A necessidade da virtualização em *Software* Livre em proveito das Operações Cibernéticas na utilização do Sistema Naval de Ações Cibernéticas

11

Suboficial (HN) Renato Evaristo **Alfaia**

Ingressou na MB em 1994 por meio da Escola de Aprendizes-Marinheiros do Espírito Santo (EAMES). Realizou os cursos de Especialização e Aperfeiçoamento em Hidrografia e Navegação, além do Curso de Assessoria de Estado-Maior para Suboficiais (CASEMSO). Graduado em Sistemas de Informação e pós-graduado em Segurança da Informação. Integrou a turma pioneira de praças no Curso de Guerra Cibernética para Sargentos do Exército no CIGE. Em sua trajetória profissional, foi Administrador de Redes no Navio Oceanográfico Almirante Câmara, na Diretoria de Hidrografia e Navegação e no Navio Hidrográfico Sirius; Supervisor de Segurança da Informação na Diretoria de Hidrografia e Navegação; Encarregado da Seção de Segurança da Informação e Comunicações e Defesa Cibernética no CLTI do Centro de Hidrografia da Marinha; e Operador de Segurança da Informação nas Olimpíadas do Rio de Janeiro em 2016. Participou de várias operações na área de Cibernética (Cibersecuritas, Baluarte, Octopus e Guardião Cibernético) e de operações conjuntas com o Ministério da Defesa (Amazônia, Ágata Norte e Ágata Oeste).

Introdução

A virtualização, um termo proeminente na Tecnologia da Informação e Comunicações, possibilita criar múltiplos ambientes sem a necessidade de *hardware* exclusivo, o que é fundamental para soluções computacionais diversas. Na era de interconexão e dependência da Internet, as organizações devem se precaver contra falhas de *hardware* que afetam decisões estratégicas.

Segundo o Plano Estratégico da Marinha (PEM 2040), a Cibernética é um elemento-chave no contexto naval. O espaço cibernético, um teatro de operações militares sem fronteiras físicas, requer o preparo das Forças Armadas para responder de modo eficaz às ameaças contemporâneas. Assim, a criação de um ambiente concebido para treinamento e o fornecimento de equipamentos e artefatos adequados voltados para a esfera cibernética tornam-se imperativos.

> O espaço cibernético não possui fronteiras físicas, permeia todos os setores (marítimo, terrestre, aéreo e espacial) e é considerado um teatro de operações militares. A vulnerabilidade nesse espaço é uma ameaça contemporânea a ser enfrentada (BRASIL, 2020, p. 31).

É imprescindível, portanto, que as Forças estejam devidamente preparadas para fazer frente a esse tipo de ameaça, respondendo com eficácia e resiliência.

Figura 1: Aspecto básico da virtualização.

Fonte: Truenet Blog, [s.d.].

1. Histórico

Antes mesmo da concepção do PEM 2040, a Marinha do Brasil já desenvolvia iniciativas para testar e preparar as Equipes de Ataque e Defesa Cibernética em suas respectivas áreas de atuação. Em 2011, foram implementadas as Operações Baluarte e Ciber Securitas, cada uma com seus contextos e escopos bem definidos. A primeira tinha como foco principal avaliar as defesas da Rede de Computadores Integrada da Marinha (RECIM) por meio de ataques e explorações reais

em sua infraestrutura, enquanto a segunda criava um ambiente virtual com múltiplas interações, simulando situações quase realistas.

Todas essas operações demandavam considerável capacidade dos recursos computacionais disponíveis, garantindo a condução eficaz dos exercícios e a conclusão satisfatória de seus objetivos. Até 2018, a Divisão de Guerra Cibernética do Comando de Operações Navais (ComOpNav) supervisionava esses exercícios, mas, com a criação do Comando Naval de Operações Especiais (CoNavOpEsp) em 2019, essa responsabilidade foi transferida para a nova organização.

Desde então, a virtualização passou a ser utilizada como um componente adicional, aproveitando-se dos diversos recursos físicos disponíveis na época para criar ambientes adequados às missões propostas, tendo alcançado relativo sucesso em sua execução.

2. O problema da continuidade com a falta de padronização

Apesar dos êxitos alcançados, surgia a impressão de que a criação de cenários e artefatos carecia de continuidade. A diversidade de sistemas e a falta de um padrão pré-estabelecido resultavam em soluções que pareciam não se harmonizar, dando a sensação de que cada operação exigia um recomeço, o que acarretava um considerável retrabalho para as equipes da Divisão de Guerra Cibernética.

Como resposta a essa situação, juntamente com a fundação do CoNavOpEsp, foi criado o Laboratório de Ações Cibernéticas. Subordinado ao Departamento de Operações de Informação, o Laboratório é dedicado à centralização do desenvolvimento de artefatos e infraestrutura para a condução das atividades de Guerra Cibernética.

No entanto, persistiam desafios a serem enfrentados. A proliferação de soluções e a ausência de padronização exigiam que os desenvolvedores se especializassem em diversas tecnologias para criar os artefatos necessários. Além disso, eram consideráveis os custos para manter múltiplas infraestruturas operacionais (tanto físicas quanto virtuais) atualizadas e plenamente funcionais.

3. A solução em *Software* Livre: o Proxmox

Entre as tecnologias disponíveis no Laboratório, uma que não recebia a devida atenção era o Proxmox, uma solução de virtualização fundamentada no GNU/Linux, distribuída sob a licença *GNU Affero General Public License* (AGPL).

Essa solução engloba duas tecnologias essenciais: o *Kernel-based Virtual Machine* (KVM) e os *Linux Containers* (LXC). O hipervisor oferece suporte tanto para a virtualização total quanto para a virtualização assistida por *hardware* fornecida pelo KVM. A empresa mantenedora do projeto, *Proxmox Server Solutions GmbH*, disponibiliza licenças de suporte empresarial que incluem acesso ao repositório empresarial. No entanto, vale ressaltar que a versão gratuita do projeto é robusta e respaldada por uma comunidade ativa.

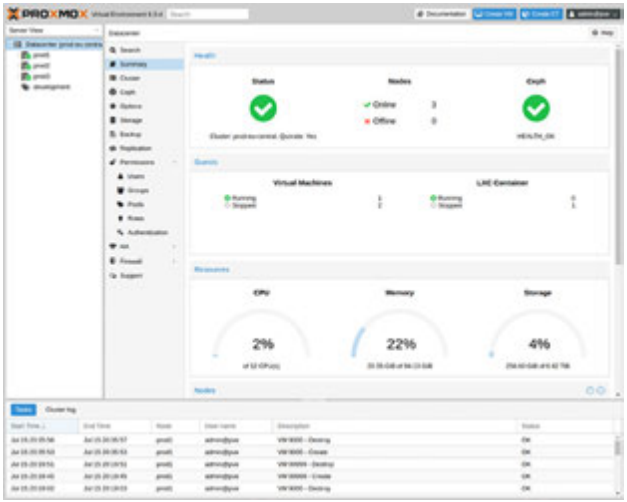
Uma das principais vantagens do Proxmox é sua natureza de código aberto, que se baseia em tecnologias similares. Isso permite o acesso a recursos avançados sem a necessidade de desembolsar quantias vultosas em licenças, em contraste com outras soluções que impõem custos significativos.

Suas características primordiais estão descritas nos subitens a seguir.

3.1. Interface de gerenciamento baseada na *web*

O Proxmox pode realizar todas as tarefas de gerenciamento com a interface gráfica do usuário (GUI) integrada, não havendo necessidade de instalar uma ferramenta de gerenciamento separada. A interface *web* central é baseada na estrutura JavaScript e pode ser acessada a partir de qualquer navegador moderno.

Figura 2: Interface *web* – GUI do Proxmox.



Fonte: Proxmox.

Além das tarefas de gerenciamento, também fornece uma visão geral do histórico de tarefas e dos *logs* do sistema de cada nó. Isso inclui: execução de tarefas de *backup*, migração em tempo real, armazenamento definido por *software* ou atividades acionadas por alta disponibilidade. A ferramenta multiusuário permite o gerenciamento de todo o *cluster* a partir de qualquer nó, não sendo necessário um nó gerenciador dedicado.

3.2. Interface de linha de comando (CLI)

Para usuários avançados acostumados com o conforto do Shell Unix ou do Windows Powershell, o Proxmox VE fornece uma interface de linha de comando para gerenciar todos os componentes do ambiente virtual. Essa interface possui preenchimento inteligente de guias e documentação completa na forma de páginas de manual do Unix.

3.3. Sistema de arquivos de *cluster* Proxmox (PMXCFS)

O Proxmox VE usa o *Proxmox Cluster File System* (PMXCFS), um sistema de arquivos baseado em banco de dados que permite sincronizar arquivos de configuração em seu *cluster*. Ao usar o sistema Corosync, esses arquivos são replicados em tempo real para todos os nós do agrupamento. O sistema de arquivos armazena todos os dados dentro de um banco de dados persistente em disco; no entanto, uma cópia desses dados reside na RAM. O tamanho máximo de armazenamento atualmente é de 30 MB – mais que suficiente para armazenar a configuração de vários milhares de máquinas virtuais.

3.4. Migração ao vivo/online

Com o recurso integrado de migração ao vivo/online, é possível mover máquinas virtuais em execução de um nó do *cluster* Proxmox VE para outro sem qualquer tempo de inatividade ou efeito perceptível por parte do usuário final.

Os administradores podem iniciar esse processo pela interface da *web* ou pela linha de comando, o que permite minimizar o tempo de inatividade caso seja necessário colocar o sistema *host* inativo para manutenção.

3.5. Administração baseada em funções

O acesso é granular a todos os objetos (como máquinas virtuais, armazenamento, nós, etc.) usando o sistema de gerenciamento de permissões baseado em função. Isso permite definir privilégios e ajuda a controlar o acesso aos objetos. Esse conceito também é conhecido como listas de controle de acesso: cada permissão especifica um assunto (um grupo de usuários ou *token* de API) e uma função (conjunto de privilégios) em um caminho específico.

3.6. *Cluster* de alta disponibilidade (HA) Proxmox VE

Um *cluster* Proxmox VE de vários nós permite a criação de servidores virtuais altamente disponíveis. O Proxmox VE HA *Cluster* é baseado em tecnologias Linux de alta disponibilidade comprovada, fornecendo um serviço estável e confiável. Todo o *cluster* Proxmox VE HA pode ser facilmente configurado a partir da interface de usuário integrada baseada na *web*.

O Proxmox também oferece uma solução empresarial para *backup* e restauração de máquinas, contêineres e *hosts* físicos. O Proxmox Backup Server não só garante mais segurança de dados, com criptografia forte e métodos de garantia de integridade, como também economiza espaço de armazenamento nos servidores físicos.

3.7. Redes em ponte (*bridge*)

O Proxmox usa um modelo de rede em ponte também chamado de *bridge*. Cada *host* pode ter até 4.094 pontes. Essas interfaces são como *switches* de rede física, implementados em *software* no *host* Proxmox. Todas as máquinas podem compartilhar uma ponte, como se os cabos de rede virtuais de cada convidado estivessem todos conectados ao mesmo *switch*. Para conectar máquinas virtuais (VMs) ao mundo externo, elas são anexadas a placas de rede físicas atribuídas a uma configuração TCP/IP.

Para maior flexibilidade, são possíveis VLANs (IEEE 802.1q) e ligação/agregação de rede. Dessa forma, é possível construir redes virtuais complexas e flexíveis para os *hosts* virtualizados, aproveitando todo o poder da pilha de rede Linux.

O Proxmox também suporta Open vSwitch (OVS) como alternativa às pontes, ligações e interfaces VLAN do Linux. O OVS fornece recursos avançados, como suporte RSTP, VXLANs e OpenFlow, e suporta múltiplas VLANs em uma única conexão.

3.8. Benefícios

Considerando as características descritas anteriormente, o Proxmox apresenta o melhor custo-benefício para virtualizar tanto a infraestrutura de TI quanto as infraestruturas operativas, uma vez que otimiza os recursos existentes e aumenta a eficiência com despesas mínimas.

Nesse sentido, ele oferece gerenciamento descomplicado e interface simples, que reduz a quantidade de horas de trabalho e, ao mesmo tempo, garante segurança na operação e em *backups*.

4. Emprego Operacional

A utilização do Proxmox mudou o paradigma das soluções utilizadas no ambiente das operações cibernéticas. Utilizando somente essa ferramenta para a virtualização de sistemas, foi possível criar uma padronização na operacionalização dos diversos artefatos e cenários componentes das várias necessidades operativas dentro do ambiente computacional.

4.1. Operação Baluarte

Dentro dessa operação, uma série de configurações de ativos se faz necessária, abrangendo desde a criação de estações de trabalho operacionais até sistemas de roteamento diferenciados, destinados a auxiliar os operadores cibernéticos na condução de suas missões conforme estabelecido no contexto da atividade.

Em operações anteriores, essas configurações eram realizadas em vários hipervisores, demandando um tempo considerável para reunir as diversas características necessárias em diferentes ambientes. Isso acarretava atrasos para a equipe de desenvolvedores do Laboratório, uma vez que algumas configurações poderiam estar ausentes ou desatualizadas, o que resultava em retrabalho e atrasos na implantação das estruturas essenciais do exercício. Graças à facilidade de manutenção do Proxmox e à familiaridade dos desenvolvedores com essa solução devido à sua padronização, esse tempo foi reduzido quase a zero.

4.2. Operação Ciber Securitas

Operação criada para ser um ambiente virtualizado a ser utilizado na instrução de militares de diversas Organizações Militares no contexto da Segurança e da Defesa Cibernética. As edições de 2020 e 2021 do evento utilizaram o paradigma do Proxmox na criação do exercício.

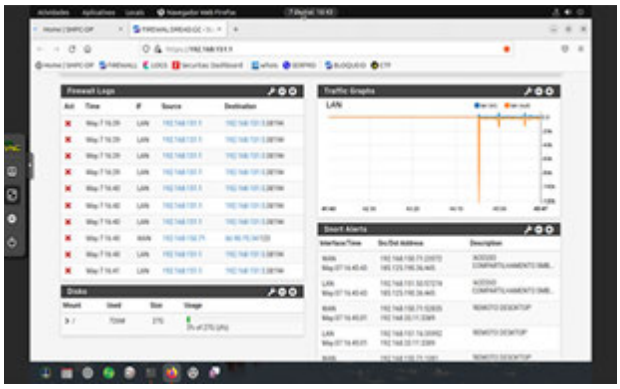
Figura 3: Desenvolvedores do ambiente virtual com o Proxmox.

Fonte: Defesa em Foco, 2021.

No ano de 2023, o ambiente virtualizado pelo Proxmox proposto pelo Laboratório de Ações Cibernéticas do CoNavOpEsp contou com mais de 3800 instâncias virtuais, nas quais os militares puderam se capacitar não somente em *hardening* de servidores, mas também na operação do Sistema Militar de Proteção Cibernética (SMPC – conhecido como *Dreadnought*) via seus módulos (Firewall, IDS, Zabbix, web), na análise de tráfego de rede e em outros aspectos relevantes da Segurança de Informações e Comunicações.

Nesse ambiente, os militares puderam participar de uma competição de *Capture-the-Flag* (CTF) na qual foram submetidos a desafios separados por temas, com várias ações ofensivas via simuladores de tráfego. Os participantes deveriam identificar e bloquear diversos incidentes computacionais e ataques cibernéticos simulados, defendendo, assim, a rede de interesse do exercício. Todos esses eventos puderam ser criados graças às estruturas de desenvolvimento e compartimentação existentes no virtualizador.

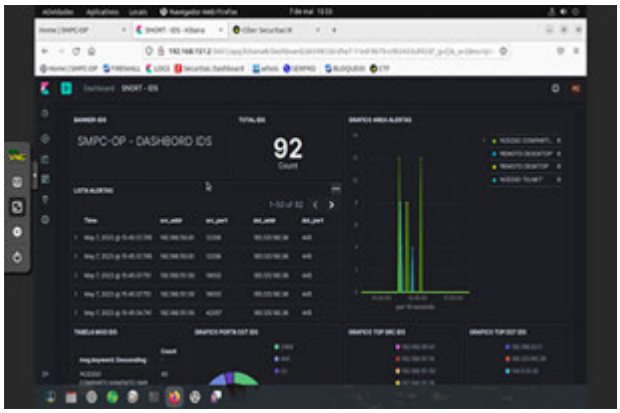
Figura 4: Tela de operação do SMPC virtualizada no Proxmox.



Fonte: O autor.

Esses são apenas alguns exemplos notáveis das aplicações que podem ser efetuadas com a adoção dessa interface de virtualização.

Figura 5: Tela de Operação do SMPC virtualizada no Proxmox.



Fonte: O autor.

Conclusão

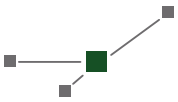
Partindo da premissa estabelecida no início deste artigo, a robustez e a segurança são imperativas tanto para os sistemas cibernéticos navais quanto para qualquer outro sistema. No ambiente operacional, essa necessidade se torna ainda mais premente, pois essas soluções serão submetidas a cargas máximas, podendo ser utilizadas para a execução de ações no contexto da Defesa Naval de ativos, na instrução de militares em relação a novas tecnologias essenciais ou na formulação de novas doutrinas e técnicas para o gerenciamento de questões militares.

Como componente fundamental do Sistema Naval de Guerra Cibernética, o CoNavOpEsp está equipado com um sistema de vanguarda e faz uso eficaz dos recursos

computacionais. O novo paradigma introduzido pela adoção do Proxmox não fica aquém de outros sistemas comerciais que têm a mesma abordagem. Somando-se a isso, a presença de desenvolvedores e operadores competentes aptos a administrar e manter a ferramenta de maneira eficaz abre portas para diversas possibilidades, permitindo a criação e o aprimoramento contínuo dentro desse ambiente.

À medida que a Era da Informação desponta, a convergência de recursos humanos, *hardware* e *software* cria um ambiente propício para o desenvolvimento das capacidades não apenas da Marinha do Brasil, mas também, em um contexto mais amplo, da sociedade como um todo. O Proxmox contribui nesse cenário e incorpora as melhores práticas tanto na virtualização quanto na criação de um modelo integrado de pessoal, programa e máquina, o que pode resultar em inúmeros benefícios no presente e no futuro, facilitando significativamente a integração de sistemas, práticas, técnicas e paradigmas utilizados pelo Poder Naval Operacional.

É esse o caminho que buscamos e almejamos para aprimorar ainda mais o sucesso de nossa Força diante dos desafios que surgem com o advento e o avanço das novas tecnologias.



Referências Bibliográficas

4SYSOPS. **Snapshots in Proxmox VE**. By Surender Kumar. 25 jan. 2023. Disponível em: <https://4sysops.com/archives/snapshots-in-proxmox-ve/>. Acesso em: 09 set. 2023.

BRASIL. Marinha do Brasil. Estado-Maior da Armada. **Doutrina Cibernética da Marinha (EMA 419)**. Brasília, DF: EMA, 2021.

_____._____._____. **Plano Estratégico da Marinha (PEM 2040).** Brasília-DF: EMA, 2020. Disponível em: <https://www.marinha.mil.br/sites/all/modules/pub_pem_2040/book.html>. Acesso em: 07 mar. 2024.

_____. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **MD31-M-07: Doutrina Militar de Defesa Cibernética**. Brasília, DF: EMCFA, 2014.

CLOSS, T. A. **Virtualização em ambiente corporativo com ferramentas de *open source***. Trabalho de Conclusão de Curso (monografia). Bacharelado em Engenharia de Computação. Instituto Federal de Educação, Ciência e Tecnologia, Cuiabá, Mato Grosso, 2021.

DEFESA EM FOCO. **CoNavOpEsp realiza Operação "Ciber Securitas VIII"**. Por Marcelo Barros. 30 out. 2021. Disponível em: <https://www.defesaemfoco.com.br/conavopesp-realiza-operacao-ciber-securitas-viii/>. Acesso em: 09 set. 2023.

LAUREANO, M. A. P.; MAZIERO, C. Virtualização: conceitos e aplicações em segurança. In: **Minicursos do Simpósio Brasileiro de Segurança da Informação e Sistemas** (SBSeg). Sociedade Brasileira de Computação, 2008. p. 151-200. Disponível em: <https://www.researchgate.net/publication/237681120_Virtualizacao_Conceitos_e_Aplicacoes_em_Seguranca>. Acesso em: 09 set. 2023.

MOTA JUNIOR, S.; MARTINS, N.L. Sistema *Dreadnought* na Vanguarda da Proteção Cibernética Operativa. In: **Revista Passadiço**, ano 35, ed. 42, 2022. Marinha do Brasil. Centro de Adestramento Almirante Marques de Leão. Niterói, Rio de Janeiro. Disponível em: <https://www.marinha.mil.br/caaml/sites/www.marinha.mil.br.caaml/files/flipping_book/passadio_digital_2022_0/index.html#p=52>. Acesso em: 09 set 2023.

PROXMOX SERVER SOLUTIONS GMBH. **Proxmox Virtual Environment – Features**. Disponível em: <https://www.proxmox.com/en/proxmox-virtual-environment/features>. Acesso em: 09 set. 2023.

TRUENET. Blog. **Tipos de virtualização**. Disponível em: <https://blog.truenet.pt/tipos-de-virtualizacao/>. Acesso em: 04 fev. 2024.