes Red Hat OpenShift®.

As demais tecnologias incluem funcionalidades para você lidar com problemas específicos de conformidade e segurança. A Red Hat entende que a completa orquestração de auditoria, conformidade e segurança é necessária no cenário atual onde tudo está em constante transformação. Por isso, fornecemos as plataformas e ferramentas necessárias para o gerenciamento e o controle da sua rede e TI.

Para tirar dúvidas ou saber mais, entre em contato com seu representante da Red Hat ou leia sobre a [automação de serviços financeiros](#).



Sobre a Red Hat

A Red Hat é a líder mundial em soluções de software open source empresariais e utiliza uma abordagem impulsionada pela comunidade para oferecer tecnologias confiáveis e de alto desempenho em Linux, nuvem híbrida, containers e Kubernetes. A Red Hat ajuda os clientes a integrar aplicações de TI novas e existentes, desenvolver aplicações nativas em nuvem 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 é a parceira de confiança das empresas listadas na Fortune 500. Como parceira estratégica de provedores de nuvem, integradores de sistemas, fornecedores de aplicações, clientes e comunidades open source, a Red Hat ajuda as empresas a se prepararem 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
#F23392_0420

Copyright © 2020 Red Hat, Inc. Red Hat, o logotipo da Red Hat, Ansible e o OpenShift 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 Estados Unidos e em outros países.