AUTOMAÇÃO DA CONFORMIDADE E SEGURANÇA COM A RED HAT

AUTOMAÇÃO DE TODA A TI E DAS REDES PARA GARANTIR SEGURANÇA APRIMORADA E PROATIVA

VISÃO GERAL

De acordo com o Gartner, "as equipes de segurança sofrem com a falta de profissionais qualificados, o aumento na quantidade de alertas e ameaças e a necessidade constante de realizar mais com menos recursos".[1]

INTRODUÇÃO

À medida que as redes e as infraestruturas crescem e ficam mais complexas, a automação é necessária para garantir que as implantações e arquiteturas distribuídas estejam seguras, em conformidade e que alcancem o desempenho esperado. Configurações e patches inconsistentes são difíceis de gerenciar em um ambiente híbrido e complexo que reúne sistemas operacionais Windows e Linux®, infraestruturas virtualizadas, clouds públicas e privadas e containers. Com o crescimento desse ambiente misto, a complexidade e os riscos aumentam enquanto a visibilidade e o controle se tornam ainda mais reduzidos. Como resultado dessa falta de visibilidade, o monitoramento manual da conformidade e da segurança se torna progressivamente mais difícil. Além disso, muitas vezes, há uma certa tensão nas relações entre os times de desenvolvimento, operações e segurança. E, como consequência, as equipes de segurança são as últimas a serem informadas sobre problemas e alterações nas configurações.

Quando vulnerabilidades são identificadas, leva algum tempo até que os problemas sejam solucionados e as correções automatizadas. Normalmente, os problemas persistentes são aqueles que costumam deixar as organizações em apuros. Segundo o Gartner[2], o maior problema enfrentado pelas empresas são as vulnerabilidades conhecidas. Além disso, quando as correções são finalmente implementadas, as empresas têm dificuldades para documentar o problema reparado, incluindo informações como: quando aconteceu, quais problemas foram resolvidos e por quem. Os provedores de serviços também precisam adotar os padrões de segurança do setor, como o PCI-DSS, que exige que os processos de verificação, manutenção e correção sejam executados e documentados para fins de conformidade.

AUTOMAÇÃO VOLTADA PARA CONFORMIDADE E SEGURANÇA

Para lidar com questões de conformidade e segurança, os provedores de serviços 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 patch
  - Proteção do sistema operacional para atender a conformidade básica de segurança, garantindo o provisionamento de tempo necessário para se obter consistência e imutabilidade.
- Infraestrutura e segurança como código
  - Capacidade de reprodução, compartilhamento e verificação, além de auxílio para receber aprovação nas auditorias de conformidade e segurança
  - Linguagens de programação e script rápidas de aprender e aplicar, possibilitando a utilização por toda a organização

1 *Chuvakin, Anton; Barros, Augusto Barros. "Preparing Your Security Operations for Orchestration and Automation Tools.", gartner.com: Gartner, 22 de fevereiro de 2018.* https://www.gartner.com/doc/3860563/preparing-security-operations-orchestration-automation

2 *Moore, Susan. "Focus on the Biggest Security Threats, Not the Most Publicized.", gartner.com: Gartner, 2 de novembro de 2017.* https://www.gartner.com/smarterwithgartner/focus-on-the-biggest-security-threats-not-the-most-publicized/

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

DESAFIOS NA AUTOMAÇÃO DA CONFORMIDADE E DA SEGURANÇA

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

- O processo é demorado e entediante
- 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
- É difícil obter aprovação em auditorias devido a informações inconsistentes e incompletas no histórico de alterações
- A comunicação entre as equipes de segurança e operações é ineficaz ou inexistente

Os provedores de serviços precisam determinar o local e a frequência da execução de tarefas manuais. Além disso, é necessário implementar uma estratégia de automação com as tecnologias mais flexíveis e robustas disponíveis. Escolher as tecnologias de automação adequadas é o segredo para realizar uma implementação rápida e poder ampliá-la para mais dispositivos e serviços na rede.

AUTOMAÇÃO INTELIGENTE DA SEGURANÇA COM A RED HAT

As tecnologias Red Hat possibilitam uma estratégia para a automação do stack de software completa e abrangente, incluindo sistemas operacionais com segurança reforçada, softwares de automação e dezenas de integrações com fornecedores (AWS, Cisco, Juniper, VMware etc.), atendendo às necessidades de automação da rede e 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, o Red Hat Satellite e o Red Hat Insights formam uma poderosa combinação para a automação da conformidade e segurança.

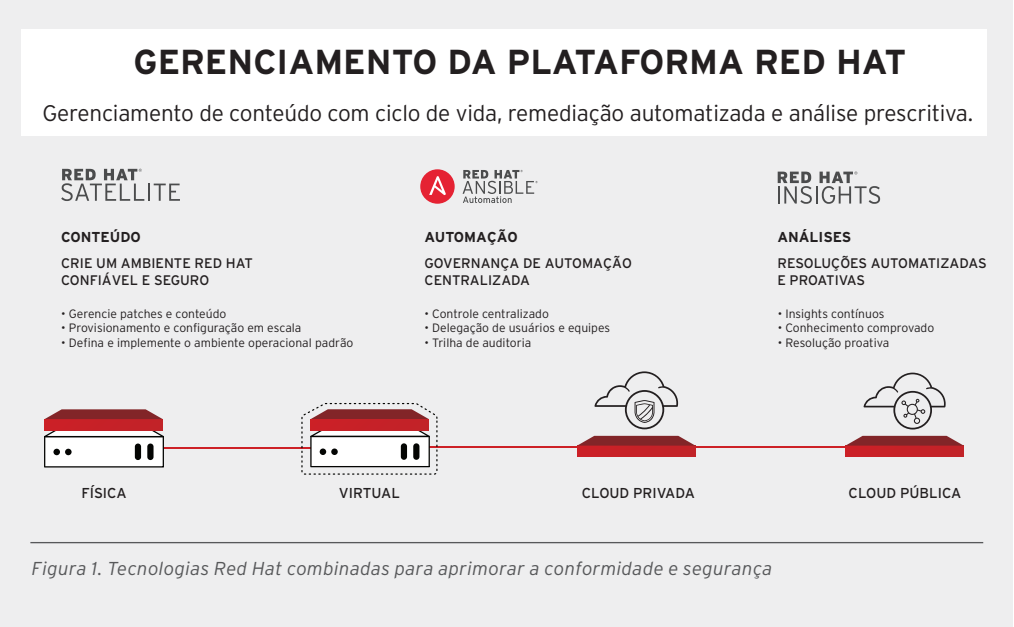

Figura 1. Tecnologias Red Hat combinadas para aprimorar a conformidade e segurança

Essas tecnologias trabalham juntas para garantir os seguintes benefícios adicionais:

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
- Diretrizes de Implementação Técnica de Segurança (STIG) do DISA
- Política de segurança dos Serviços de Informação da Justiça Criminal (CJIS)
- Serviços de Cloud Corporativa (C2S)
- Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA)
- NIST 800-171
- Perfil de Proteção do Sistema Operacional (OSPP) v4.2
- Perfil Corporativo Red Hat para Provedores de Cloud Certificados

Para atender melhor às várias necessidades de segurança da computação híbrida, o Red Hat Enterprise Linux 7.5 fornece automação aprimorada da segurança do software. Ela reduz os riscos por meio da integração do OpenSCAP com o Red Hat Ansible Automation. Essa integração oferece suporte à utilização de playbooks da Red Hat previamente criados e playbooks compatíveis do Ansible, possibilitando a correção dos sistemas para garantir a conformidade com os parâmetros de segurança. Além disso, ela permite a criação de playbooks do Ansible a partir de um perfil de segurança específico e diretamente das verificações do OpenSCAP, o que viabiliza uma implementação de correções no ambiente híbrido da TI com mais rapidez e consistência.

As funções de sistema do Red Hat Enterprise Linux também ajudam na automação da segurança. Elas são um conjunto de módulos e funcionalidades do Ansible que fornecem uma interface de configuração consistente e estável, permitindo o gerenciamento remoto do Red Hat Enterprise Linux 6.10 e versões superiores. Por exemplo, a função de sistema do Security-Enhanced Linux (SELinux) pode ser usado para configurar de maneira adequada e com consistência o Security-Enhanced Linux (SELinux) nos sistemas Red Hat Enterprise Linux.

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

O Red Hat Ansible Automation é uma tecnologia de automação de TI sem agente, simples e poderosa que inclui o Red Hat Ansible Tower. Esta solução oferece uma plataforma comum de automação para toda a organização, garantindo os seguintes benefícios de conformidade e segurança:

- Capacidade de reprodução e rastreamento para fins de conformidade
- Redução do tempo gasto com tarefas comuns e repetitivas
- Abordagem de gerenciamento da infraestrutura consistente, reduzindo o risco de períodos de inatividade
- 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 custos por meio da redução de esforços
- 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
- Automatização de implantações, configurações e gerenciamento do ciclo de vida de configurações, incluindo a disponibilização 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 a automação do Ansible em processos e ferramentas de segurança preexistentes por meio de interfaces de programação de aplicações de transferência de estado representacional (APIs RESTful)
- É uma solução de alta escalabilidade com controle de acesso, cofre de credenciais, programação de tarefas e fluxos de trabalho, controle de fontes integrado e auditoria com gerenciamento gráfico de inventário que simplifica a representação de todos os componentes e fornece visibilidade em todas as atividades de automação

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

RED HAT SATELLITE

O Red Hat Satellite fornece informações de TI sobre os sistemas Red Hat presentes 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 Red Hat Ansible Automation funciona com o Red Hat Satellite para implantar e gerenciar automaticamente configurações de software, garantindo completo controle de sistemas e aplicações durante o ciclo de vida. Assim, você mantém a segurança, a conformidade e documentação para auditoria.

- Define e garante um ambiente operacional padrão (SOE).
- Usa o Ansible Automation para implantar funções de sistema do Red Hat Enterprise Linux e instalar o Insights no SOE.
- Identifica desvios do SOE e usa o Ansible Automation para corrigir esses problemas.
- Identifica riscos na disponibilidade, estabilidade, desempenho e segurança por meio do Insights. O Insights gera playbooks do Ansible de forma dinâmica para realizar a execução direta de 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 para importar e rodar funções de sistema do Red Hat Enterprise Linux.
- O Ansible Tower usa o Satellite como uma fonte de inventário dinâmico.
- É possível implantar o Insights usando o Ansible Automation no Satellite.

RED HAT INSIGHTS

O Red Hat Insights está incluído no Red Hat Satellite e funciona independentemente, como um complemento do Red Hat Enterprise Linux. Com as descobertas do Insights, você garante dados analíticos preditivos e utilizáveis. Quando o Insights é integrado ao Ansible Tower, é possível configurá-lo para gerar playbooks automaticamente e, assim, aplicar as correções. O Ansible Tower usa a API do Insights para oferecer suporte a trabalhos de correção em toda a organização. Também é possível integrar os recursos de detecção e correção do Insights a scripts e sistemas externos. Isso garante às equipes de operações a capacidade de escalar correções orientadas em toda a empresa.

É possível configurar o Ansible Tower para conectar-se à API do Insights e, assim, recuperar informações. Por exemplo, o Ansible Tower pode extrair os playbooks do Ansible usados na versão Red Hat Insights do Portal do Cliente. Assim, é possível iniciar esses playbooks diretamente do Ansible Tower, possibilitando a correção automatizada de problemas encontrados pelo Insights.

O Insights é integrado ao Satellite. Por isso, você pode executar playbooks de correção diretamente da interface web do Red Hat Satellite.

Figura 2. Conformidade e segurança automatizadas com a Red Hat

CASO DE USO: GERENCIAMENTO AUTOMATIZADO DE PATCHES

Juntos, o Red Hat Satellite, Red Hat Insights e Red Hat Ansible Automation detectam de forma otimizada riscos nos hosts gerenciados pelo Red Hat Satellite. Eles usam os playbooks do Red Hat Ansible Automation 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 a ser enviado ao Satellite, possibilitando 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.

A combinação do Red Hat Satellite, Red Hat Ansible Automation e Red Hat Insights, ajuda você a detectar e corrigir falhas antes que elas se transformem em grandes problemas. Isso garante o monitoramento contínuo com ações de segurança e conformidade automatizadas.

RESUMO

As redes estão evoluindo em direção a uma maior capacidade de programação. E, com o surgimento de outras tecnologias, como a virtualização de funções de rede (NFV), a complexidade da TI também aumenta. Dessa forma, ter uma solução de automação é essencial para gerenciar o ambiente de rede e de TI. As tecnologias incluídas na solução de conformidade e automação da Red Hat atendem aos interesses dos provedores de serviços ao fornecer automação completa de redes e de TI.

O Red Hat Ansible Automation fornece uma linguagem de automação comum e uma camada operacional que expõe as APIs necessárias para realizar uma automação completa em organizações com necessidades de dispositivos e aplicações específicas, garantindo uma segurança holística. Isso se aplica quando você conecta o Red Hat Satellite para provisionar e configurar sistemas com segurança em conformidade, usando os dados do Red Hat Insights para corrigir problemas de segurança de forma proativa, ou utiliza a automação simples para implantar, gerenciar e atualizar a cloud. O Red Hat Ansible Automation fornece automação para todo o ambiente do Red Hat Enterprise Linux, incluindo a descoberta de informações, adesão às políticas organizacionais e alterações de configuração relacionadas.

Todas as soluções da Red Hat são independentes de fornecedor. Isso garante o suporte ao seu ambiente de TI sem a substituição de processos e aplicações legadas, além de fornecer orquestração e integração de processos e tarefas de segurança em dispositivos, plataformas e fornecedores. Com a Red Hat, você concentra seus recursos na inovação, enquanto cuidamos do suporte à sua estratégia de automação da segurança e simplificamos o gerenciamento dos seus serviços.

PRÓXIMAS ETAPAS

- Para iniciar ou ampliar a automação da conformidade e segurança de sua empresa, agende uma discovery session da Red Hat e aproveite para analisar o ambiente em busca de oportunidades. 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, Red Hat Satellite e Red Hat Ansible Tower para identificar falhas atuais ou possíveis configurações problemáticas de acordo com o Insights. Essas soluções proporcionam uma estrutura escalável na qual é possível usar e personalizar playbooks fornecidos pelo Insights, além de utilizar e implantar playbooks do cliente para corrigir vulnerabilidades e garantir uma trilha de auditoria no ambiente da TI.
- Assista a um vídeo do Red Hat Satellite 6.4 trabalhando com o Red Hat Insights e o Red Hat Ansible Automation para detectar de forma simplificada riscos nos hosts gerenciados pelo Red Hat Satellite e corrigir problemas descobertos com facilidade usando o playbook do Red Hat Ansible Automation disponível para correção pelo Insights. Veja como descobrir erros e corrigi-los antes que eles causem problemas.

SAIBA MAIS

- O Red Hat Satellite, Red Hat Insights e Red Hat Ansible Automation também fornecem controle e gerenciamento de segurança adicionais em todo o portfólio da Red Hat, por exemplo, para clientes do o Red Hat OpenStack® Platform.
- O Red Hat OpenStack Platform e demais tecnologias, oferecem 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 mais informações, entre em contato com um representante da Red Hat.

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
f190279_1118