Segurança de Ativos com Suse Manager

Rafael Belanga Furlan

Curso Superior de Tecnologia em Segurança da Informação – Faculdade de Tecnologia de Americana (FATEC Americana)
Americana – SP - Brasil

furlanrb@gmail.com

Abstract. *With the advancement of technology and the possibility for companies to use resources without the need for physical machines locally, there was also a significant increase in virtual resources, and with that, the administration of large amounts of virtual machines, containers, among other assets became painful, if not done through automations and manager software. The main objective of this article is to present the Suse Manager software as an option to manage large amounts of assets, such as virtual machines, physical machines, and instances.*

Resumo. *Com o avanço da tecnologia e a possibilidade de empresas utilizarem recursos sem a necessidade de máquinas físicas localmente, houve também um aumento expressivo de recursos virtuais, e com isso, a administração de grandes quantidades máquinas virtuais, containers, entre outros ativos se tornou penosa, caso não feito através de automações e softwares gerenciadores. O objetivo central desse artigo é apresentar o software Suse Manager como uma opção para gerenciar grandes quantidades de ativos, como máquinas virtuais, máquinas físicas, e instâncias.*

1. Introdução

A área de tecnologia está sempre em constante evolução. Há pouco tempo era tido como padrão empresas utilizarem grandes datacenters, sem automações de processos, o que resultava em tarefas repetitivas para a resolução de problemas, e com uma demanda de tempo que poderia ser utilizada em outros projetos. Com o advento da utilização de máquinas virtuais, containers, e mais ainda recentemente, a nuvem, os profissionais puderam focar de forma mais ativa em automação e gerenciamento inteligente dos sistemas que estão em suas responsabilidades, pois com essas novas tecnologias as questões provenientes de hardware e configurações de serviços e softwares, ficaram mais simplificadas para o administrador daquelas máquinas.

Com isso, surgiram softwares que auxiliam no gerenciamento e orquestração dessas novas tecnologias. O SUSE Manager é um desses softwares que facilitam a vida do Administrador de Sistemas, levando em foco as questões relacionadas com segurança e automação de ações. Portanto, o objetivo geral deste artigo é trazer ao leitor as principais ferramentas disponibilizadas pelo SUSE Manager para a administração de conformidades de segurança e automatização de tarefas de servidores, além de analisar um problema para os profissionais que administram uma quantidade grande de servidores: O gerenciamento de forma eficaz e ágil de máquinas virtuais, instâncias e containers. Consequentemente, o objetivo específico deste artigo será analisar o ganho que ocorre ao utilizar uma solução como SUSE Manager, em detrimento de realizar as tarefas manualmente.

2. Revisão Bibliográfica

Nessa seção será abordado os assuntos básicos relacionados ao tema principal do estudo, para um melhor entendimento do leitor que não esteja tão familiarizado com alguns conceitos que serão apresentados nas próximas seções.

2.1. GNU/Linux

> "Linux é um sistema operacional de computador. Um sistema operacional consiste no software que gerencia seu computador e permite que você execute aplicativos nele." (Negus, p. 4)

Linux, ou mais corretamente GNU/Linux (quando é falado não somente do kernel, que seria o core do sistema operacional, mas também dos utilitários e ferramentas que acompanham o kernel), é o nome dado a um Sistema Operacional de código aberto, criado pelo finlândes Linus Torvalds, em 1991. Por ser de código aberto, ou seja, seu código fonte podia ser utilizado e alterado por qualquer pessoa que tivesse conhecimentos em desenvolvimento de software, logo ele se tornou muito popular, e começou a ser melhorado por muitas pessoas ao redor do mundo, deixando-o mais seguro e com mais funcionalidades. Atualmente, o GNU/Linux é majoritariamente utilizado como Sistema Operacional principal nos servidores das maiores empresas de tecnologia do mundo. O GNU/Linux também é o sistema padrão para utilização em nuvens, como GCP da Google e AWS da Amazon, e também é a base para a tecnologia de containers. Ainda segundo o site opensource.org, Linux é o sistema operacional de código aberto mais conhecido e mais usado (levando em consideração servidores, sistemas mobile como o Android, IoT, e outros projetos). Como um sistema operacional, o Linux é um software que fica por baixo de todos os outros softwares em um computador, recebendo solicitações desses programas e retransmitindo essas solicitações para o hardware do computador.

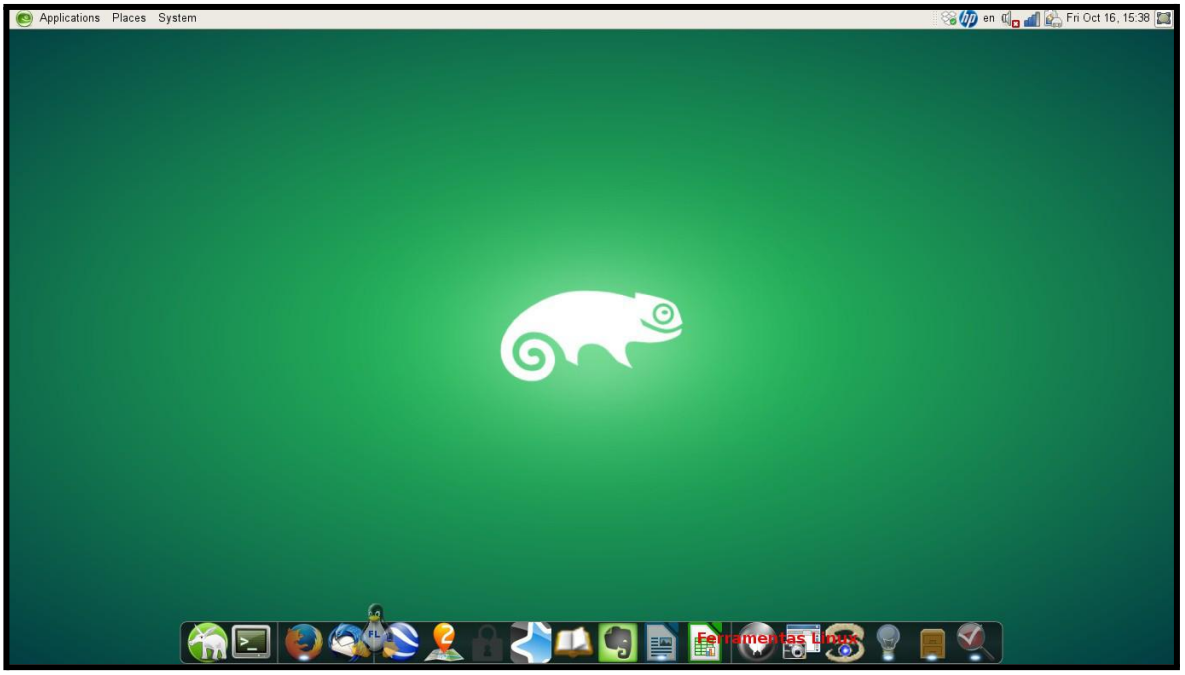

Figura 1. Suse Linux

Fonte: portallinuxferramentas

2.2. Máquinas Virtuais (VMs)

> "*Defino virtualização como a abstração de um recurso de computação de outro recurso de computação. Quando a maioria dos profissionais de TI pensa em virtualização, eles pensam em virtualização de hardware (ou servidor): abstraindo o sistema operacional do hardware subjacente em que é executado, permitindo assim que vários sistemas operacionais sejam executados simultaneamente no mesmo servidor físico. Essa é a tecnologia na qual a VMware tem construído sua participação de mercado."* (Fritz et al., p. 19)

De acordo com o site da red hat, uma máquina virtual, ou VM (Virtual Machine), é um ambiente virtual que funciona como um sistema de computação com seu próprio processador, memória, interface de rede e armazenamento. Esse sistema virtual é criado a partir de um sistema de hardware físico localizado on-premise ou não.

Para entender melhor como essa tecnologia é importante, pode ser feito um exercício e retornar ao tempo, no início do uso de computadores pelas empresas. Caso uma organização tivesse a intenção de utilizar um novo serviço, era preciso comprar um novo computador e realizar toda a sua configuração e alocação. E se em outro caso, um computador falhasse, era necessário realizar toda a troca dele, criando indisponibilidade nos serviços até que a aquisição de um novo computador tivesse sido feita.

A tecnologia de máquinas virtuais pode ser dita como uma revolução no uso de Sistemas Operacionais, porque com ela as empresas podiam manter um datacenter com a tecnologia hipervisor, que é a qual possibilita o uso de VMs, e subir e/ou remover máquinas em poucos minutos. Por isso são chamadas de máquinas virtuais, ou VMs (Virtual Machines). As VMs, falando de forma simplificada, funcionam exatamente como um computador físico, igual ao que há nas residências, porém ele é hospedado em datacenters com a já dita tecnologia hipervisor, que separa do hardware os recursos utilizados pela máquina virtual e os provisiona adequadamente. Quando é provisionada uma nova máquina, o hipervisor reconhece a quantidade de recursos que foi requisitado (processador, memória, disco rígido, etc.), realiza a alocação e isolamento desses recursos para essa máquina em questão.

Sendo assim, o uso de máquinas virtuais facilita e agiliza a criação e configuração de novos serviços de T.I na organização.

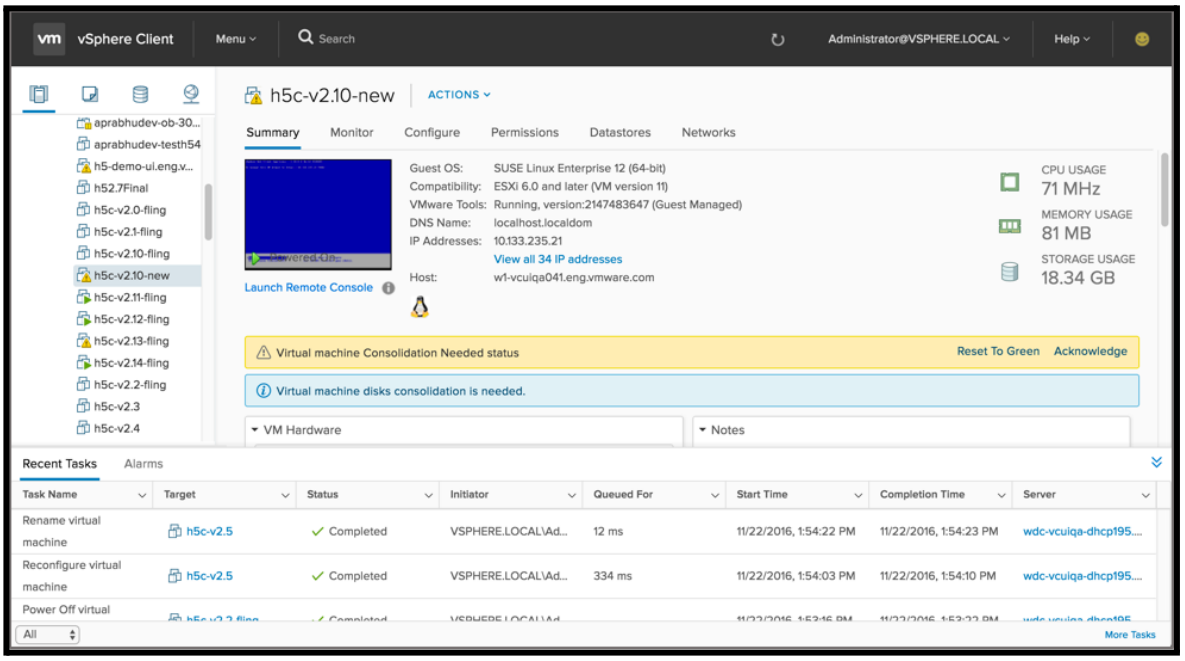

Figura 2. VMWARE vSphere Client (Gerenciador de VM's)

Fonte: blogs.vmware.com, 2016.

2.3. Containers

> "O software conteinerizado é exatamente a mesma ideia do contêiner de mercadorias em navios: uma embalagem e distribuição padrão que é genérico e muito difundido, permitindo um transporte muito maior de capacidade, custos mais baixos, economias de escala e facilidade de manuseio. O container contém tudo o que o aplicativo precisa para ser executado, incorporado em um arquivo de imagem que pode ser executado por um software gerenciador de containers" (Arundel e Domingus, p. 8)

Outra definição interessante sobre containers é do portal IT Forum:

> "...a tecnologia de container é uma metodologia utilizada para empacotar aplicações para que possam ser executadas/disponibilizadas com o seu subset de dependências de maneira isolada e eficiente no intuito de segregar e facilitar a portabilidade dessas aplicações."

Somando às definições ditas, é possível também entender a tecnologia de forma lúdica, como imaginar um Engenheiro de Software que está criando uma aplicação em uma linguagem de programação, como Python por exemplo. Nesse projeto, o Engenheiro utiliza várias bibliotecas do Python (uma linguagem de programação), criadas pela comunidade. Para isso é preciso baixá-las para o computador. Terminado o projeto, o Engenheiro envia sua aplicação para quem encomendou-a, porém, assim que a pessoa que o contratou vai iniciar a aplicação, ele recebe vários erros, de falta de bibliotecas e até erros provenientes da versão diferente do Python que ele tem no sistema. Esse problema conhecido como "no meu computador funciona, mas no seu não", era algo comum para Engenheiros de Software, antes da tecnologia de containers. Assim como dito na definição da IT Fórum, com a tecnologia de containers é possível empacotar a aplicação, com todas as dependências necessárias para que ela rode de forma satisfatória. Além disso, há uma camada a mais de segurança, pois o sistema vai

rodar essa aplicação no container, assim, a aplicação estará isolada do sistema principal. Com isso, ataques e acessos indevidos no container não conseguem acesso direto ao sistema principal. Por fim, de forma simplificada, containers são extremamente leves, construídos com sistemas Linux, apenas com o essencial para que ele rode a aplicação em questão, podendo serem customizados da forma que for desejável.

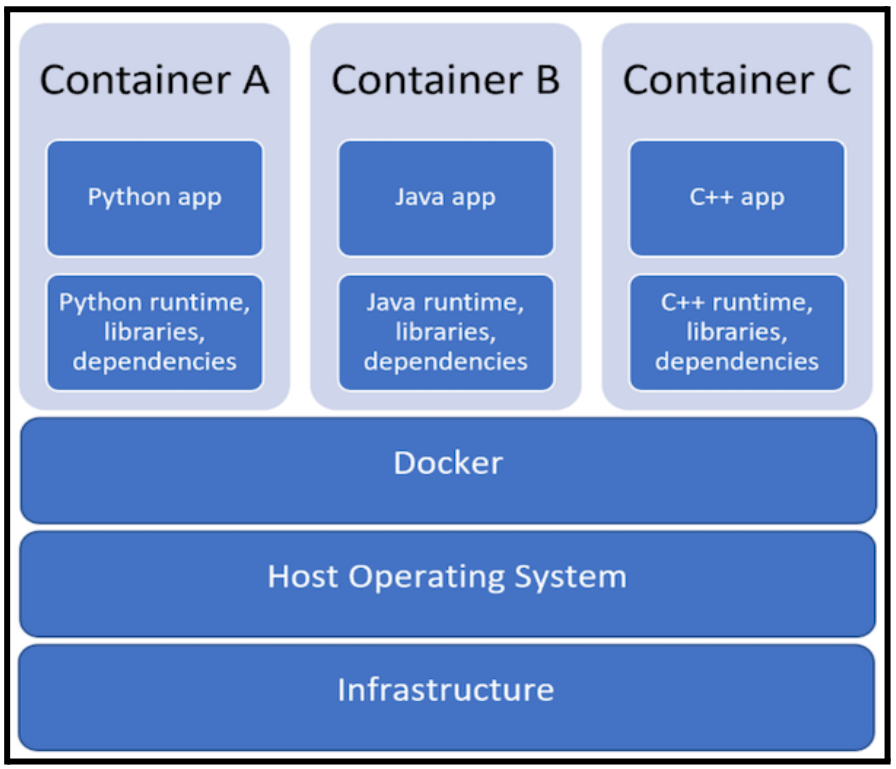

Figura 3. Arquitetura de um container docker

Fonte: code.visualstudio.com.

2.4. Computação em Nuvem

> *"Quando você usa a infraestrutura em nuvem para executar seus próprios serviços, o que você está comprando é infraestrutura como serviço (IaaS). Você não precisa gastar capital para comprá-lo, você não precisa construí-lo e você não precisa atualizá-lo. É apenas uma mercadoria, como eletricidade ou água."* (Arundel e Domingus, p. 3)

Já é de conhecimento que máquinas virtuais e containers trouxeram grande praticidade para os profissionais de T.I e as empresas. Agora, com a chegada da computação de nuvem, nem mesmo os datacenters para alojar as VM's e/ou os containers são necessários manter na empresa. Essa é a premissa da computação em nuvem. Como a própria definição da AWS diz, a computação em nuvem é a entrega de recursos de T.I sob demanda por meio da Internet com definição de preço de pagamento conforme o uso. Com isso, em vez de comprar, ter e manter datacenters e servidores físicos na empresa, é possível acessar serviços de tecnologia, como capacidade computacional, armazenamento e bancos de dados, conforme a necessidade, usando um provedor de nuvem. Com o advento da nuvem, ou cloud (nuvem em inglês), a empresa pode ter toda a praticidade de recursos de T.I entregues como um serviço. O setor de tecnologia precisa de nova instância (VM) com 16gb de memória, 8 cores de

processador e rodando um sistema operacional Linux, ou mesmo Windows ou MacOs? Isso é possível com poucos cliques, e em alguns minutos já há uma nova instância, ou um cluster (conjunto) de containers rodando, sem se preocupar com hardware. As empresas que oferecem serviços em nuvem, como Amazon AWS, Google e Microsoft, mantêm datacenters ao redor do mundo para alocar todos esses serviços, e com isso também oferecem grande disponibilidade desses recursos, pois há uma replicação dos dados ao redor dos datacenters. Ou seja, não é preciso mais se preocupar em realizar o backup de dados para recuperá-los caso por exemplo o disco rígido queime, o provedor de nuvem mantém esses dados em mais de um lugar para evitar esses problemas.

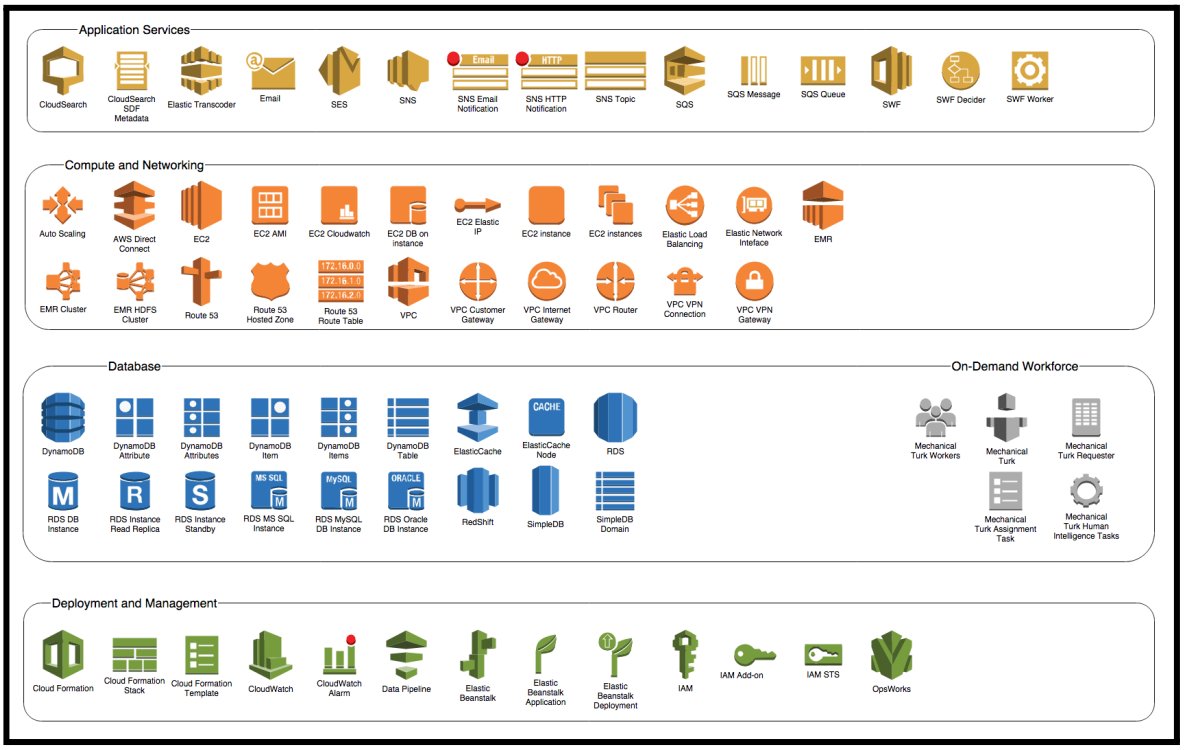

Figura 4. Serviços oferecidos pela Amazon Web Services

Fonte: blog.saninternet.com

2.5. Suse Manager

> *"O SUSE Manager é uma ferramenta única que permite ao pessoal de TI provisionar, configurar, gerenciar e atualizar todos os sistemas Linux na rede da mesma forma, independentemente de como e onde eles estão implantados. Da instalação remota à orquestração da nuvem, atualizações automáticas, configuração personalizada, conformidade e segurança auditorias, o SUSE Manager habilmente lida com o ciclo de vida de Clientes Linux." (Cayouette and SUSE Manager Team, p. 2)*

Segundo a própria homepage da empresa SUSE, o SUSE Manager é uma solução de gerenciamento de infraestrutura de T.I de código-fonte aberto para a sua infraestrutura. O software foi projetado para ajudar as equipes de Operações de TI e DevOps (profissional de T.I que foca em automação e soluções de problemas desenvolvendo aplicações) das empresas a reduzir a complexidade e recuperar o controle de bens de TI, permitindo gerenciamento abrangente de sistemas Linux, VM's e containers com uma solução única e centralizada.

O SUSE Manager provê uma série de ferramentas para facilitar o dia-a-dia do Administrador, como a possibilidade de automatização de várias tarefas, aplicação de patches, monitoração, controle, auditoria e a geração de relatórios de sistemas como VM's e containers, para assegurar a conformidade com políticas internas e normas externas vigentes. Sua implementação, deve ocorrer em servidores com Sistema Operacional Suse Linux, e o valor de uma licença SUSE Manager varia entre $250 a $2.000 de acordo com as especificações contratadas. O SUSE Manager também conta com um software de configuração de sistemas chamado SALT, da empresa Saltstack, que pode auxiliar muito na aplicação de automações de forma única em todos os sistemas. Será apresentado essas ferramentas citadas, e outras mais, de forma aprofundada no decorrer do relatório.

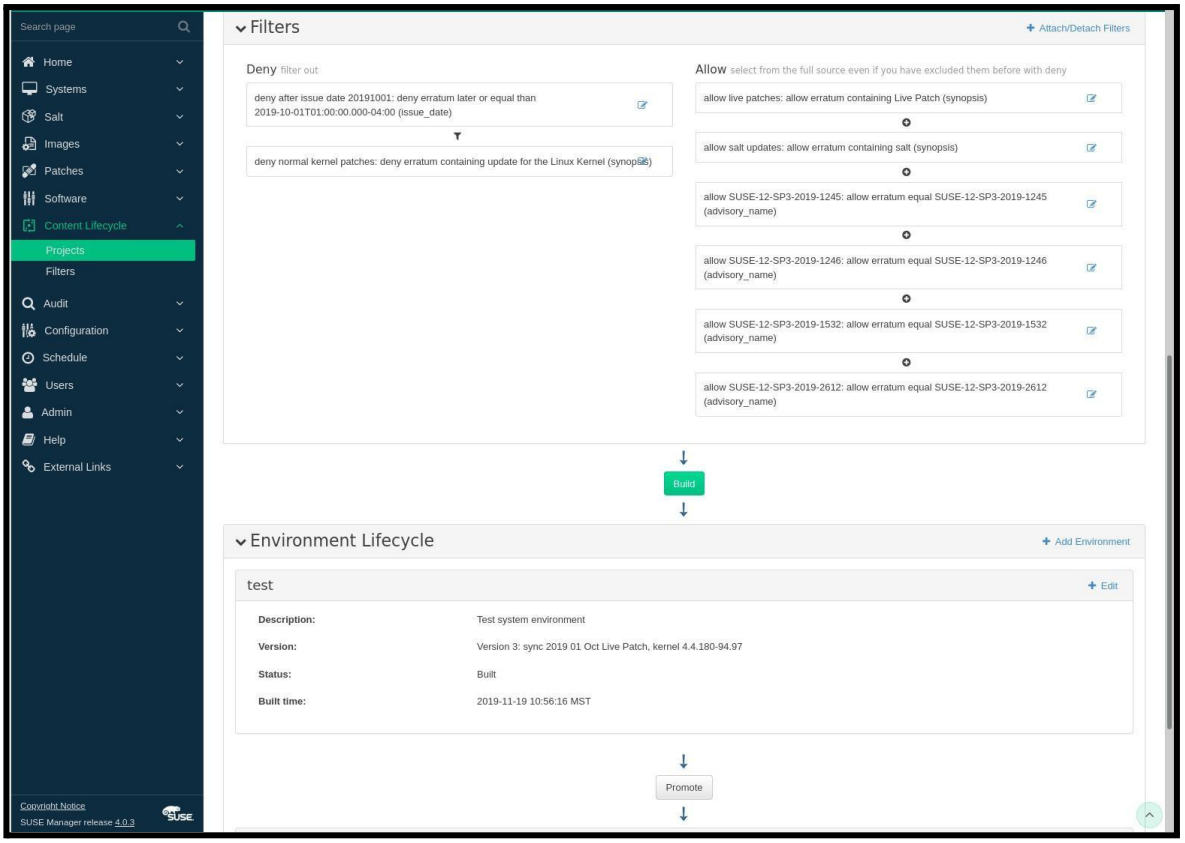

Figura 5. Painel do Suse Manager

Fonte: suse.com

2.6. Saltstack

> *"SaltStack (ou Salt, para abreviar) é um projeto de código aberto originalmente destinado a ser um sistema de execução remota extremamente rápido. Salt é a maneira mais fácil e poderosa de gerenciar seus servidores. Se você tem alguns, centenas ou mesmo dezenas de milhares de servidores, você pode usar Salt para gerenciar a partir de um único ponto central. Você pode usá-lo para segmentar com flexibilidade qualquer subconjunto de seus servidores para executar comandos ou realizar tarefas." (Myers, p. 1)*

O Salt, como dito por Myers, é uma ferramenta de automatização de configuração de servidores. O software Salt lembra muito outra ferramenta mais conhecida, o Ansible, pois ambos usam como estrutura de serialização de dados o formato YAML. Esse formato de código tem a vantagem de ser de fácil entendimento para humanos. Com isso, até uma pessoa leiga em desenvolvimento consegue analisar o que determinada automação irá realizar quando esta for executada.

O Salt é utilizado pelo SUSE Manager para a comunicação entre a Master (Servidor SUSE Manager) e os Minions (Servidores registrados no SUSE Manager), assim, por conta da conveniência de haver de uma forma fácil a configuração do Salt já feita, quando implementado o Gerenciador de Ativos SUSE Manager, é interessante para a companhia utilizar o Salt para realizar diversos tipos de automações caso deseje.

Assim como o Ansible, o Salt conta com vários módulos criados pela comunidade, para atuar com muitas tecnologias diferentes, desde tarefas simples como a criação de usuários, à configuração de clusters VMWare ESXi. Em consequência dessa praticidade, a ferramenta Salt pode ser muito útil para que o Administrador mantenha de forma ágil o compliance (conformidade) de servidores, sendo necessário apenas o desenvolvimento de uma única automação para realizar a configuração de centenas ou milhares de servidores da forma desejada, com apenas um clique.

Na figura 6 abaixo, há um exemplo de uma automação para criação do usuário “fred”, e a remoção do usuário “testuser”.

Figura 6. Exemplo de uso do módulo ‘user’ do Salt

Fonte: docs.saltproject.io

É possível analisar como a utilização do formato YAML facilita o entendimento do que irá ser feito.
Já na figura 7 abaixo há a utilização do módulo ‘file’ para a cópia de um template entre o repositório da automação e os servidores.

```jinja
/etc/http/conf/http.conf:
  file.managed:
    - source: salt://apache/http.conf
    - user: root
    - group: root
    - mode: 644
    - attrs: ai
    - template: jinja
    - defaults:
        custom_var: "default value"
        other_var: 123
{% if grains['os'] == 'Ubuntu' %}
    - context:
        custom_var: "override"
{% endif %}
```

Figura 7. Exemplo de uso do módulo ‘file’ do Salt

Fonte: docs.saltproject.io

Nesse contexto, é possível também verificar que está sendo utilizada a condicional if/else para que a variável custom_var receba outro valor quando a execução da automação for realizada em hosts com o Sistema Operacional Ubuntu. É interessante reparar nisso para que seja entendido o quão customizável pode ser a automação de acordo com as necessidades do Administrador de Sistemas.

3. Atualizações de Segurança

Na seção atual será abordado métodos relacionados a manutenção de servidores Linux atualizados com os patches de segurança para software e bibliotecas dos sistemas.

3.1. Patches

Patches, ou Erratas, na área de T.I, são pacotes que são aplicados em softwares com a finalidade de consertar bugs e/ou adicionar novas funções ao software em questão. Nesse caso em específico, é considerado como patches de seguranças aqueles que tem o principal intuito de resolver vulnerabilidades encontradas no software, e que podem acarretar uma facilidade para que pessoas mal intencionadas à explorem para obter algum tipo de acesso ao sistema, e/ou a dados.

Segundo pesquisa de Jean Carlos Bormanieri (2018, p.4), 37,5% das micro e pequenas empresas pesquisadas não possuíam nenhum processo de atualização de Sistemas Operacionais com patches de segurança, e mesmo as que responderam que tinham algum processo para atualização de patches, 62,5% possuíam apenas o gerenciador de aplicação de patches padrão do Windows, sem citar algo equivalente para ambientes Linux. O que torna a atualização de patches em larga escala, uma tarefa penosa, por não haver um gerenciador que englobe e automatize a aplicação em todos os sistemas.

O processo de atualização de patches em sistemas de produção pode ser uma tarefa complicada. O Administrador precisa levar em consideração inúmeras variáveis antes de decidir realizar a atualização do software defasado, seja ele de terceiros, ou do próprio Sistema Operacional. Segue abaixo alguns pontos:

1 - Essa atualização impactará o funcionamento do software, ou de outros que dependem dele?

2 - Será necessário reiniciar o host após aplicação do patch? Caso sim, haverá uma janela de manutenção para realizar a tarefa?

3 - Preciso parar algum serviço interno do host, antes da aplicação do patch?

4 - O patch altera comportamentos do software, sendo necessário eu alterar serviços?

5 - Há incompatibilidade do software, com outros serviços, após aplicação do patch?

Por conta dessa gama de probabilidades de problemas ao atualizar um software, ambientes produtivos necessitam de gerenciadores de patches que facilitem o trabalho do Administrador em ambientes com uma quantidade grande de máquinas.

3.2. Repositórios de patches

Repositórios de softwares e patches são servidores mantidos pelas empresas responsáveis pela distribuição Linux, onde são disponibilizados softwares e patches para

o Sistema Operacional. Dessa forma, o Administrador consegue apontar seu Sistema Linux para obter esses softwares e patches via download pela internet.

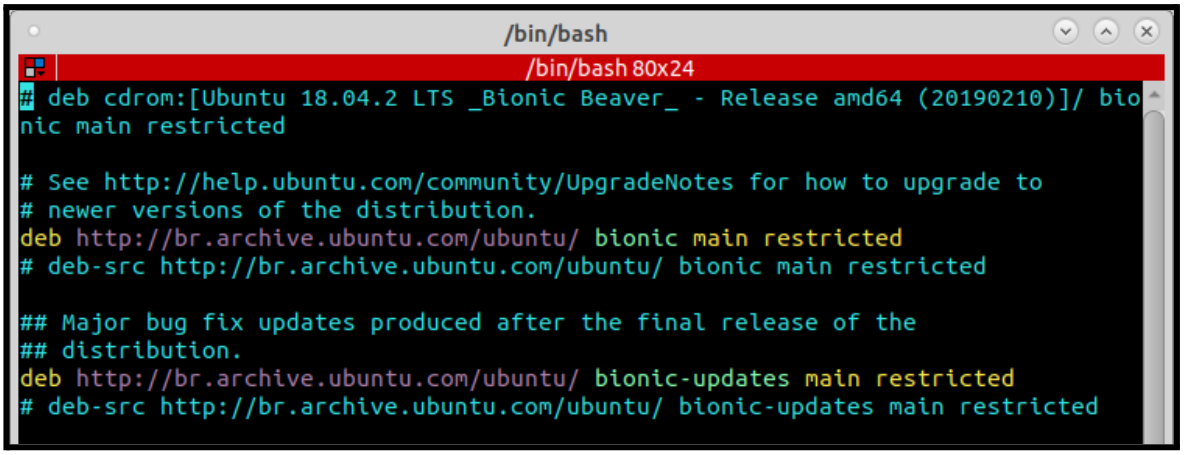

Figura 8. Arquivo de configuração de repositórios no sistema Linux

Fonte: próprio autor.

Analisando a figura 8, é possível verificar endereços web onde o Sistema Operacional irá se conectar em busca de novos softwares e patches. A configuração desses repositórios feito de forma manual, através da edição de arquivos de configuração no terminal Linux, pode levar tempo e acarretar erros de sintaxe e digitação. O problema se agrava se a empresa tem uma quantidade grande de hosts a serem gerenciados. Isso é pode ser melhor gerenciado utilizando algumas ferramentas do SUSE Manager

3.3. Gerenciamento de repositórios via SUSE Manager

O SUSE Manager conta com algumas ferramentas para facilitação no gerenciamento de repositórios do Sistema Operacional, de forma que possa ser realizada a configuração e customização em larga escala para o parque de máquinas de Sistemas Linux da empresa.

Através de seu painel é possível realizar a criação de repositórios customizados, configuração de canais de repositórios para inúmeras distribuições Linux de uma só vez, sincronização dos repositórios internamento, além da alteração e exclusão desses canais de repositório de maneira simples.

3.4. Sincronização Interna de repositórios

Após a habilitação de determinada distribuição Linux através do painel de produtos do SUSE Manager, a ferramenta se conecta aos servidores de repositórios da distribuição e realiza o download de todos os pacotes e patches de software do repositório em questão. E isso se repete rotineiramente para que haja sempre novos patches disponíveis internamente para servir aos hosts.

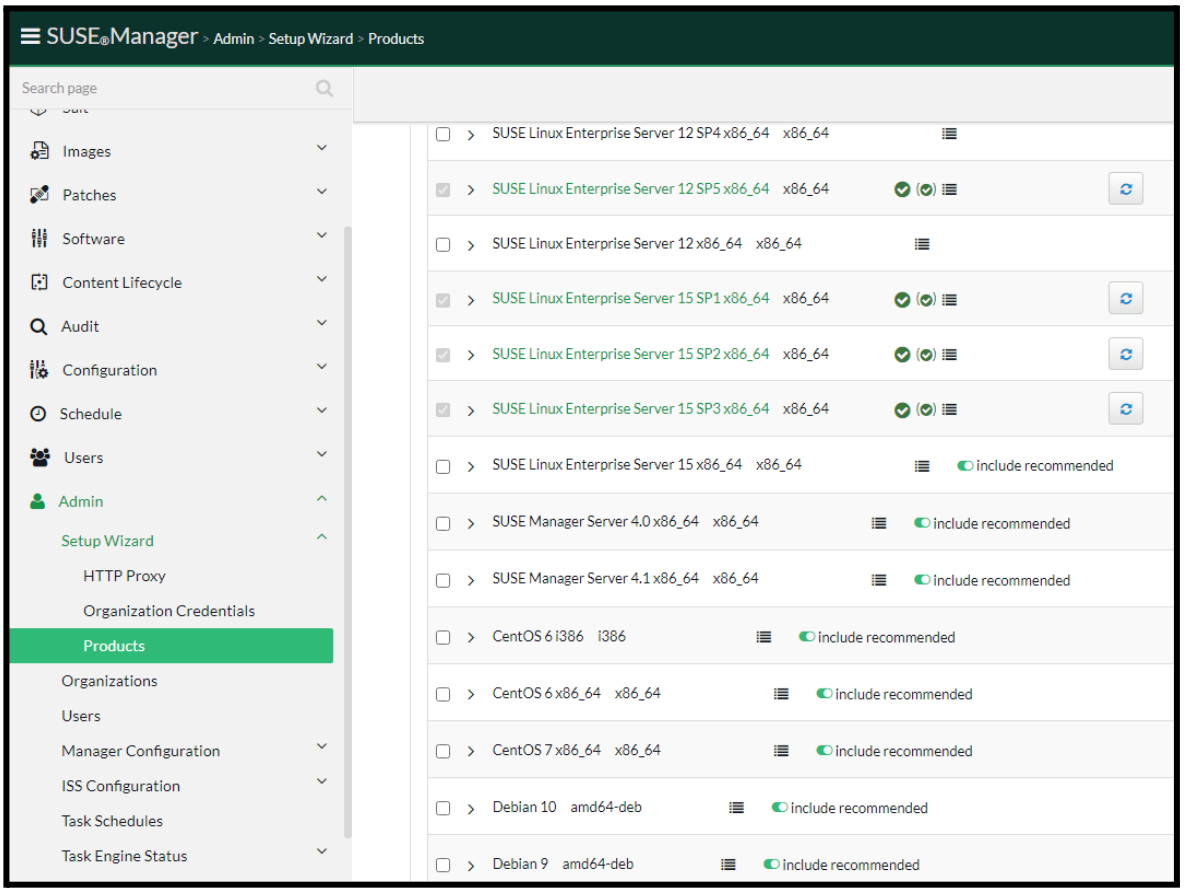

Figura 9. Amostra de repositórios de produtos disponíveis no SUSE Manager
Fonte: próprio autor.

Com isso, os hosts não precisam necessariamente ter conexão com a internet para realizar a atualização de seu Sistema Operacional ou de softwares e serviços instalados. Assim, há uma camada de segurança importante para os hosts que estão registrados no SUSE Manager e dependem desses patches de segurança.

3.5. Ciclo de vida de conteúdo dos repositórios

Além dos repositórios oficiais, que estão rotineiramente sendo atualizados de forma automática pelo SUSE Manager, há uma ferramenta chamada Content Lifecycle Management, que, como o nome diz, facilita o gerenciamento do ciclo de vida de conteúdos do repositório. Segundo o próprio site da SUSE, o Content Lifecycle Management permite personalizar e testar pacotes antes de atualizar os sistemas de produção. Isso é especialmente útil se for preciso aplicar atualizações durante uma janela de manutenção limitada. Ou seja, é possível criar etapas para os repositórios, como uma simulação de ambientes que ocorra dentro da empresa (desenvolvimento, qualidade e produção, por exemplo). Com isso, é realizado testes em máquinas menos críticas, e caso necessário, ajustado o repositório antes de promovê-lo para ambientes em produção.

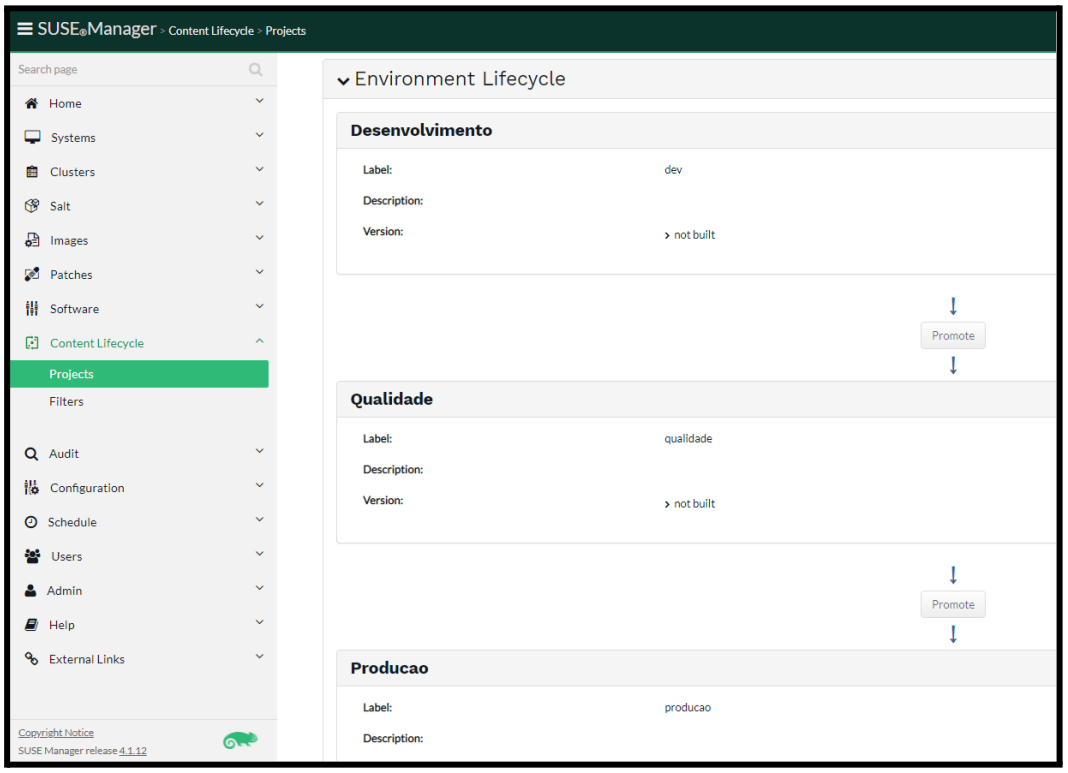

Figura 10. Criação de ambientes para testes de repositórios

Fonte: próprio autor.

Essa ferramenta ainda possibilita que seja aplicado filtros para reter ou liberar pacotes que o responsável deseje que façam parte, ou não, dos repositórios que serão entregues às máquinas. Dessa forma, não haverá surpresas indesejáveis, como a atualização de um software que conflite com os apps do time de desenvolvimento, por exemplo.

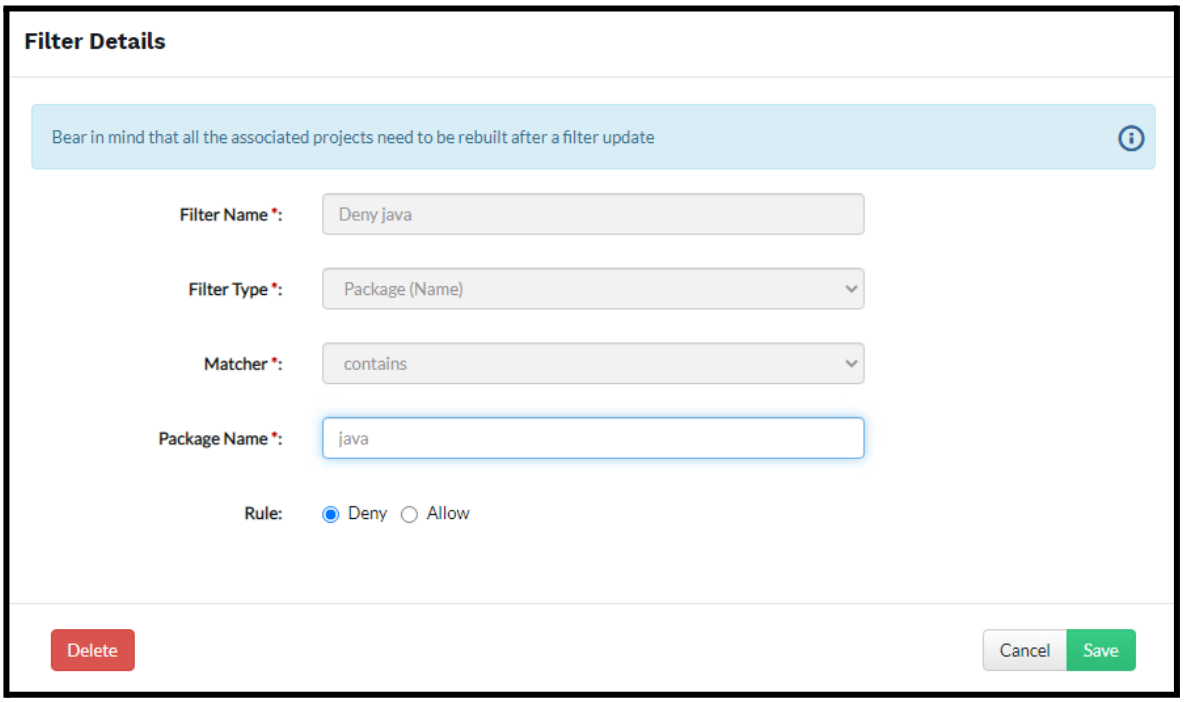

Figura 11. Criação de filtro

Fonte: próprio autor.

Por fim, quando é criado um projeto no Content Lifecycle, ele realiza um "congelamento" dos repositórios escolhidos como as fontes do projeto. As fontes, são onde a ferramenta irá buscar por novos patches de correções. Essa é uma forma melhor de gerenciamento dos repositórios do Content Lifecycle. Assim, diferentemente de apontar os servidores para um repositório oficial que é atualizado constantemente, e com isso, todos os dias ter patches e pacotes novos que nem sempre o responsável tem tempo para analisar minuciosamente, o que será realizado de mudanças nos servidores ao aplicá-lo, no Content Lifecycle esse congelamento dos repositórios mantém os mesmos pacotes e patches do dia que foi feito o projeto. Dessa forma, após testes serem realizados pelo Administrador, é possível criar um rebuild do projeto com novos patches e pacotes da data atual, e assim sucessivamente, de uma maneira mais segura.

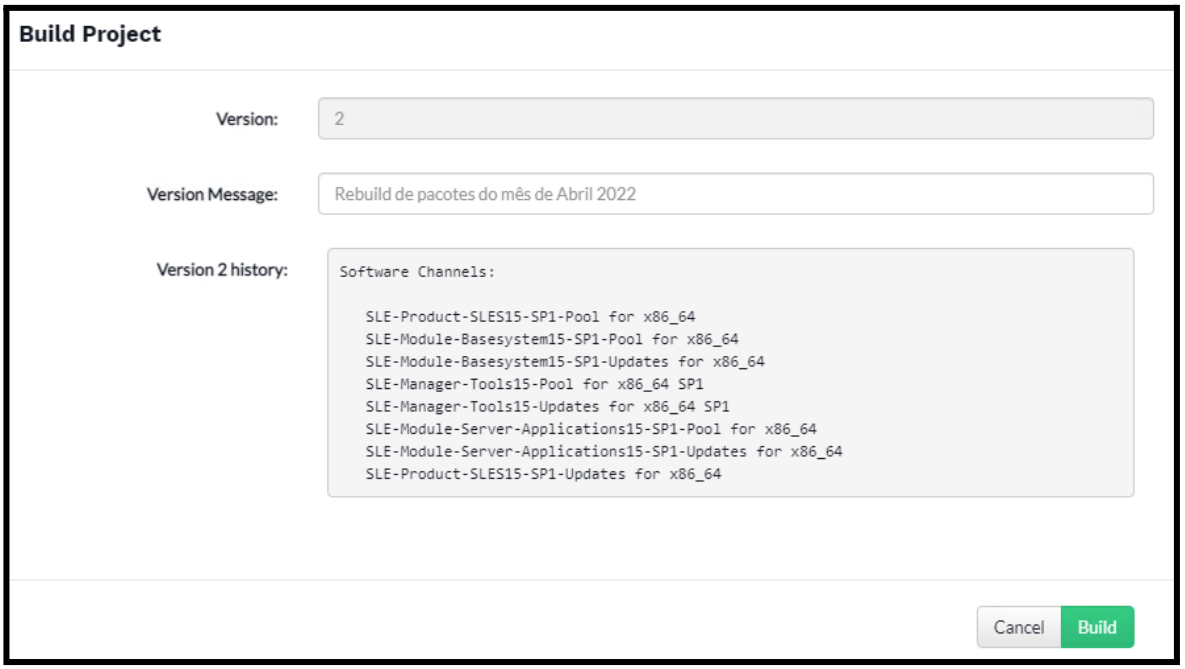

Figura 12. Rebuild de Projeto no Content Lifecycle

Fonte: próprio autor.

Na figura acima é apresentado a tela de rebuild de canais de repositórios com novos patches do mês vigente, a serem adicionados.

4. Auditoria de Segurança

Nessa seção serão estudadas as ferramentas disponíveis no SUSE Manager para a auditoria de segurança em sistemas operacionais.

4.1. Escaneamento de vulnerabilidades com OpenSCAP

O SUSE Manager oferece a possibilidade de realizar scans utilizando o OpenSCAP para analisar se o sistema encontra-se compliance com as especificações de diretrizes de segurança de órgãos reguladores.

Segundo o site do projeto, o OpenSCAP fornece ferramentas de auditoria para verificação automatizada de vulnerabilidades, permitindo que sejam tomadas as medidas para evitar ataques antes que eles aconteçam. Essas ferramentas auxiliam administradores e auditores na avaliação, medição e aplicação de linhas de base de segurança.

Ainda de acordo com a documentação do SUSE Manager, O Security Certification and Authorization Package (SCAP) é uma solução padronizada de verificação de conformidade para infraestruturas Linux de nível empresarial. É uma linha de especificações mantida pelo Instituto Nacional de Padrões e Tecnologia (NIST) para manter a segurança do sistema para sistemas corporativos. O SUSE Manager utiliza o OpenSCAP para implementar as especificações do SCAP. O OpenSCAP utiliza o Extensible Configuration Checklist Description Format (XCCDF). O XCCDF é uma maneira padrão de expressar o conteúdo da lista de verificação de segurança. Ele também combina com outras especificações, como Common Platform Enumeration (CPE), Common Configuration Enumeration (CCE) e Open Vulnerability and Assessment Language (OVAL), para criar uma lista de verificação expressa por SCAP.

Através do Painel do SUSE Manager é possível realizar o escaneamento dos servidores, como no exemplo da figura abaixo.

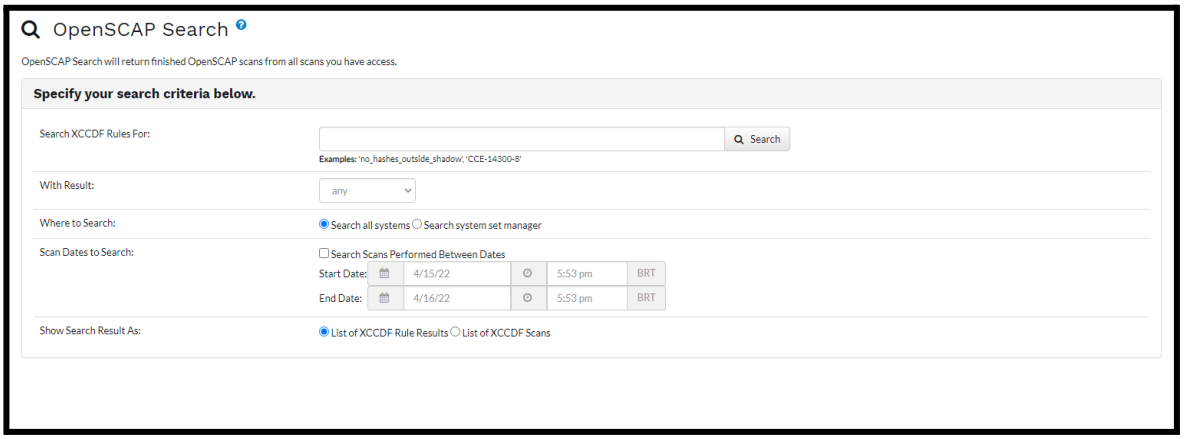

Figura 13. OpenSCAP Search

Fonte: próprio autor.

De acordo com a documentação do SUSE Manager, o OpenSCAP verifica a presença de patches usando o conteúdo produzido pela SUSE Security Team, e analisa as configurações de segurança do sistema e os examina quanto a sinais de comprometimento usando regras baseadas em padrões e especificações.

4.2. CVE's

De acordo com o site ECOIT, a Commom Vulnerabilities and Exposures, ou CVE, é uma iniciativa colaborativa de diversas organizações de tecnologia e segurança que desenvolvem listas de nomes padronizados para vulnerabilidades e outras exposições de segurança.

A CVE tem como objetivo padronizar as vulnerabilidades e riscos conhecidos no mundo da Tecnologia da Informação, dessa forma, facilitando a procura, o acesso e o compartilhamento de dados entre diversos indivíduos e empresas, auxiliando os profissionais da Tecnologia da Informação na procura e correção de vulnerabilidades de forma mais ágil e organizada.

4.3. Ferramenta CVE Audit

No SUSE Manager, há uma ferramenta chamada CVE Audit que auxilia o Administrador a saber se determinado CVE está aplicado nos sistemas que ele é responsável. Além disso, pesquisando pela CVE, é possível saber se há patches disponíveis para correção daquelas vulnerabilidades nos canais de repositórios atrelados ou não aos seus sistemas.

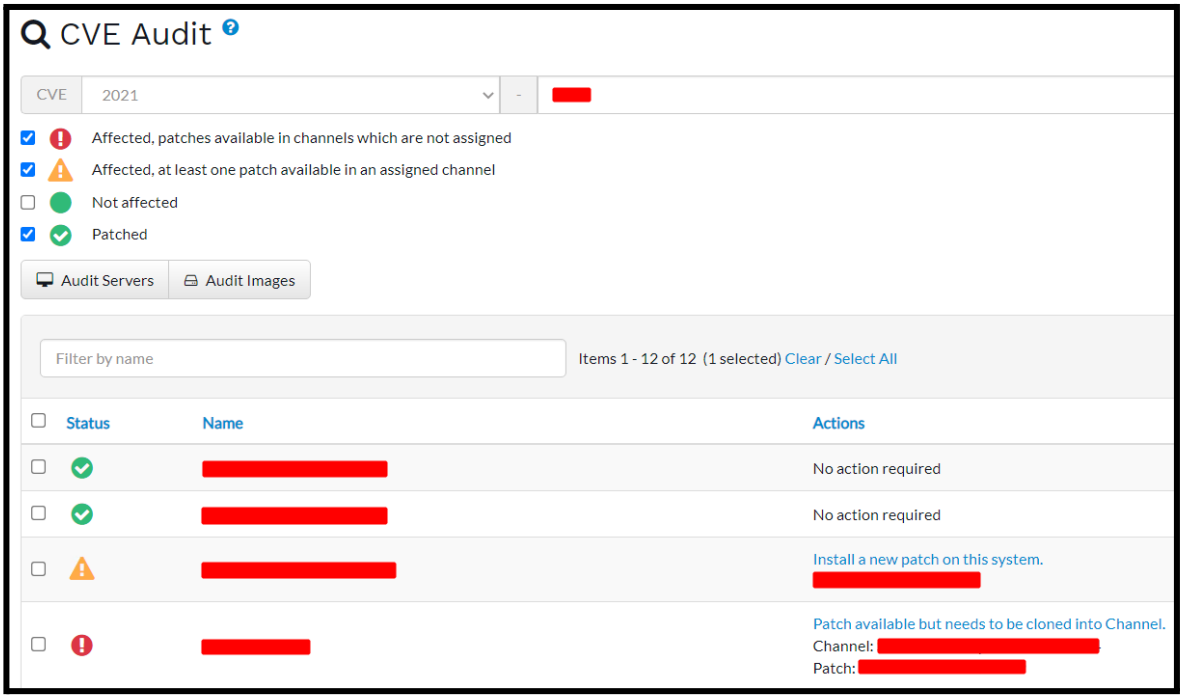

Figura 14. CVE Audit

Fonte: próprio autor.

Analisando a figura acima, é possível identificar a pesquisa por uma CVE (omitida aqui, juntamente com o nome dos sistemas, e o patch de correção, por uma

questão de segurança) em específico. Com isso, existe o retorno da pesquisa com o resultado de sistemas Linux que podem estar vulneráveis e expostos a falhas de códigos encontrados pelas organizações e descritos na CVE. É possível também analisar que dentre os quatro sistemas que aparecem, há três cenários. Dois deles já contam com os patches, para aquela CVE, aplicados. Um, é afetado pela CVE, mas há um patch nos canais de repositórios do Sistema que ao ser aplicado solucionará a vulnerabilidade. E por fim, há um sistema que também é afetado pelas vulnerabilidades descritas na CVE, porém é necessário realizar o clone desse patch de outro canal de repositórios, pois o mesmo não está atrelado ao Sistema em questão.

5. Automação com Saltstack

Nessa seção serão expostas as principais ferramentas disponibilizadas pelo SUSE Manager para automação de configurações através do Salt. Apesar de haver a possibilidade de utilizar o painel gráfico do SUSE Manager para trabalhar com o Salt, o Administrador pode desenvolver suas próprias automações, utilizando o Salt, e aplicar elas aos sistemas também via linha de comando, diretamente do terminal dos servidores do SUSE Manager, ou mesmo dentro dos sistemas.

5.1. Comandos Remotos

Através da ferramenta Remote Command, disponibilizada pelo SUSE Manager, é possível realizar comandos remotos Salt nos sistemas clientes registrados. Essa ferramenta se mostra muito útil para o Administrador que queira rodar comandos dos mais variados (alteração de arquivos, criação de novos diretórios, recuperação de informações, entre outros), em sistemas sem a necessidade de entrar em cada um deles localmente ou por SSH (Protocolo de Shell Seguro). É ainda possível utilizar wildcards nos nomes dos sistemas para realizar um filtro, e assim executar o comando em vários sistemas de uma única vez.

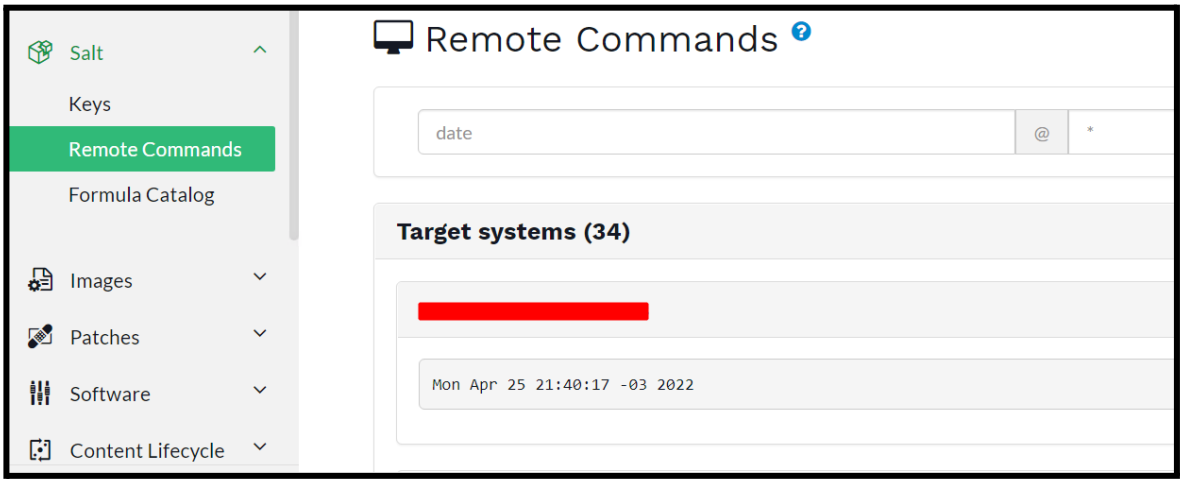

Figura 15. Comando remoto em vários hosts

Fonte: próprio autor.

5.2. Catálogo de Fórmulas Salt

Segundo a documentação do Projeto Saltstack, as fórmulas são módulos do Salt em conjunto para um fim específico de configuração. Eles são de código fonte aberto, como os próprios módulos do Salt, e podem ser usados para tarefas como instalar um pacote, configurar e iniciar um serviço, configurar usuários ou permissões e muitas outras tarefas comuns.

No SUSE Manager, existem algumas dessas fórmulas prontas para serem utilizadas em sistemas clientes registrados. Com isso, é possível ter um serviço instalado e configurado em poucos cliques diretamente do painel gráfico.

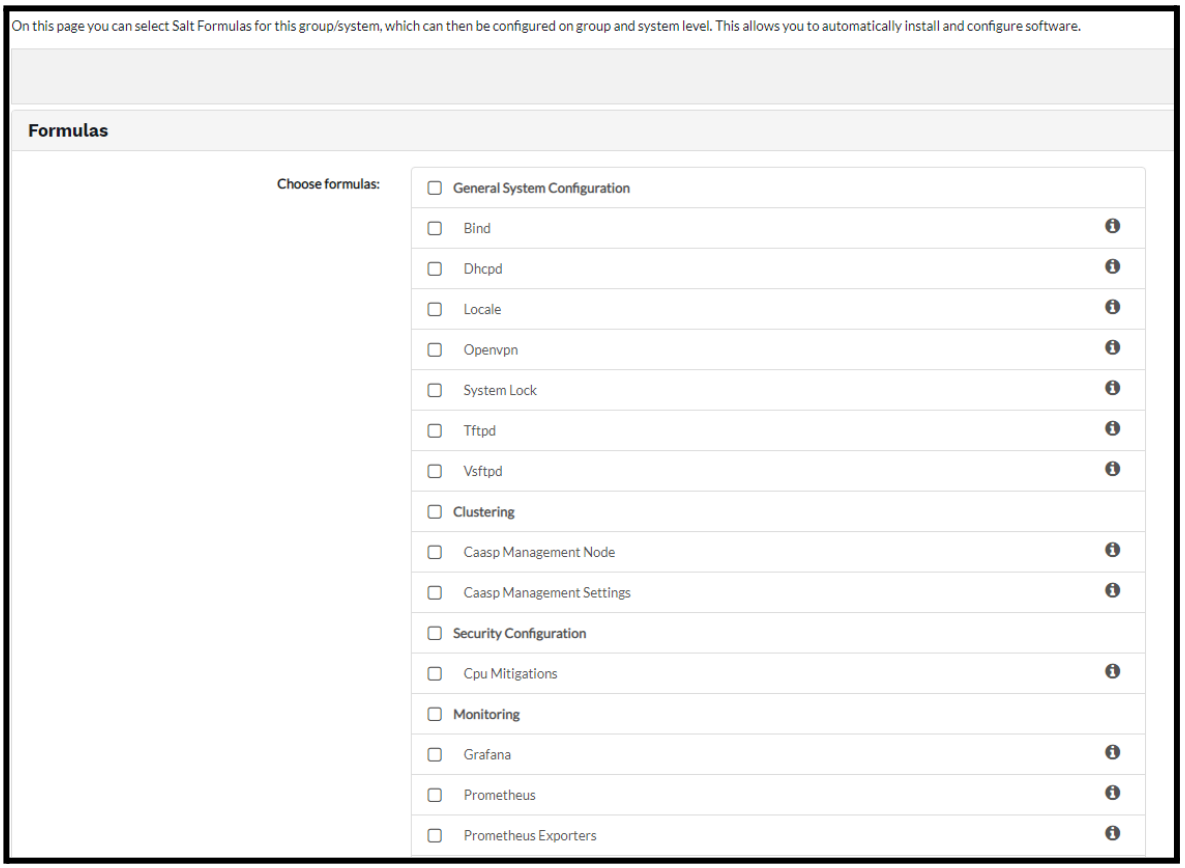

Figura 16. Utilizando Fórmulas Salt

Fonte: próprio autor.

6. Configuração Centralizada de Sistemas

Através do menu Configuration, é possível criar arquivos de configuração inicial para vários sistemas clientes registrados no SUSE Manager. Esses arquivos são executados no momento que o arquivo de configuração for atribuído ao Sistema, e de acordo com os parâmetros passados no arquivo, os sistemas são modificados da maneira escolhida. Dessa forma, o Administrador tem a certeza que seus sistemas estarão em compliance com as diretrizes de Segurança da Organização.

Na figura abaixo há um exemplo da tela de gerenciamento de configuração centralizada de sistemas via arquivos.

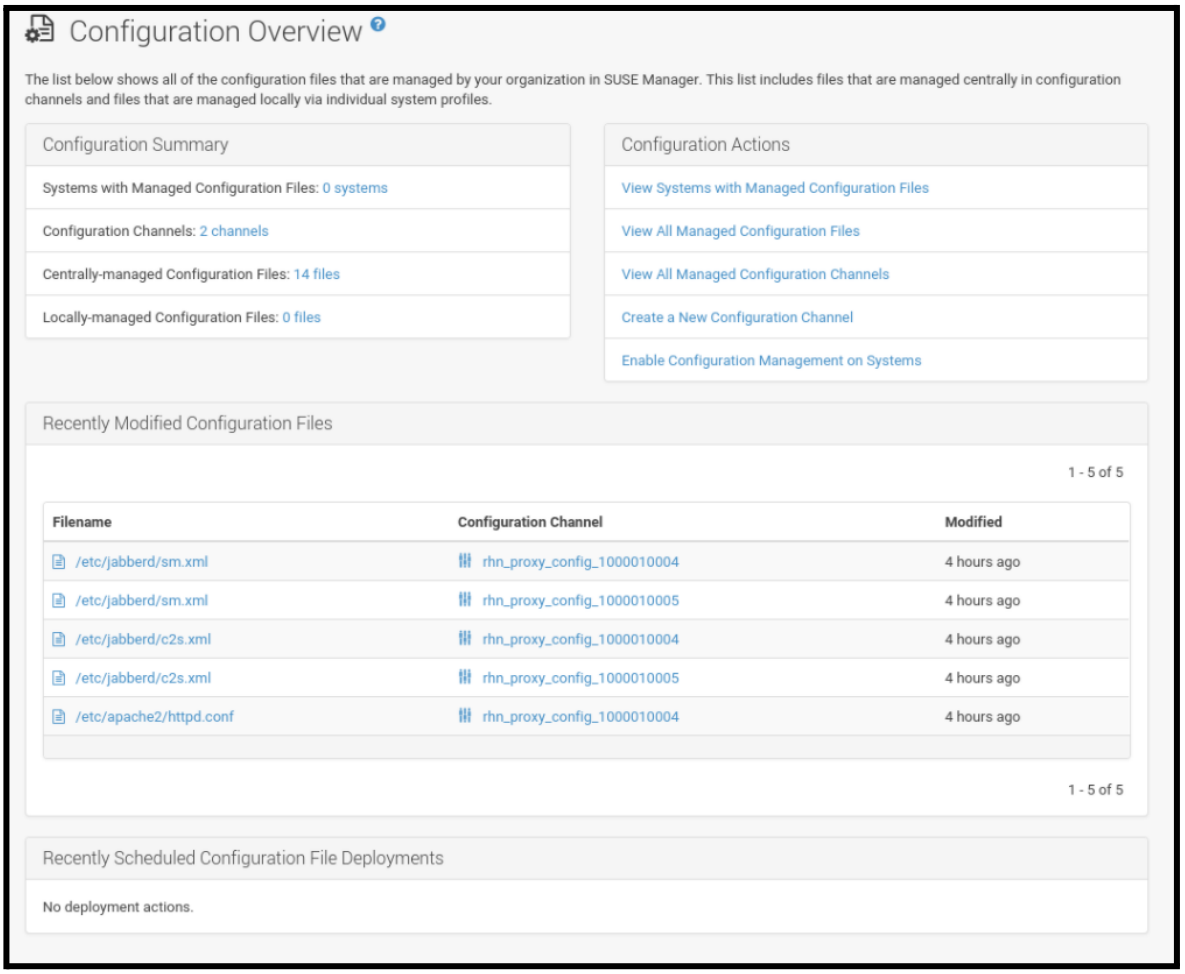

Figura 17. Menu de Configuração Centralizada de Sistemas

Fonte: documentation.suse.com.

7. Estudos de Casos

Nesta seção será apresentado ao leitor alguns estudos de casos de sucesso ao utilizar o SUSE Manager na resolução de problemas, bem como melhorias nos processos da Tecnologia da Informação da organização. Os estudos aqui apresentados podem ser conferidos diretamente através do endereço suse.com/pt-br/success.

7.1. Via Varejo

A Via Varejo é uma varejista de eletroeletrônicos que mantém em sua administração lojas físicas e virtuais como Casas Bahia e Ponto. A empresa está presente em mais de 400 municípios brasileiros, com cerca de 1 mil lojas físicas, 26 centros de distribuição e 41 mil colaboradores. A empresa conta com cerca de 25 mil hosts.

7.1.1. O problema

A Via Varejo, por conta de seu porte e atividades em todo o território, mantém cerca de 25 mil terminais espalhados pelo Brasil, e a manutenção, atualização e gerenciamento de políticas de segurança de todos esses hosts se tornou penosa e complexa, com dificuldades logísticas e problemas para se ter uma visão ágil e centralizada dessas máquinas.

7.1.2. A solução

Com a implementação do SUSE Manager, foi possível realizar a automação dos sistemas, centralização do acesso às informações de toda a infraestrutura, permitindo assim que os administradores pudessem executar intervenções ágeis e eficientes ao se deparar com algum problema.

Segundo José Maria Pessoa, Diretor de Industries da SUSE, os grandes varejistas devem seguir políticas de segurança e conformidade específicas para o segmento, e com as ferramentas de segurança e auditoria disponibilizadas pelo SUSE Manager, permitiu que a Via Varejo garantisse a disponibilidade de terminais conforme regras de negócio definidas e as regulamentações vigentes.

Agora a Via Varejo tem a possibilidade de realizar atualizações e políticas de segurança diretamente do Data Center do grupo em São Caetano, na grande São Paulo.

De acordo com Márcio Borges, Gerente de Infraestrutura da Via Varejo, a solução permitiu a eles escanear todo o ciclo das máquinas e atualizar as configurações do Sistema em tempo ágil. Por exemplo, quando há uma nova campanha, existe a possibilidade de atualizar os cerca de 25 mil terminais de uma única vez, como adicionar uma nova tela referente a promoção nos pontos de atendimento.

7.2. Viollier

A Viollier é um conceituado laboratório de saúde suiço, que é especializado em diagnóstico clínico, patologias, cardiológicas e medicamentos. A empresa conta com 700 funcionários, espalhados por 15 pontos de atendimento na Suíça.

7.2.1. O problema

Após a passagem de toda a infraestrutura física para um ambiente de virtualização, a Viollier se deparou com muitas vantagens, como realizar testes de forma fácil e ágil sem impactar sistemas de produção. Porém, com o aumento expressivo de máquinas virtuais no ambiente, a empresa se encontrou numa questão complicada: Como gerenciar a segurança de seu ambiente em constante crescimento, sem a necessidade de aumentar substancialmente o número de funcionários da área?

Marc Karcher, Gestor de projetos da Viollier, afirma: “Executamos em torno de 50 instâncias do SUSE Linux Enterprise Server. No passado, era difícil e demorado mantê-las protegidas pelos mais recentes patches de segurança, uma vez que tínhamos de atualizar cada instância individualmente. Quando a nossa empresa parceira nos fez uma demonstração esclarecedora de como um bug, como o Shellshock, pode atacar e destruir sistemas vulneráveis, nós sabíamos que tínhamos que encontrar uma forma melhor de proteger o nosso ambiente”.

7.2.2. A solução

Com a implementação do SUSE Manager, a empresa Viollier resolveu os problemas relacionados com a aplicação de patches de segurança. Segundo o Caso estudado, a empresa agora pode realizar testes de novas atualizações cuidadosamente para detectar e resolver quaisquer problemas e, em seguida, aplicá-las à estrutura de produção.

De acordo com Marc Karcher, anteriormente, a empresa demorava cerca de 25 horas para realizar a aplicação de patches em todos os ambientes Linux, pois todo o processo era realizado de forma manual, servidor por servidor. Após a implementação do SUSE Manager, a aplicação de patches caiu para 4 horas, ou seja, 84% mais rápido.

8. Considerações Finais

Com a pesquisa realizada para desenvolver esse trabalho, foi possível entender que o mercado atual de T.I, que está, sempre em constante ampliação e mudança para reter novas tecnologias, até mesmo em empresas pequenas, exige cada vez mais soluções que facilitem o gerenciamento de servidores de forma ágil e automatizada, ainda mais atualmente, que conceitos como IaC (Infra as Code), são tão buscados pelas empresas. Além disso, questões como conformidade e segurança são de extrema importância para a organização, que precisa se adequar a normas internacionais e proteger os dados contra possíveis vazamentos e invasões que podem afetar diretamente os negócios. Pensando nisso, o software SUSE Manager se mostrou muito útil já que conta com várias ferramentas para a facilitação do gerenciamento do parque de máquinas da empresa, sejam eles físicos ou virtuais.

Com relação a verificação de ganho de tempo para o Administrador, foi realizado um teste, com 20 máquinas virtuais, sendo que 10 foram aplicados patches manualmente (via ssh) e 10 foram aplicados patches via SUSE Manager. Como no painel do SUSE Manager é possível realizar a aplicação em todas as máquinas de uma vez, a aplicação manual em todas 10 máquinas, levou um tempo até 10 vezes superior em comparação à aplicação via SUSE Manager. Com isso, é possível concluir que há um ganho de tempo considerável para o Administrator.

Na empresa onde foi pesquisada a utilização do SUSE Manager, no momento do desenvolvimento desse estudo, a solução SUSE Manager se mostra muito útil tanto para Engenheiros de Sistemas, que o utilizam para automatização de processos de configuração e atualização, quanto para Engenheiros de Segurança que fazem uso de ferramentas de auditoria, CVEs e relatórios de segurança. Ainda, o SUSE Manager conta com uma API que é utilizada para realizar integrações com outras ferramentas, agilizando processos e fluxos, e diminuindo interações manuais que são suscetíveis a erros humanos e tempo maior de execução.

Com isso dito, o estudo conclui que ferramentas de gerenciamento de ativos, podem dar uma vantagem para as empresas que o utilizam, por facilitar, padronizar e agilizar processos relacionados às tarefas do dia-a-dia na área da Tecnologia da Informação.

9. Referências Bibliográficas

Arundel, John, and Justin Domingus. Cloud Native DevOps with Kubernetes: Building, Deploying, and Scaling Modern Applications in the Cloud. 1ª ed., Sebastopol, CA, O'Reilly Media, Incorporated, 2019.

BORMANIERI, Jean Carlos. A importância da gestão de patches e atualizações de softwares no ambiente corporativo. Gestão da Segurança da Informação-Unisul Virtual, 2018.

Cayouette, Joseph, and SUSE Manager Team. SUSE Manager 3.1: Best Practices Guide. Edited by SUSE Manager Team, 1ª ed., 12th Media Services, 2017.

Configuration Overview :: SUSE Manager Documentation. SUSE Documentation, 2022. Disponível em: <https://documentation.suse.com/external-tree/en-us/suma/4.0/suse-manager/reference/configuration/config-overview.html>. Acesso em: 10 de mar. de 2022.

Entenda o que é CVE (Common Vulnerabilities and Exposures). Eco IT - Segurança Digital, 2019. Disponível em: <https://blog.ecoit.com.br/o-que-e-cve/>. Acesso em: 10 de mar. de 2022.

Formula Catalog :: SUSE Manager Documentation. SUSE Documentation, 2022. Disponível em: <https://documentation.suse.com/external-tree/en-us/suma/4.0/suse-manager/reference/salt/salt-formula-catalog.html>. Acesso em: 10 de mar. de 2022.

Fritz, G. Blair, et al. Mastering VMware VSphere 6.7. 1ª ed., Indianapolis, Wiley, 2018.

Home | OpenSCAP portal. Openscap, 2022. Disponível em: <https://www.open-scap.org/>. Acesso em: 20 de abr. de 2022.

Máquina virtual (VM): o que é e para que serve uma virtual machine?. Red Hat, 2019. Disponível em: <https://www.redhat.com/pt-br/topics/virtualization/what-is-a-virtual-machine>. Acesso em: 22 de abr. de 2022.

MYERS, Colton. Learning Saltstack - Learn how to manage your infrastructure by utilizing the power of SaltStack. 1ª ed., Birmingham B3 2PB, UK, Packt Publishing Ltd., 2015.

Na era da conteinerização… Afinal, alguém sabe o que é container?. IT Forum, 2020. Disponível em: <https://itforum.com.br/noticias/na-era-da-conteinerizacao-afinal-alguem-sabe-o-que-e-container/>. Acesso em: 15 de mar. de 2022.

Negus, Christopher. Linux Bible. 9ª ed., Indianapolis, Wiley, 2015.

O que é cloud computing (computação em nuvem)? - Amazon Web Services. AWS, 2022. Disponível em: <https://aws.amazon.com/pt/what-is-cloud-computing/>. Acesso em: 20 de mar. de 2022.

SUSE Manager 4 Content Lifecycle Management Deep Dive. SUSE, 2020. Disponível em: <https://www.suse.com/c/suse-manager-4-content-lifecycle-management-deep-dive/>. Acesso em: 12 de mai. de 2022.

SUSE Manager. SUSE, 2021. Disponível em: <https://www.suse.com/pt-br/solutions/manager/>. Acesso em: 12 de mai. de 2022.

System Security via OpenSCAP :: SUSE Manager Documentation. SUSE Documentation, 2022. Disponível em: <https://documentation.suse.com/external-tree/en-us/suma/4.0/suse-manager/reference/audit/audit-openscap-overview.html>. Acesso em: 12 de mai. de 2022.

Via Varejo | Comunidades SUSE. SUSE, 2021. Disponível em: <https://www.suse.com/pt-br/success/suse-supports-via-varejo-in-the-expansion-of-its-business-with-the-digital-transformation-of-its-stores/>. Acesso em: 16 de mai. de 2022.

Viollier | Comunidades SUSE. SUSE, 2021. Disponível em : <https://www.suse.com/pt-br/success/viollier/>. Acesso em: 18 de mai. de 2022.

What is Linux?. Opensource.com, 2022. Disponível em: <https://opensource.com/resources/linux>. Acesso em: 19 de mai. de 2022.