UNIVERSIDADE
EDUARDO
MONDLANE

Faculdade de Engenharia

Departamento de Engenharia Electrotécnica

Curso de Engenharia Informática

RELATÓRIO DE ESTÁGIO PROFISSIONAL

Instalação de um sistema de backups na infra-estrutura da fábrica da HEINEKEN Moçambique, em Bobole.

Autor:

Castigo Hermenegildo Dramuce

Supervisores:

Eng. Cristiliano Maculuve (UEM) Sete Matimele (HEINEKEN)

Maputo, Janeiro de 2024

UNIVERSIDADE
EDUARDO
MONDLANE

Faculdade de Engenharia

Departamento de Engenharia Electrotécnica

Curso de Engenharia Informática

RELATÓRIO DE ESTÁGIO PROFISSIONAL

Instalação de um sistema de backups na infra-estrutura da fábrica da HEINEKEN Moçambique, em Bobole.

Autor:

Castigo Hermenegildo Dramuce

Supervisores:

Eng. Cristiliano Maculuve (UEM) Sete Matimele (HEINEKEN)

Maputo, Janeiro de 2024

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

Curso de Engenharia Informática

Instalação de um sistema de backups na infra-estrutura da fábrica da HEINEKEN Moçambique, em Bobole.

CASTIGO HERMENEGILDO DRAMUCE

Relatório a ser apresentado ao Departamento de Engenharia Electrotécnica, Faculdade de Engenharia da Universidade Eduardo Mondlane – UEM como requisito para a realização da disciplina Estágio Profissional. Supervisor: Cristiliano Maculuve e a Directora do Curso: Eng.ª Ivone Cipriano

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE ENGENHARIA

Curso de Engenharia Electrónica

TERMO DE ENTREGA DE RELATÓRIO DO ESTÁGIO PROFISSIONAL

Declaro que o estudante Castigo Hermenegildo Dramuce entregou no dia ____ / ____ / 2024 as ____ cópias do relatório do seu Estágio Profissional, com a referência: _____ intitulado: Instalação de um sistema de backups na infra-estrutura da fábrica da HEINEKEN Moçambique, em Bobole.

Maputo, _____ de Janeiro de 2024

O (a) Chefe de Secretaria

_____

Agradecimentos

Todo o progresso conseguido não seria possível sem a ajuda de meus pais, que fizeram de tudo para que eu sempre estivesse focado no objectivo ao qual eu me submeti, que é a realização do curso.

A todos aqueles que de alguma forma estiveram e estão próximos de mim, fazendo a minha vida valer cada vez mais a pena.

Aos meus amigos e ex-colegas de carteira Aiton Cumbi, Valério Macumbuia, André Comé, Júlio Langa, e Frederico Muianga pelo incentivo e grande ajuda com o fornecimento de material para a realização deste trabalho, pela ajuda, no tempo da realização das cadeiras do curso, com material didáctico e explicações que me puderam dar e os pude dar.

Também aos professores que me deram as lições didácticas tanto como morais que tenho usado como ferramentas no meu dia-a-dia.
Ao meu supervisor de estágio pelo tempo que pôde reservar para me auxiliar na elaboração do presente relatório

Ao pessoal da HEINEKEN Moçambique, por toda ajuda que me foi dada durante o percurso do meu estágio. Pela boa recepção, os elogios, e por terem feito eu me sentir à vontade e confiante nas actividades desempenhadas durante o estágio.
Ao meu supervisor Sete Matimele por desempenhar um papel fundamental ao orientar-me na compreensão da importância crítica da infra-estrutura informática para os negócios contemporâneos. Seu conhecimento e experiência foram inestimáveis para o meu desenvolvimento profissional.

À todos estes meu muito obrigado.

Resumo

O relatório relata o processo da implementação de um sistema de backups na fábrica da HEINEKEN Moçambique em Bobole. O relatório aborda sobre conceitos sobre o tópico em torno de backups, nomeadamente os tipos de backup, o processo de restauração e a importância dos mesmos. Ao longo do relatório, serão detalhados os desafios específicos associados à ausência de sistemas de backup na infra-estrutura e os passos seguidos para a resolução do mesmo. Além disso são analisadas propostas para a implementação de sistemas de backups robustos na qual pudesse servir como ponto de partida no caso de algum desastre ou falha humana. Por fim é detalhado o processo de comissionamento do sistema de backups na empresa e os testes de backups e restauração feitos após a implementação.

Palavras-chave: PCD, Backups, Infra-estrutura, Virtualização

Abstract

The report describes the process of implementing a backup system at the HEINEKEN Mozambique brewery in Bobole. The report covers concepts on the topic of backups, namely the types of backup, the restoration process and their importance. Throughout the report, the specific challenges associated with the absence of backup systems in the infrastructure and the steps taken to resolve them are detailed. Proposals for the implementation of robust backup systems that could serve as a starting point in the event of a disaster or human failure are also analyzed. Finally, the process of commissioning a backup system in the company and the backup and restoration tests carried out after the implementation are also detailed.

Key words: PCD, Backups, Infrastructure, Virtualization

Índice

Lista de siglas

PCD – Process Control Domain

D&T – Digital & Technology

SCCM – System Center Configuration Manager

AMEE – Africa, Middle East & Europe

PXE – Pre-boot Execution Environment

OpCo – Operational Company

AD – Active Directory

SAS – Serial Attached SCSI

SCSI – Small Computer System Interface

HBA – Host Bus Adapter

AP – Access Point

VM – Virtual Machine

DNS – Domain Name System

DHCP – Dynamic Host Configuration Protocol

IP – Internet Protocol

SSID – Service Set Identifier

DDI – DNS, DHCP, and IPAM

BMC – Baseboard Management Controller

TB – Terabyte

GB – Gigabyte

HDD – Hard Disk Drive

SSD – Solid State Drive

SSH – Secure Shell

TI – Tecnologias de Informação

DR – Disaster Recovery

ISP – Internet Service Provider

PLC – Programmable Logic Controller

SD-WAN – Software-Defined WAN

VLAN – Virtual Local Area Network

RAID – Redundant Array of Inexpensive Drives

ISO – Optical Disc Image

KVM – Kernel-based Virtual Machine

Lista de figuras

Lista de tabelas

1. CAPÍTULO I – INTRODUÇÃO

No cenário empresarial actual, a infra-estrutura informática desempenha um papel vital, impulsionando o sucesso e a eficiência das organizações. O presente relatório é uma exploração abrangente da minha experiência de estágio na HEINEKEN Moçambique, uma empresa pertencente ao grupo Heineken Holding NV que opera principalmente na indústria de cervejas, bem com de outras bebidas, onde tive a oportunidade de testemunhar em primeira mão como uma infra-estrutura informática sólida sustenta e impulsiona as operações de negócios.

Durante o estágio na HEINEKEN Moçambique, tive o privilégio de mergulhar profundamente na gestão da infra-estrutura informática da organização. Esta empresa, que no nosso país somente opera no sector de produção de cerveja e também na venda de bebidas alcoólicas e não-alcoólicas, destaca-se pelo seu compromisso com a excelência em na sua área de actuação e também pela presença em alguns projectos de responsabilidade social.

Nesse período de estágio não deixou de ser notável a infra-estrutura informática que contém equipamentos de alta robustez e performance. Isso inclui sistemas de servidores, redes e aplicações que suportam o negócio. A empresa investe continuamente em tecnologia avançada para melhorar sua eficiência operacional para atender às demandas das operações e do mercado, de forma a manter-se à frente das empresas concorrentes.

O relatório não apenas destaca a minha jornada de estágio na HEINEKEN Moçambique, mas também ilustra a relevância da infra-estrutura informática em sustentar o sucesso organizacional, bem como ressalta a importância de um sistema robusto de Backups.

1.1 Contextualização

Neste relatório, além de detalhar minha experiência e contribuições gerais durante o estágio, também apresentarei uma descrição aprofundada da infra-estrutura informática da empresa, o que irá incluir uma visão geral das principais tecnologias e sistemas em uso, dando mais foco para o ambiente *Process Control Domain* (PCD), o que será explicado ao detalhe ao longo do trabalho.

Pouco antes do início do estágio houve ocorreu um incidente onde o servidor virtual onde estava instalada a aplicação Brewmaxx parou repentinamente. Esta aplicação é muito crítica pois é responsável pela gestão de produção, gestão de estoque, controlo de qualidade, entre outras usadas na produção da cerveja. Com esta situação, houve paragem da produção e foram reunidos esforços para instalar mesma aplicação em um outro servidor físico.

1.2 Problema

Com a situação descrita acima, a empresa viu a necessidade da instalação de um sistema de backups que permita salvaguardar os dados e informações de a poder restaurar os sistemas após uma falha. A empresa enfrenta o desafio de não possuir um mecanismo de backup eficaz para proteger e recuperar os dados e informações, o que em algum momento poderá causar paragem de produção no caso de uma falha pois a ausência de sistemas de backups robustos na infra-estrutura coloca a empresa em risco de perda irreparável de dados, o que poderia ter sérias repercussões para a continuidade dos negócios. Com base nestes acontecimentos surge então a questão: Como garantir que no futuro haja um tempo de paragem menor no caso situação descrita anteriormente voltar a acontecer?

1.3 Justificativa

O problema se manifesta na necessidade urgente de implementar soluções de backup robustas na infra-estrutura. A motivação da escolha do tema foi o facto da não existência do sistema de backups na infra-estrutura o que constitui uma não-conformidade com os controlos de informática em vigor na empresa.

Outra razão que foi levada em conta é o facto de que a solução trará vários benefícios para a empresa no caso desta passar por um incidente similar ao descrito anteriormente.

Para além disso é de grande interesse do autor que o trabalho possa de alguma forma agregar de forma positiva ao leitor com informações de boas práticas usadas nas infra-estruturas de TI em ambientes corporativos.

1.4 Objectivos

1.4.1. Geral

- Instalar um sistema de backups na infra-estrutura da fábrica da HEINEKEN Moçambique, em Bobole;

1.4.2. Específicos

- Descrever a situação actual da infra-estrutura de virtualização do ambiente de produção da HEINEKEN Moçambique;
- Analisar as diferentes propostas de solução para a existência e operacionalização de um sistema de backups;
- Implementar a melhor proposta tendo em conta a robustez e viabilidade da solução;

1.5 Metodologia

Como forma de responder à pergunta de pesquisa, foi usada uma abordagem qualitativa para a análise dos dados, como forma de aprofundar os conceitos fundamentais necessários para compreender o tema em causa, o que consistiu em pesquisas exaustivas na internet, fazendo uso de ferramentas como Google Académico, Google Books, Academia.Edu, entre outras, com vista a e ir ao encontro e trazer tópicos apresentados no trabalho.

Para a colecta dos dados o autor utilizou técnicas de observação directa intensiva onde foram realizadas sessões de análise dos instrumentos existentes para a execução do trabalho, o que resultou na elaboração e apresentação de desenhos ilustrativos e explicativos das fases da implementação.

Quanto aos objectivos foi realizado um estudo de pesquisa exploratório, visto que o autor realizou uma pesquisa abrangente para maior familiarização com o tema de infra-estruturas de TI e soluções de backup, a fim de compreender as melhores práticas usadas e também para escolha da solução final.

1.6 Estrutura do Trabalho

O presente relatório está organizado da seguinte forma:

- **Capítulo 1 – Introdução**

  Neste capítulo, é dada uma abordagem introdutória sobre o trabalho, dando a conhecer o problema, a justificativa, a metodologia, os objectivos gerais e específicos do trabalho;

- **Capítulo 2 – Revisão de literatura**

  Neste capítulo, é fornecida a informação necessária para que seja possível compreender os conceitos relacionados aos backups, infra-estruturas informáticas e os demais elementos que a compõem, como também é feita a explicação de alguns componentes usados na infra-estrutura de empresa;

- **Capítulo 3 – Descrição das actividades desenvolvidas**

  Neste capítulo, são apresentadas as actividades que foram desempenhas durante o período de estágio. É também apresentada de forma breve a informação do departamento em que fui acolhido;

- **Capítulo 4 – Caso de estudo**

  Neste capítulo é apresentada a situação actual da infra-estrutura de TI da empresa, onde são descritos os dispositivos que lá existem e fazem parte do escopo do trabalho, e é também descrito ao detalhe a forma como está estrutura da rede da infra-estrutura. Por fim é apresentado o problema que existe na actual infra-estrutura;

- **Capítulo 5 – Proposta de solução**

  Neste capítulo são apresentadas as possíveis soluções para o problema, é descrita a solução escolhida e os critérios a usados na escolha. De seguida é descrito o processo de implementação da solução escolhida. São também partilhados os desafios encontrados e as lições aprendidas nesse processo. Por fim é feita uma apresentação dos resultados obtidos com a implementação.

- **Capítulo 6 – Conclusões e recomendações**

  Neste capítulo, são apresentadas as conclusões obtidas com a realização do trabalho, e será detalhado o aprendizado tido ao longo da realização do projecto e o que se pode ter em conta como melhoria para na infra-estrutura.

1.7 Apresentação da Empresa

A Heineken, em Moçambique iniciou as suas actividades em 2016, com o nome "Heineken Vendas e Distribuição" (HVD), somente na componente de vendas e distribuição de produtos, com um escritório de vendas e promoções, e importando cervejas como Heineken, Amstel, Amstel Lite e Sagres, de forma a alargar a gama de produtos disponíveis aos consumidores moçambicanos.

A Heineken Moçambique (HM) teve a sua criação com a abertura da fábrica que está localizada em Bobole, no distrito de Marracuene, província de Maputo. Foi inaugurada pelo Presidente da República, a sua excelência Filipe Jacinto Nyusi, a 13 de Março de 2019. O empreendimento foi erguido num espaço de 113 hectares que comportaram todos os compartimentos importantes nas diferentes fases de produção, incluindo área social e de serviços de assistência médica com uma capacidade de produção de 800 mil hectolitros por ano. A Heineken Moçambique, tem a sua sede Avenida da Marginal, n.º 141, 2.º andar, em Maputo.

A HEINEKEN Moçambique faz parte de um grupo de empresas HEINEKEN no mundo, denominadas *Operational Company* (OpCo). Cada planta da HEINEKEN existente em um país, corresponde a uma OpCo, sendo que em Moçambique existe, somente uma (1) planta da HEINEKEN, o país contém somente uma OpCo que é denominada "***MZ1 OpCo***".

1.7.1. Missão

Ser reconhecida como a empresa que coloca clientes e consumidores em primeiro lugar, fornecendo apenas marcas da mais alta qualidade, sempre e em qualquer lugar, com pessoas felizes e engajadas

1.7.2. Visão

Preparar a alegria da união, fornecendo as melhores cervejas e sidras aos consumidores, colocando-os sempre a frente.

1.7.3. Princípios

- Colocar a segurança em primeiro lugar
- Cuidar das pessoas e do planeta
- Agir com integridade e transparência

2. CAPÍTULO II – REVISÃO DA LITERATURA

Nesta secção, serão abordados conceitos relacionados aos servidores, redes e backups. Para além disso, como forma de providenciar um melhor entendimento do trabalho são apresentadas definições de algumas ferramentas que são usadas no ambiente da empresa.

2.1. Virtualização de servidores

Virtualização é a criação de uma abstracção de algo que existe fisicamente, como por exemplo, um sistema operativo, um servidor, dispositivos de alojamento ou dispositivos de rede, etc. A virtualização de um servidor muda as regras do modelo tradicional de funcionamento do sistema físico, em que um servidor físico faz o papel de servidor hospedeiro, onde está instalado um *hypervisor* e onde são instaladas várias máquinas virtuais. Neste contexto, a virtualização é um método de executar vários sistemas operativos virtuais independentes num único computador físico. Esta abordagem maximiza o retorno do investimento no servidor. (Brandão, 2018)

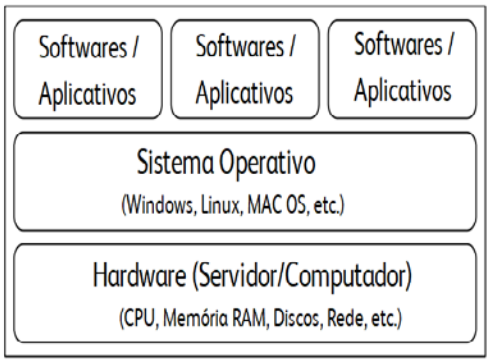


Figura 1: Arquitectura de sistema tradicional.
Fonte: (McCrory, Reynolds , & Marshall , 2006)

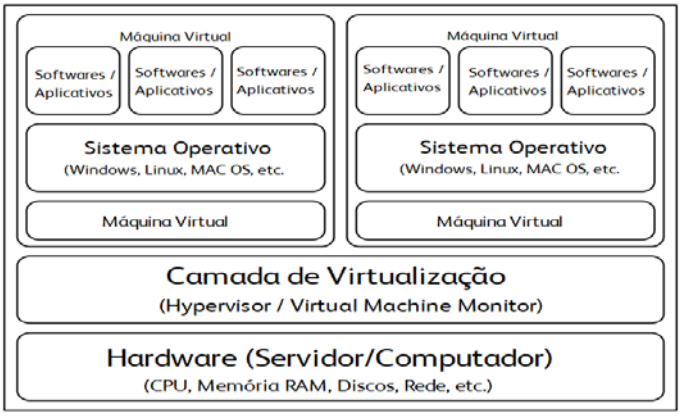


Figura 2: Arquitectura de sistemas virtualizados.
Fonte: (McCrory, Reynolds , & Marshall , 2006)

Por outras palavras, a virtualização pode ser representada como o processo de implementação de um conjunto de tecnologias capazes de camuflar as características físicas dos recursos dos servidores, recursos de redes, e recursos de alojamento, da forma como habitualmente os sistemas, aplicações ou utilizadores finais interagem com esses referidos recursos, e uma máquina virtual é um ambiente de execução

único e isolado criado através de software pela camada de virtualização (hypervisor) (McCrory, Reynolds , & Marshall , 2006). A ilustração destes conceitos pode ser vista nas figuras 1 e 2 acima.

2.2. Hypervisors

Na figura 2 podemos ver a segunda camada (baixo para cima) de nome “Camada de Virtualização” onde é encontrado o *Hypervisor* ou Monitor de Máquina Virtual (*Virtual Machine Monitor* – VMM) cuja tarefa principal é abstrair os recursos reais do computador e fornecer os ambientes virtuais nos quais os sistemas operativos podem ser instalados. Dependendo da plataforma de virtualização plataforma de virtualização, o software da camada de virtualização pode ser instalado directamente no computador ou pode ser instalado num sistema operativo existente que resida no hardware do computador. (McCrory, Reynolds , & Marshall , 2006)

Os hypervisors desempenham um papel fundamental na execução de máquinas virtuais (*Virtual Machines* – VM) e na alocação de recursos de hardware, permitindo que múltiplos sistemas operacionais funcionem de forma independente em um único servidor físico. Estes são classificados em duas categorias principais vistas a seguir:

1. **Hypervisors do tipo 1 (também chamados Bare-Metal)** – Este tipo, que será o foco do presente trabalho, é instalado directamente no hardware físico do servidor e não requer um sistema operativo hospedeiro. Estes oferecem alto desempenho e eficiência, sendo ideais para ambientes de produção. A arquitectura quando o hypervisor é do tipo 1 é o visto na figura 2.
2. **Hypervisors do tipo 2 (também chamados Hosted)**: Esses hypervisors são instalados como aplicativos em sistemas operativos hospedeiros. Estes são mais adequados para ambientes de aprendizado, desenvolvimento e teste. A arquitectura quando o hypervisor é do tipo 2 é o visto na figura 3 abaixo.

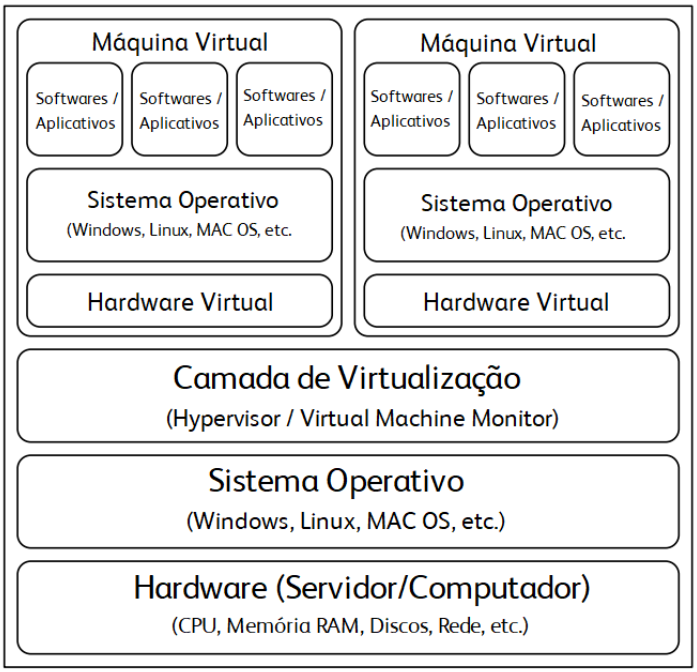


Figura 3: Virtualização com hypervisor do tipo 2. Fonte: (McCrory, Reynolds , & Marshall , 2006)

2.2.1. Vantagens do uso dos hypervisors

Para além de garantir o retorno no investimento, previamente mencionado, o uso dos hypervisors na virtualização apresentam outras vantagens que são descritas abaixo:

- **Abstracção de hardware**: Os hypervisors abstraem os recursos de hardware, permitindo que as máquinas virtuais sejam executadas em diferentes tipos de servidores físicos sem modificação, proporcionando flexibilidade e portabilidade;
- **Isolamento de recursos:** os hypervisors garantem que cada VM tenha seus próprios recursos isolados, como CPU, memória e armazenamento, proporcionando segurança e desempenho;
- **Migração de máquinas virtuais entre servidores**: hypervisors de nível empresarial (geralmente do tipo 1) como o VMware e Hyper-V por exemplo, suportam a migração de máquinas virtuais usando as tecnologias vMotion e *Live Migration* respectivamente, permitindo a movimentação das máquinas virtuais entre servidores (físicos) sem interrupções;
- **Clusterização (cluster) e alta disponibilidade (high availability)**: as plataformas de virtualização, como por exemplo as duas mencionadas no

ponto anterior, oferecem recursos avançados para criar e gerir *clusters* e garantir a alta disponibilidade das máquinas virtuais;

- **Recuperação de desastres**: plataformas de virtualização geralmente incluem funcionalidades de *snapshot*, replicação e backup, facilitando a implementação de soluções robustas de recuperação de desastres para as máquinas virtuais.

2.2.2. Exemplos de hypervisor do tipo 1 mais conhecidos

Existem vários hypervisors do tipo 1 actualmente, cada um com a suas vantagens e benefícios. Para o presente trabalho serão tragos três que são amplamente conhecidos, o Kernel-based Virtual Machine (KVM), Microsoft Hyper-V e o VMware ESXi.

Kernel-based Virtual Machine (KVM)

O KVM é uma solução de virtualização completa para Linux em hardware x86 contendo extensões de virtualização (Intel VT ou AMD-V). Ele consiste em um módulo de kernel carregável que fornece a infra-estrutura de virtualização central e um módulo específico do processador. (KVM)

O KVM é um software de código aberto. O componente do kernel do KVM está incluído na linha principal do Linux, a partir da versão 2.6.20. O componente de *userspace* do KVM está incluso na linha principal do QEMU (Emulador de Máquina), a partir da versão 1.3. (KVM, 2023)

Usando o KVM, é possível executar várias máquinas virtuais executando imagens não modificadas do Linux ou do Windows. Cada máquina virtual tem hardware virtualizado privado: uma placa de rede, disco, adaptador gráfico, etc. Embora o KVM seja executado num sistema operativo Linux, ele é considerado um hypervisor tipo 1 por fornecer acesso directo aos recursos de hardware.

Pelo facto do KVM estar disponível em quase todas as distribuições do Linux, não existe um ISO específico ou aplicação para fazer descarregar e instalar, pois isso é feito manualmente instalando os módulos KVM, na distribuição de Linux que estiver instalada.

VMware ESXi

O VMware ESXi é um hipervisor *bare-metal* que se instala directamente no servidor físico. Com acesso directo e controlo dos recursos subjacentes, o VMware ESXi particiona eficazmente o hardware para consolidar aplicações e reduzir custos. (VMWARE)

A arquitectura do VMware ESXi inclui o sistema operativo subjacente, denominado VMkernel, e os processos que são executados sobre o mesmo. O VMkernel fornece meios para executar todos os processos no sistema, incluindo aplicações e agentes de gestão, bem como máquinas virtuais. Tem o controlo de todos os dispositivos de hardware no servidor e gere os recursos para as aplicações. (Chaubal, 2008)

Os principais processos que são executados sobre o VMkernel são:

- Direct Console User Interface (DCUI) – a interface de configuração e gestão de baixo nível, acessível através da consola do servidor, utilizada principalmente para a configuração básica inicial;
- Virtual Machine Monitor (VMM) – que é o processo que fornece o ambiente de execução para uma máquina virtual, bem como um processo auxiliar conhecido como VMX. Cada máquina virtual em execução tem o seu próprio processo VMM e VMX.;
- Agentes – usados para permitir o gerenciamento de alto nível da infra-estrutura VMware a partir de aplicativos remotos.

Microsoft Hyper-V

O Microsoft Hyper-V é um sistema baseado em hypervisor de tipo 1 para arquitecturas de sistema operativo x86-64. O Hyper-V tornou-se parte integrante das edições Enterprise, Education e Pro. É activado no sistema operativo Windows como um “role”, tal como vários outros serviços da família Microsoft. (Đorđević, Jovičić, Kraljević, & Timčenko, 2022)

Existem algumas funcionalidades do Hyper-V que funcionam de forma diferente no sistema operativo Windows (desktop) e no Windows Server. O modelo de gestão da memória é diferente para o MS Hyper-V, em que o MS Hyper-V gere a memória no

servidor assumindo que apenas as máquinas virtuais são executadas no servidor e, no sistema operativo Windows (desktop), é gerido com a expectativa de que a maioria das máquinas clientes executa software no host para além das máquinas virtuais

Tabela comparativa entre o KVM, Hyper-V e VMware ESXi

Recurso	**KVM**	**VMware ESXi**	**Hyper-V**
Baseado em	Linux KVM	VMkernel	Windows
Tipo de produto	Código aberto	Proprietário	Proprietário
Gestão centralizada	Incorporado	Suportado com licença paga	Suportado
Alta disponibilidade	Suportado	Suportado	Suportado
Live Migration	Suportado	Disponível com licença paga	Suportado
Migração/Conversão	Possível com ferramentas de terceiros	Possível com ferramentas nativas e de terceiros	Possível com ferramentas nativas e de terceiros
Cópia de segurança e restauro	Suportado	Suportado	Suportado
Licenciamento	Grátis	Gratuito (limitado) & Pago (todas as funcionalidades)	Gratuito/incluso na licença do Windows
Opções de gestão remota	Cliente Web e CLI	Cliente Web, CLI, PowerCLI, vCenter Server	Hyper-V Manager, PowerShell, System Center VMM
Max. RAM/Host	12TB	12 TB	24TB
Max. RAM/VM	6 TB	6 TB	12 TB
Max. CPUs/VM	240	128	240
Max. Disco VM	10TB	62TB	64 TB
Hot plug de recursos virtuais	Sim	Sim	Sim

Tabela 1: Tabela comparativa entre o KVM, Hyper-V e VMware ESXi. Fonte: (Gupta, 2018)

2.3. Baseboard Management Controller (BMC)

Baseboard Management Controller é um microcontrolador ou processador dedicado que está integrado na placa-mãe de um servidor, que permite o controlo remoto, a gestão e a monitorização do hardware, mesmo quando o sistema/servidor está desligado. (Lavoie, 2023)

Permite que os administradores de sistemas possam executar tarefas remotamente, como configuração da BIOS, actualizações de firmware, monitorizar sensores críticos, como a temperatura e a velocidade das ventoinhas, entre outros.

Pode também oferecer alertas para que, se algum dos sensores estiver fora dos limites especificados ou se houver uma falha de hardware, o administrador possa ser imediatamente notificado, possibilitando que as medidas correctivas possam então ser tomadas de forma atempada.

O BMC fornece vários recursos de grande utilidade para sistemas de servidor, incluindo:

- **Gestão remota**: os administradores podem aceder e fazer a gestão do hardware do servidor remotamente, mesmo que o servidor esteja desligado ou o sistema operativo principal não esteja em execução.
- **Monitorização do estado do sistema**: o BMC monitoriza constantemente o estado do sistema do servidor, incluindo as temperaturas dos componentes, as velocidades das ventoinhas e as fontes de alimentação. Pode alertar os administradores para potenciais problemas antes que estes se tornem críticos e causem tempo de inactividade.
- **Suporte de media virtual**: os administradores podem montar remotamente imagens ISO, imagens de disco e outros tipos de multimédia no servidor como se estivessem fisicamente presentes.
- **Gestão de *power***: os administradores podem ligar, desligar ou reiniciar o servidor remotamente.
- **Segurança**: o BMC fornece uma interface de gestão separada que está isolada do sistema operativo principal. Isto aumenta a segurança do servidor, limitando o acesso às funções críticas de gestão do sistema.

Exemplos de BMC

Dois dos vários exemplos de um BMC são o **Integrated Lights-Out (iLO)** e **Integrated Dell Remote Access Controller (iDRAC)** que são brevemente descritos a seguir

1. A **Integrated Lights-Out (iLO)** é uma tecnologia de gestão proprietária, incorporada nos produtos HPE que permite o acesso de controlo remoto aos servidores da família ProLiant, mesmo sem estarem ligados à rede principal da organização. (Hewlett Packard Enterprise (HPE))
2. A **Integrated Dell Remote Access Controller (iDRAC)** é uma tecnologia concebida para uma gestão segura de servidores locais e remotos e ajuda os administradores de TI a implementar, actualizar e monitorizar os servidores PowerEdge em qualquer lugar e a qualquer momento, que oferece transmissão de telemetria iDRAC9, verificação segura de componentes, gerenciamento de servidor incorporado sem agente. (Dell Technologies)

2.4. Host Bus Adapter (HBA)

Um Host Bus Adapter (HBA) é um adaptador de circuito integrado que liga um sistema anfitrião (host), como um servidor, a um dispositivo de armazenamento ou de rede. Um HBA também fornece processamento de entrada/saída (Input/Output – I/O) para reduzir a carga no microprocessador do host ao armazenar e ler dados, ajudando no geral a melhorar o desempenho do host. (Controle Net)

Figura 4: Diferentes exemplos de HBA. Font (Controle Net)

Conforme ilustra a figura acima, os HBAs podem usar vários tipos de interfaces, como *Fiber Channel*, SCSI, SATA, SAS, e iSCSI, dependendo do tipo da rede e das necessidades de armazenamento.

Os HBAs são geralmente projectados para as interfaces PCIe, pois oferecem velocidades altas, como também são um formato muito comum nos hardwares modernos.

2.5. Active Directory

O Active Directory é o serviço de directório de utilizadores, pertencente a empresa Microsoft, para as organizações gerirem e organizarem os perfis do seu pessoal para efeitos de autenticação, autorização e contabilidade. Este funciona numa estrutura de domínio de rede e, como tal, é necessária uma máquina com o Windows Server 2000 (ou mais recente) para actuar como o controlador de domínio para executar o serviço.

Neste contexto, um domínio pode ser definido como um "subconjunto distinto da Internet com endereços que partilham um sufixo comum ou sob o controlo de uma determinada organização ou indivíduo" (McDonald, Papadopoulos, Ahmad , Pitropakis, & Buchanan, 2022)

O Active Directory oferece vários serviços úteis para gerir a infra-estrutura de TI de uma organização. O principal objectivo do Active Directory é fornecer às organizações medidas de autorização, autenticação e contabilidade às organizações para utilização pelos administradores de sistemas/rede. (McDonald, Papadopoulos, Ahmad , Pitropakis, & Buchanan, 2022)

Os perfis de utilizador são necessários para os utilizadores iniciarem sessão em máquinas ligadas ao domínio. Quando um utilizador tiver iniciado sessão numa máquina através da autenticação, as suas acções serão restringidas com base na autorização e registadas através da contabilidade. A partir destas contas de utilizador, as políticas podem ser aplicadas através de *Group Policy Objects* (GPOs) para vários fins no local de trabalho, tais como atribuição de grupos de utilizadores com base no departamento, atribuição de impressoras ou partilha de ficheiros a esses utilizadores, ou qualquer política que a organização exija. Para muitas organizações, estes serviços são essenciais para as operações.

2.6. System Center Configuration Manager (SCCM)

O System Center Configuration Manager fornece uma solução completa para a gestão de sistemas num ambiente de TI centrado nas pessoas, incluindo a capacidade de catalogar hardware e software, fornecer novos pacotes de software e actualizações e implementar (deployment) sistemas operativos Windows com facilidade. (Meyler, Holt, Oh, & Sandys, 2012)

Fornece gestão da configuração, gestão de patches, distribuição de software e sistemas operativos, controlo remoto, gestão de activos, inventário de hardware e software, integração na nuvem através do Microsoft Intune e uma estrutura de relatórios robusta para dar sentido à variedade de dados disponíveis para sistemas internos, rastreio e requisitos de relatórios regulamentares. (Meyler, Holt, Oh, & Sandys, 2012)

A arquitectura do SCCM é composta por alguns elementos dos quais vale a pena destacar:

1. **Configuration Manager Site** – também designado por “site”, é a função principal do SCCM, que dependendo dos requisitos da organização, a arquitectura pode ser simples, que é composto apenas por um único site primário. Grandes empresas podem necessitar de começar com um site de administração central (Central Adminstration Site – CAS) e possuir pelo menos um site primário. A figura 5 ilustra a hierarquia dos sites no SCCM.

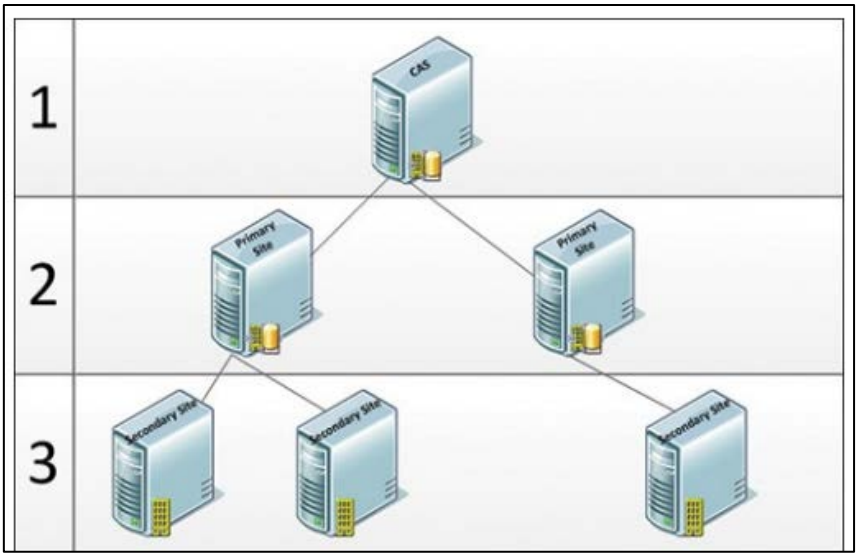


Figura 5: Ilustração da hierarquia dos sites no SCCM

2. **Site Primário** – é um tipo de Configuration Manager Site. Todas as implementações do Configuration Manager requerem pelo menos um site primário. Trata-se de um site ao qual podem ser atribuídos clientes e que pode ser administrado utilizando a consola do Configuration Manager.

   Um site primário quando for standalone, sem um CAS (Central Administration Site), suporta 150.000 desktops/laptops e gere até 250 Sites Secundários.

3. **Site Secundário** – é um tipo de Configuration Manager Site. Suporta até 15.000 desktops/laptops. Estes recebem automaticamente as funcionalidades de ponto de gestão de proxy e de e ponto de distribuição (Distribution Point – DP). Um site secundário é sempre um site filho de um site primário e só pode ser administrado por um site primário. Os sites secundários ajudam a controlar a utilização da largura de banda, gerindo o fluxo de informações do cliente enviadas para a hierarquia. Além disso, os sites secundários podem ser colocados em camadas para ajudar a controlar a distribuição de conteúdo para sites remotos.
4. **Distribution Point (DP)** – é uma função/role que armazena conteúdo e facilita a transferência de conteúdo para dispositivos. Um site pode conter vários DPs para ajudar a compensar um grande volume de transferência de conteúdo para dispositivos ou situar o conteúdo mais perto de um grupo de dispositivos, reduzindo o impacto no tráfego através da WAN. Os DPs são usados para disponibilizar conteúdo aos clientes. Desempenham um papel fundamental na entrega de pacotes (packages), programas, actualizações de software, aplicações, actualizações de software e conteúdo relacionado com OSD (Operating System Deployment – instalação do sistema operativo).

A Microsoft inclui componentes de implementação do sistema operativo (Operating System Deployment – OSD) no SCCM. Esta funcionalidade envolve a entrega de uma implementação em massa de uma nova instância do sistema operativo Windows em dispositivos compatíveis.

É um processo completo que permite definir acções (também chamadas de Task Sequence) antes de a imagem ser aplicada a um sistema. Isto inclui o particionamento e a formatação da unidade ou mesmo actualizações do BIOS e acções após a

aplicação da imagem, como a instalação de actualizações de software ou a implementação de aplicações.

Para instalação dos sistemas operativos usando o SCCM é importante definir o conceito de PXE que desempenha um papel importante no processo de OSD.

Preboot Execution Environment (PXE) – em termos simples, o PXE é um ambiente cliente/servidor padrão que permite que uma máquina inicialize um sistema operacional que é recuperado da rede. O lado do cliente deve ter uma placa de interface de rede (Network Interface Card – NIC) com capacidade de inicialização PXE; o lado do servidor SCCM lida com um processo que intercepta o pacote PXE, lê-o e entrega o sistema operacional ao cliente que o solicitou. (Meyler, Holt, Oh, & Sandys, 2012)

De salientar que o PXE não é um conceito do ConfigMgr ou mesmo da Microsoft; é mais um conceito de toda a indústria implementado em diferentes sabores em uma grande variedade de sistemas operacionais de servidor

2.7. Cópias de Segurança (Backups)

Em um mundo cada vez mais digitalizado, a segurança e a preservação de dados tornaram-se uma prioridade crítica para organizações e indivíduos. O backup de dados é uma prática essencial que desempenha um papel fundamental na protecção contra perda de dados devido a falhas de hardware, erros humanos, ataques cibernéticos e desastres naturais.

Backup é o processo de criar e manter cópias duplicadas de dados, arquivos ou sistemas de computador para a protecção contra perda de dados devido a falhas de hardware, erros humanos, corrupção de dados, ataques cibernéticos ou desastres naturais (Stallings, 2017).

Para (Nelson, 2011) os backups podem ser definidos como cópias instantâneas de dados obtidas num determinado momento, armazenadas num formato globalmente comum e monitorizadas durante algum período de utilidade, sendo cada cópia subsequente dos dados mantida independentemente da primeira.

2.7.1. Tipos de backups

Os tipos de backup referem-se a diferentes estratégias e métodos de cópia de dados, utilizados para garantir a segurança, disponibilidade e integridade das informações.

Full Backups (Cópias de Segurança Completas)

Os backups completos representam um “instantâneo” (snapshot) completo dos dados que se pretende proteger. Os backups completos fornecem a linha de base para todos os outros níveis de backup. É útil para a recuperação rápida de todos os dados, mas consome mais armazenamento e largura de banda.

Backup Diferencial (Cópias de Segurança Diferencias)

O backup diferencial, também conhecido como backup incremental cumulativo, captura os backups que ocorreram desde o último backup completo. Este tipo de backup é normalmente utilizado em ambientes que não sofrem muitas alterações. (Nelson, 2011)

O backup diferencial deve ser usado com cuidado, pois pode crescer rapidamente ao ponto de igualar ou exceder o tamanho do backup completo original. A figura abaixo ilustra a forma como os backups diferenciais são feitos.

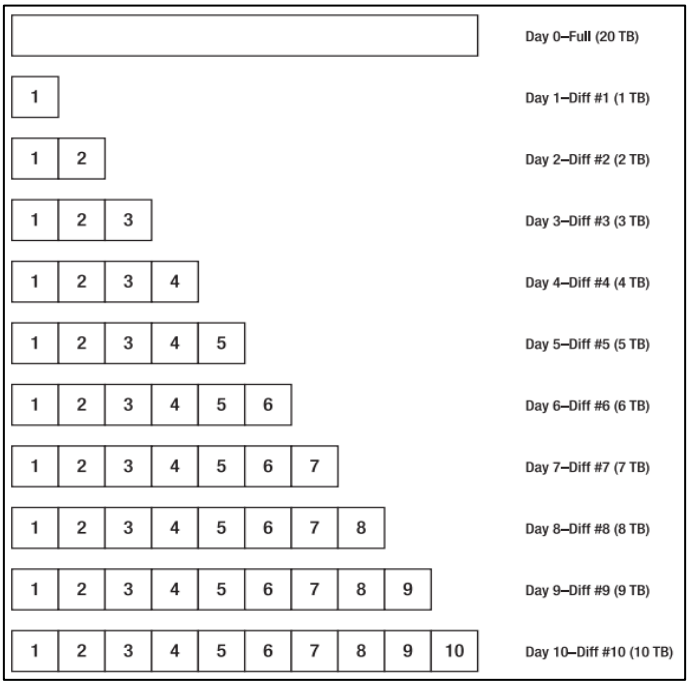


Figura 6: Ilustração de backups diferenciais. Fonte:

A vantagem de usar backups diferenciais, especialmente durante uma restauração, é o número de imagens de backup necessárias para executar a restauração. Uma

restauração diferencial requer apenas o backup completo mais o último mais o último backup diferencial para completar a restauração de qualquer arquivo na imagem de backup. Como há apenas um número limitado de imagens necessárias, a probabilidade de ambas as imagens serem perdidas ou corrompidas é diminuída significativamente.

Backup Incremental (Cópias de Segurança Incremental)

Este tipo de backup captura as alterações que ocorreram desde o último backup de qualquer tipo (incremental, diferencial ou full). Esta é a forma mais utilizada de backup em combinação com um backup completo pela sua vantagem na economia de espaço, comparado com o backup Diferencial.

O backup incremental contém a menor quantidade de dados necessários durante um ciclo de backup, reduzindo a quantidade de dados movidos e, em geral, o tempo necessário para um backup. (Nelson, 2011)

Para o exemplo da figura 7 do backup completo de 20 TB, no primeiro dia após o backup completo, o tamanho do backup seria de 1 TB (gerado), no segundo dia, 1 TB (gerado), e assim por diante. A quantidade de dados copiados depende apenas da diferença entre o backup anterior e o actual, pelo que o tamanho (e proporcionalmente o tempo necessário) para o backup é relativamente consistente. Se de um dia para o outro não houver mudanças o backup será de aproximadamente zero.

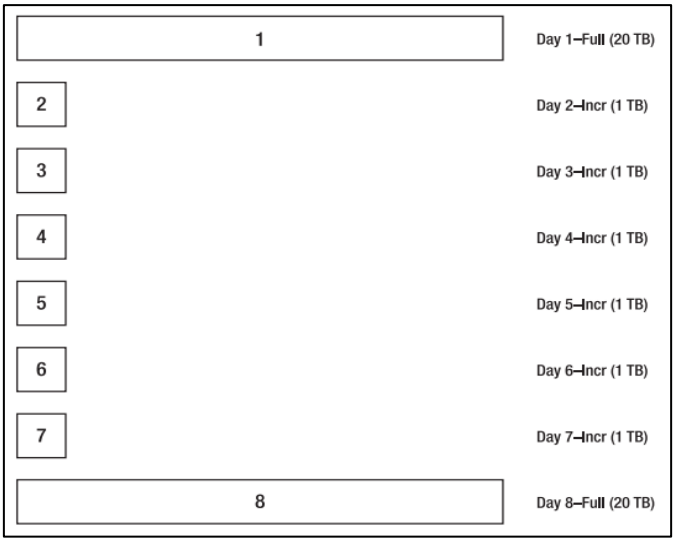


Figura 7: Ilustração de backups incrementais. Fonte: (Nelson, 2011)

Existem algumas desvantagens nas cópias de segurança incrementais. Por exemplo, se estiver a recuperar um conjunto de ficheiros a partir de um conjunto de backups completos e incrementais, é provável que necessite de mais de duas imagens de backup (incrementais) diferentes para concluir o a restauração. Se por exemplo estiver a recuperar um conjunto de ficheiros a partir de um conjunto de backups completos e incrementais, irá necessitar de mais de duas imagens do backup diferentes para concluir a restauração. Isto pode causar problemas durante o restauro porque é muito fácil seleccionar uma cópia de um ficheiro que não deve ser restaurado.

2.7.2. Importância dos backups

Os backups desempenham um papel fundamental na preservação, disponibilidade e segurança dos dados em qualquer organização ou ambiente de computação. Abaixo estão descritos alguns benefícios que se pode ter com a existência de backup:

- **Recuperação de dados**: graças aos backups é possível recuperar dados em caso de perda, devido as falhas de hardware, erros humanos, ataques de malware, desastres naturais ou corrupção de dados. Eles garantem que os dados possam ser restaurados com o mínimo de perda.
- **Continuidade dos negócios**: ajudam a garantir a continuidade das operações de negócios, permitindo que as empresas restaurem rapidamente sistemas e dados essenciais após incidentes de interrupção.
- **Conformidade e regulamentações**: muitos sectores têm regulamentações rígidas que exigem a retenção de dados por um período específico. Backups são essenciais para cumprir essas regulamentações.
- **Testes e desenvolvimento**: backups podem ser usados para criar ambientes de teste e desenvolvimento idênticos aos ambientes de produção, economizando tempo e recursos.
- **Minimização de perdas financeiras**: perder dados críticos pode resultar em perdas financeiras substanciais. Backups eficazes ajudam a minimizar essas perdas.

2.8. Restauração de Sistemas

Estratégias de recuperação de desastres (Disaster Recovery – DR) são conjuntos de planos, procedimentos e recursos que uma organização implementa para garantir a continuidade das operações em situações de desastres, seja ele natural ou causado pelo homem. O objectivo das estratégias de recuperação de desastres é minimizar o tempo de inactividade, proteger dados críticos e permitir que a organização volte a funcionar o mais rápido possível após um evento catastrófico. (Nelson, 2011)

2.9. DNS, DHCP e IPAM (DDI)

DDI é a abreviatura para a integração de DNS, DHCP e IPAM num serviço ou solução unificada. A DDI constitui a base dos serviços de rede principais que permitem todas as comunicações através de uma rede baseada em IP. (Infoblox)

Os serviços de DNS, DHCP e IPAM são úteis individualmente, mas a sua utilização combinada através de uma solução DDI produz melhores resultados em termos de uma melhor gestão e visibilidade da rede.

DNS (Domain Name Service): O serviço DNS ajuda a associar o nome de domínio de um dispositivo ou website ao respectivo endereço IPv4 ou IPv6.

DHCP (Dynamic Host Configuration Protocol): O DHCP permite que os dispositivos se liguem e troquem dados com êxito através de uma rede, atribuindo-lhes endereços IP únicos.

IPAM (IP Address Management): O IPAM, que em português significa Gestão de endereços IP, é uma técnica que abrange toda a rede para manter um controlo sobre os endereços IP atribuídos e não atribuídos numa rede.

Abaixo são apresentadas algumas das características mais populares das ferramentas DDI (SolarWinds):

- **Painel de controlo (dashboard) unificado para gestão de DDI**: As soluções modernas de DDI ajudam a gerir de forma inteligente os serviços de DNS, DHCP e IPAM através de uma consola centralizada para operações de rede

suaves e fiáveis. O painel de controle fornece uma visão holística dos ambientes DNS e DHCP de vários fornecedores. Estes painéis personalizáveis também permitem detectar as inconsistências entre registos DNS e dados IPAM e resolvê-las rapidamente para eliminar o risco de configurações conflituosas e endereços IP duplicados.

- **Gestão de endereços IPv4 e IPv6**: A DDI ajuda a simplificar e automatizar as tarefas de gestão de endereços IP. Utilizando esta ferramenta, pode identificar rapidamente endereços IP atribuídos e não atribuídos e de seguida categorizá-los em diferentes sub-redes com base nos requisitos da rede. Também permite efectuar pesquisas de endereços IP a nível global, controlar a utilização de sub-redes e resolver conflitos de IP.
- **Gestão de servidores DNS e DHCP de vários fornecedores**: A ferramenta DDI ajuda a gerir servidores DHCP e DNS de vários fornecedores a partir de uma localização centralizada. Pode encaminhar automaticamente quaisquer alterações efectuadas na estrutura de endereços IP para os servidores DNS e DHCP. Poupando tempo e a evitando erros durante a administração da rede. Também é possível detectar inconsistências nos registos DNS directos (forward) e inversos (reverse) através da consola centralizada para melhorar a fiabilidade da rede.
- **Alertas e relatórios inteligentes**: A DDI pode fornecer ferramentas inteligentes de alertas e relatórios para ajudar a rastrear e resolver proactivamente problemas de rede relacionados ao IP e garantir a continuidade dos negócios. Com estas ferramentas, é possível configurar facilmente alertas de email e notificações no ambiente de trabalho para conflitos de endereços IP, alterações de endereços MAC, registos DNS incompatíveis, sub-redes esgotadas e outros problemas críticos que impedem o bom funcionamento da rede. Estas ferramentas também permitem gerar relatórios personalizados para acompanhar a utilização da sub-rede em tempo real para um melhor planeamento da capacidade.
- **Gestão de eventos e registos**: As ferramentas DDI mantêm normalmente um registo detalhado dos eventos relacionados com o IP de uma rede. Estes registos de eventos detalhados podem ajudam a identificar rapidamente a causa principal de conflitos de endereços IP, incompatibilidades de registos

DNS e outros problemas de rede e garantir uma resolução acelerada de problemas para operações ininterruptas.

2.10. Firewall

A principal função de uma firewall é proteger a rede (de uma organização ou segmento de uma organização), de uma rede não confiável, através de um processo de filtragem de pacotes usando política de segurança.

A firewall actua como uma barreira entre uma rede privada e a rede pública, geralmente a Internet. Ele é projectado para monitorar, filtrar e controlar o tráfego de rede com base em regras de segurança predefinidas. As firewalls desempenham um papel fundamental na protecção de redes e sistemas contra ameaças cibernéticas, como invasões, malware e ataques. (SenthilKumar & Muthukumar, 2018)

Funcionalidades e características das firewalls incluem:

- **Filtragem de pacotes**: examinam cada pacote de dados que entra ou sai da rede e determinam se ele deve ser permitido ou bloqueado com base em regras de filtragem;
- ***Stateful inspection* (inspecção de estado)**: monitoram o estado das conexões de rede e permitem ou bloqueiam o tráfego com base no estado da conexão.
- **Proxy**: actuam como intermediários entre os usuários e os recursos da rede. Elas podem mascarar os endereços IP internos e fornecer uma camada adicional de segurança;
- **Firewalls de aplicação**: analisam o tráfego com base nas características da camada de aplicação (da camada 7), como protocolos e aplicativos específicos;
- **Access Control List (ACL):** ACL ou listas de acesso de controlo são usadas para definir permissões e restrições para o tráfego de rede com base em endereços IP, portas e protocolos;

- **Prevenção de intrusões**: algumas firewalls têm recursos de prevenção de intrusões (Intrusion Prevention System – IPS) que identificam e bloqueiam actividades suspeitas ou ataques;
- **Registo e auditoria**: podem gerar registros detalhados de eventos de segurança para fins de auditoria e investigação;
- Segmentação de Rede: podem ser usados para criar segmentação de rede e separar diferentes partes da rede (VLANs).

2.11. Multi-Protocol Label Switching (MPLS)

Antes de entender MPLS é necessário explicar que no encaminhamento IP (routing) convencional, cada router da rede tem de tomar decisões de encaminhamento independentes para cada pacote que chega/recebe. Quando um pacote chega a um router, este tem de consultar a sua tabela de encaminhamento para encontrar o próximo salto para esse pacote com base no endereço de destino no cabeçalho IP. Para criar tabelas de encaminhamento, cada router executa protocolos de encaminhamento IP como o Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) ou Intermediate-System to Intermediate-System (IS-IS). Quando um pacote atravessa a rede, cada router executa os mesmos passos para encontrar o próximo salto para o pacote. (Porwal, Yadav, & Charhate, 2008)

Uma técnica comum usada entre os grandes ISPs (Internet Service Providers) é usar uma rede de camada 2 para gerir a rede. Nesta abordagem, os fluxos podem ser individualmente roteados através da topologia de camada 2 e a e a engenharia de tráfego pode ser alcançada. Mas o inconveniente desta é a questão da escalabilidade e o facto de um único ponto de falha pode resultar na queda de dezenas de circuitos virtuais, forçando os protocolos de roteamento IP a se reconverterem.

A solução para esse problema pode ser a coordenação entre as redes da camada 2 e a rede IP de camada 3. Esta solução é o MPLS, um conjunto de procedimentos para combinar o desempenho, a QoS (Quality of Service) e a gestão do tráfego do paradigma da com a escalabilidade e flexibilidade da funcionalidade de

encaminhamento da camada 3. O MPLS, que significa Multi-Protocol Label Switching é uma extensão da arquitectura existente do Protocolo Internet (IP). Ao acrescentar novas capacidades à arquitectura IP, o MPLS permite o suporte de novas funcionalidades e aplicações. (Porwal, Yadav, & Charhate, 2008)

As principais características do MPLS são:

- **Roteamento com base em rótulos**: no MPLS, os pacotes de dados são encaminhados com base em rótulos (labels) em vez de endereços IP. Esses rótulos são anexados a pacotes na entrada da rede e usados para direccioná-los por meio de caminhos predefinidos;
- **Túneis MPLS:** os caminhos predefinidos, chamados de LSPs (Label Switched Paths), são estabelecidos através da rede para encaminhar o tráfego de forma eficiente;
- **Quality of Service (QoS):** o MPLS permite a implementação de QoS, o que significa que é possível priorizar o tráfego com base em requisitos de desempenho, como largura de banda e latência;
- **Escalabilidade**: o MPLS é altamente escalável, tornando-o adequado para redes de todos os tamanhos, desde redes empresariais até grandes infra-estruturas de provedores de serviços;
- **VPN MPLS**: permite a criação de redes virtuais privadas (VPNs) seguras por meio de isolamento de tráfego;
- **Eficiência**: o MPLS é conhecido por sua eficiência em comparação com protocolos de roteamento tradicionais, o que resulta em tempos de resposta mais rápidos e menos sobrecarga de processamento.

2.12. Software-Defined WAN (SD-WAN)

A SD-WAN é uma arquitectura de sobreposição que cria uma conectividade unificada segura sobre qualquer transporte e fornece operações simplificadas com gestão centralizada gestão centralizada, controlo de políticas e visibilidade de aplicações. A rede SD-WAN usa princípios de roteamento comuns, separa o plano de dados (data plane) separa o plano de dados do plano de controlo (control plane) e virtualiza grande parte da funcionalidade de roteamento. (Rajagopalan, 2020)

A SD-WAN é executada como uma sobreposição em hardware económico e em controladores centralizados que supervisionam o plano de controlo. O IP virtual seguro inclui roteamento e anúncios de roteamento e a capacidade de segmentar vários fluxos de tráfego. Também fornece autenticação e encriptação para proteger os dados do utilizador. O plano de controlo, o plano de dados e o IP virtual fornecem uma rede extensível.

A SD-WAN surge como uma forma de responder aos desafios que tecnologias como MPLS e o roteamento convencional cujas desvantagens são descritas a seguir:

- Roteadores e switches dispendiosos;
- Configuração e manutenção demoradas;
- Ligações de transporte ou circuitos de transporte dispendiosos;
- Complexidade;
- Plano de controlo (control plane) distribuído;
- Gestão remota de sites, controlo de alterações e manutenção das redes

No MPLS, as filiais zonais estão ligadas aos centro de dados (datacenters) através de routers. O tráfego de origem para destino é enviado e recebido através de métodos de endereçamento TCP/IP. Esta arquitectura é muito boa para encaminhar o tráfego de e para datacenter para as filiais zonais (por exemplo de uma empresa). Quando a computação em nuvem (cloud computing) evoluiu, o padrão de tráfego mudou completamente e o modelo MPLS não suportava o novo padrão de tráfego baseado em aplicações na nuvem. (Rajagopalan, 2020)

Uma das grandes vantagens da tecnologia SD-WAN é que suporta uma variedade de conexões, incluindo links de Internet, 4G/5G, MPLS entre outros, o que oferece maior flexibilidade para escolher e combinar diferentes tipos de links de acordo com os requisitos específicos de aplicativos.

A SD-WAN pode ser comissionada rapidamente, muitas vezes sem a necessidade de hardware adicional. O provisionamento e as alterações de configuração podem ser realizados de forma mais rápida.

2.13. Jump Box Server

Um Jump Box ou Jump Server é uma máquina ou servidor que actua como um ponto de acesso seguro para a rede. O Jump Box actua como uma ponte entre duas redes diferentes. Ele fornece um método de acesso controlado de uma rede comum para outra, que normalmente contém recursos significativos e altamente protegidos, permitindo a administração de outros sistemas. (Steffen, 2017)

Um Jumpbox possui as seguintes características:

- **Segurança**: é projectada com segurança em mente. Geralmente ela é configurada com medidas de segurança rigorosas, como autenticação de dois factores, firewall, monitoramento e registro de acesso.
- **Conectividade**: os administradores se conectam ao Jump Box por meio de uma conexão segura e a partir da Jump Box, eles podem então se conectar a outros sistemas na rede interna.
- **Isolamento**: o Jump Box é frequentemente colocado em uma *Demilitarized Zone* (DMZ) para garantir que ela esteja isolada da rede interna.
- **Administração centralizada**: o Jump Box é um ponto centralizado para a administração de sistemas. Isso simplifica a gestão, monitoramento e controlo de acesso.

A figura abaixo ilustra o uso de um JumpBox, a partir de um dispositivo (cliente) da rede (com dispositivos menos críticos), para aceder à um servidor que contém informação sensível e que se encontra na rede com dispositivos críticos.

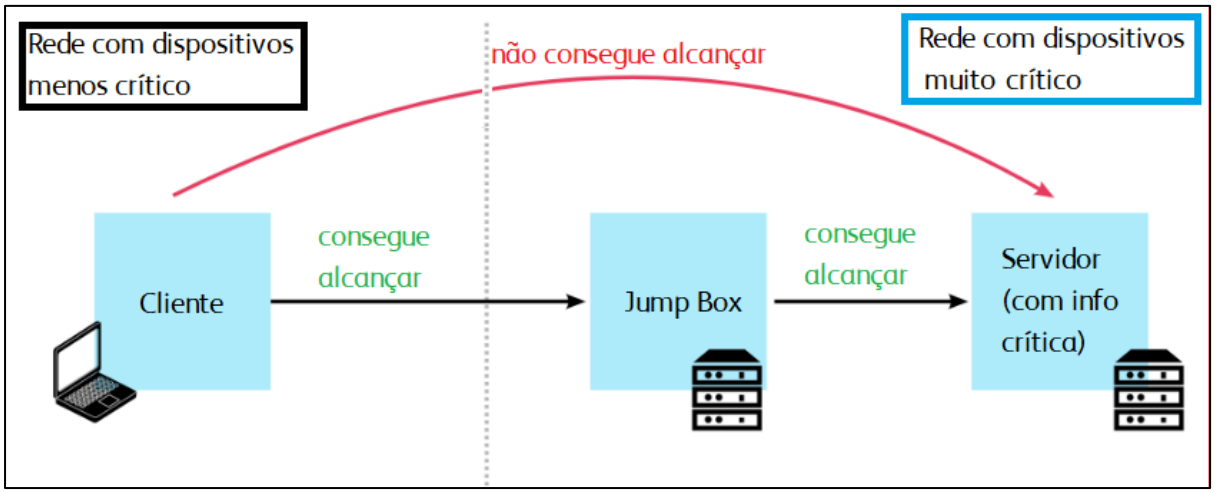


Figura 8: Acesso a um servidor em outra rede usando JumpBox. Fonte: (Servile, 2021)

A implementação de uma Jump Box é uma prática recomendada em ambientes de TI, especialmente em redes corporativas, para melhorar a segurança e a eficiência na administração de sistemas.

2.14. Process Control Domain (PCD)

Process Control Domain (PCD) ou *Process Control Network* (PCN) refere-se a uma área específica em sistemas de controle industrial, como sistemas de automação e controle de processos, onde a monitoração e o controle de processos físicos, como produção industrial, fabricação, distribuição e processamento, são realizados. (Indeed Editorial Team, 2022)

As características importantes de uma rede PCN incluem:

- **Sistemas de controlo industrial**: são sistemas que monitoram, controlam e automatizam processos físicos, como a produção em uma fábrica, refinaria, usina ou instalação de tratamento de água.
- **Redes industriais**: Essas redes são projectadas para fornecer comunicação confiável e segura entre dispositivos e controladores em um ambiente de controle de processos.
- **Controladores Lógicos Programáveis (Programmable Logic Controllers – PLC)**: os PLC são dispositivos-chave usados para automatizar tarefas e processos em um ambiente de controle industrial. Eles são programados para responder a entradas sensoriais e controlar saídas, como válvulas e motores.
- **Supervisão e controlo centralizados**: muitas vezes, os sistemas de controle industrial incluem uma estação de controle centralizada (como um SCADA - *Supervisory Control and Data Acquisition*) que permite aos operadores monitorar e controlar todo o processo.
- **Sensores e instrumentação**: a instrumentação é usada para medir variáveis físicas, como temperatura, pressão, nível e fluxo, e os dados dos sensores são usados para controlar o processo.
- **Segurança e confiabilidade**: a segurança é uma consideração crítica em ambientes de controle de processos, pois falhas ou erros podem ter impactos significativos na segurança dos trabalhadores e na eficiência do processo.

- **Manutenção preventiva**: a manutenção preventiva é crucial para garantir a operação confiável dos sistemas de controle de processos e evitar paradas não programadas.

A automação de processos em ambientes industriais é fundamental para aumentar a eficiência, reduzir erros humanos, melhorar a qualidade do produto e optimizar o uso de recursos. O Process Control Domain desempenha um papel vital na garantia de que os processos industriais funcionem de forma eficiente e segura. (Indeed Editorial Team, 2022)

2.15. Brewmaxx

BrewMaxx é uma solução de software especificamente projectada para cervejarias, oferecendo soluções de controle de processos e automação para optimizar as operações de produção de cerveja. (ProLeiT Group, 2023)

Este software é frequentemente utilizado como um software de Planejamento de Recursos Empresariais (*Enterprise Resource Planning* – ERP) para cervejarias, ajudando-as a gerenciar vários aspectos de suas operações comerciais.

Algumas das principais funcionalidades do software são:

- **Gestão de produção**: auxilia na gestão de todo o processo de produção, desde a formulação de receitas até a brassagem, fermentação, embalagem/empacotamento e controlo de qualidade.
- **Gestão de estoque**: a as cervejarias a acompanhar matérias-primas, produtos acabados e materiais de embalagem, garantindo uma gestão eficiente de estoque.
- **Controlo de qualidade**: o software frequentemente inclui ferramentas para controlo e garantia de qualidade, permitindo que as cervejarias mantenham uma qualidade de produto consistente.
- **Rastreamento de lotes**: permite que as cervejarias rastreiem lotes de produtos, o que é crucial para o controle de qualidade e o cumprimento das regulamentações da indústria.

- **Vendas e distribuição**: ajuda a gerir pedidos de vendas, distribuição e relacionamento com o cliente, garantindo que os produtos sejam entregues de forma eficiente e no prazo.
- **Gestão financeira**: pode incluir módulos financeiros para contabilidade, orçamento e relatórios financeiros.
- **Conformidade**: ajuda as cervejarias a cumprir os requisitos regulatórios relacionados à produção de cerveja e bebidas.
- **Relatórios e análises**: fornece ferramentas para gerar relatórios e analisar dados, ajudando as cervejarias a tomar decisões informadas.
- **Integração**: pode oferecer capacidades de integração com outros sistemas de software, como sistemas de ponto de venda (POS – *Point of Sale*) ou plataformas de comércio electrónico.

3. CAPÍTULO III – DESCRIÇÃO DAS ACTIVIDADES DESENVOLVIDAS

Neste capítulo, serão descritas as actividades desempenhadas durante o período de estágio, incluindo as actividades diárias na empresa, bem como os projectos e outras actividades não-rotineiras relevantes.

A minha função durante estágio estava directamente ligada à gestão e manutenção da infra-estrutura informática e na prestação de assistência aos utilizadores (helpdesk). Durante esse período, estive integrado numa equipa talentosa de profissionais de TI, que juntos contribuíam para a correcta operação dos sistemas usados na empresa, boa prestação de serviços de TI e também na optimização e monitoramento dos servidores, redes e sistemas existentes na empresa.

Para além disso, participei activamente situações de troca de experiência com colaboradores de outras funções, o que foi aprimorando as minhas habilidades técnicas e adquirindo conhecimento prático em áreas diferentes de TI.

3.1. Horário de Trabalho

O horário laboral atribuído pela empresa, para os trabalhadores administrativos é descrito abaixo:

- De segunda à sexta: entrada as 08:00 e saída as 17:00h – na sede, com direito a intervalo de 1h
- De segunda à sexta: entrada as 07:00 e saída as 16:00h – na fábrica, com direito a intervalo de 1h

De salientar que na fábrica, normalmente, as operações correm 24/7 e os trabalhadores fazem turnos. Por conta disso, em algumas ocasiões foi necessário de dar suporte à alguns colaboradores ao longo final de semana. A escala fixa semanal a mim atribuída desde a primeira semana é descrita na tabela abaixo:

Dia / **Local**	**Segunda-feira**	**Terça-feira**	**Quarta-feira**	**Quinta-feira**	**Sexta-feira**
Sede	Sim	Não	Não	Sim	Sim
Fábrica	Não	Sim	Sim	Não	Não

Tabela 2: Horário de trabalho. Fonte: Autor

3.2. Estrutura do Departamento

O departamento onde fui acolhido, designado ***Digital&Technology*** ou "D&T", era inicialmente composto por três (2) membros, nomeadamente: **Sete Matimele** (função: D&T *Manager*), **Lúcio Rebeca** (função: *Business Application Manager*) e **Castigo Dramuce** (função: IT Front Office).

Dois (2) meses após a minha chegada, o departamento passou a contar com o quarto membro: **António Pinto** (função: IT Front Office).

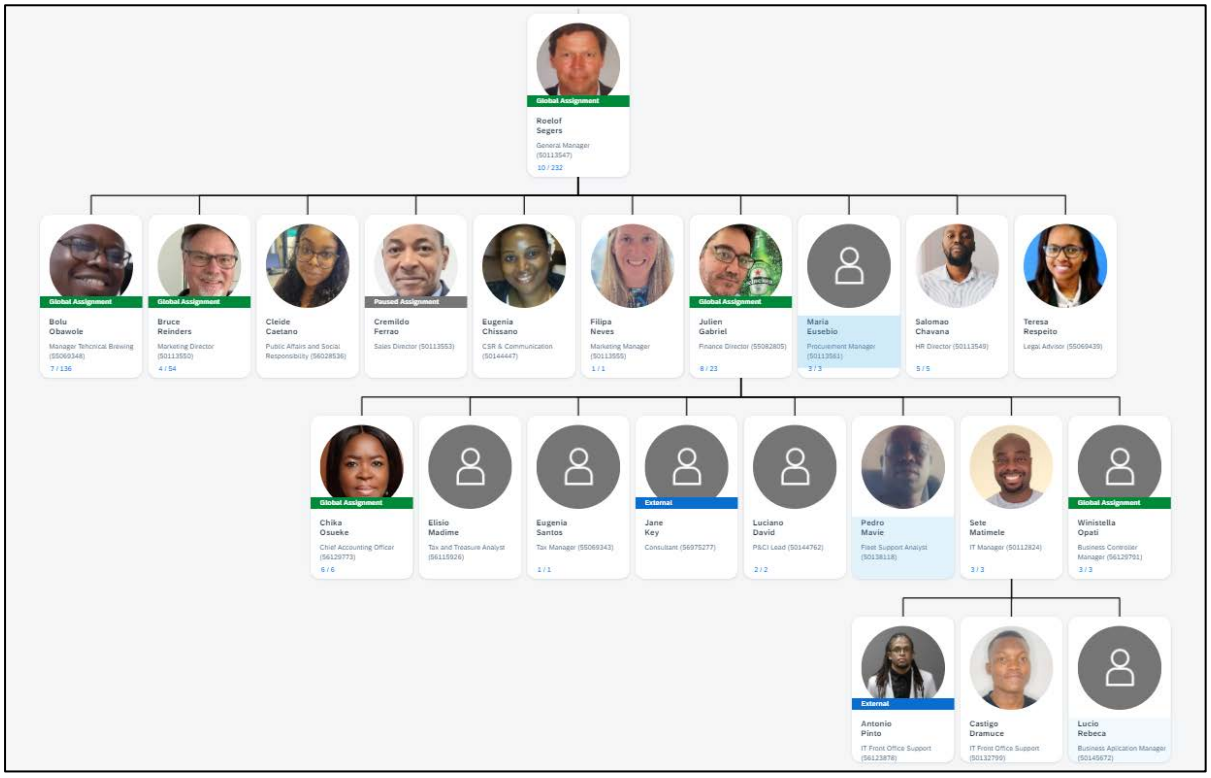


Figura 9: Organograma da empresa. Fonte: Autor

Para além da equipa local de TI acima mencionada, existe uma equipa externa, designada "**AMEE Infrastructure Hub**" ou "Hub" que é composta por especialistas em soluções digitais, análise de dados, segurança da informação e tecnologia.

A equipa **AMEE Infrastructure Hub** é responsável por dar suporte remoto às equipas locais (das OpCos) das diferentes empresas HEINEKEN, em assuntos relacionados às áreas supracitadas, somente na região da África, Médio Oriente e Europa, daí a designação "AMEE" (Africa, Middle East & Europe).

De salientar que para as diversas áreas existentes na HEINEKEN (*Procurement*, *Supply Chain*, *Planning*, etc.) existe um Hub correspondente que dá suporte à equipa local.

A equipa do Hub recebe as directrizes de uma equipa Global correspondente, que por sua vez é responsável pela construção de interacções digitais contínuas em toda a cadeia de valor, fornecendo estratégias, políticas, padrões e conhecimentos às equipas de produtos (*Product Teams*) & Hubs (regionais). A equipa Global é composta por várias equipas especializadas em diversos ramos, existindo uma equipa Global responsável pela área de Cibersegurança, outra responsável pela área de Gestão de Aplicações, outra responsável pela demais Firewalls implementadas a nível do grupo HEINEKEN, entre outras.

Para além disso a equipa Global também trabalha em colaboração com os trabalhadores de várias funções para desenvolver, seleccionar, e implementar as melhores soluções; cria planos estratégicos com as funções e possibilitam a execução fornecendo recursos de tecnologia digital.

Para que se possa ter o suporte do Hub ou das equipas Globais é feito o uso da plataforma de gestão de *tickets* usada a nível do grupo, o *Service Now* (ou SNOW), cuja gestão é também feita por uma das equipas Globais.

3.3. Actividades rotineiras

No primeiro mês as actividades resumiam-se no entendimento da estrutura organizacional, estudo dos procedimentos operacionais diários, familiarização com as ferramentas de trabalho, conhecimento da infra-estrutura e assistência aos utilizadores.

Das diversas actividades desempenhadas durante o percurso do estágio, importa ressaltar algumas que estão descritas abaixo:

3.3.1. Preparação das estações de trabalho

Todas as estações de trabalho da empresa (desktop, laptops e tablets) devem ter o sistema operativo instalado a partir de uma imagem do Windows 10 customizada. A

customização da imagem do sistema operativo é da responsabilidade de uma das equipas Globais, podendo o Hub ou a equipa local fazer de forma limitada, alterações na imagem para que as estações de trabalho tenham as ferramentas adequadas para o trabalho diário dos colaboradores.

A customização da imagem do sistema operativo é feita usando a ferramenta Microsoft SCCM (System Center Configuration Manager), agora conhecido como Microsoft Endpoint Configuration Manager. A instalação da imagem do Windows nas estações de trabalho é somente feita a partir da rede usando a tecnologia PXE Boot.

Parte do trabalho desempenhado durante o percurso do estágio envolvia a preparação das estações de trabalho, garantindo a instalação do sistema operativo Windows (customizado) e fazendo uso de um dos componentes da ferramenta SCCM, o Configuration Manager Console, para criar os objectos de computador que iam receber a imagem do Windows e também para garantir que os mesmos objectos de computador estejam nas colecções de dispositivos (*device collections*) que eram responsáveis por enviar e instalar softwares para o computador.

3.3.2. Participação em Projectos

Em diversas ocasiões tive a oportunidade de participar em alguns projectos que valem mencionar, sendo alguns deles:

- **Instalação de uma nova controladora WiFi na empresa**

Este projecto consistiu na instalação de uma controladora WiFi na sede HEINEKEN e na alocação, da controladora que antes se encontrava na sede, à fábrica. Antes do início deste projecto, todos os Access Points (AP) da fábrica como da sede se autenticavam na controladora Cisco 2500 Series que se encontrava na sede. Esta controladora tem uma licença para vinte e cinco (25) AP.

O objectivo deste projecto foi de fazer o uso de uma segunda controladora, Cisco 3500 Series, que já havia sido adquirido antes da minha chegada mas não estava em uso, e tinha licença para 6 AP.

Abaixo pode ser visto como estava a configuração da controladora e AP antes da configuração.

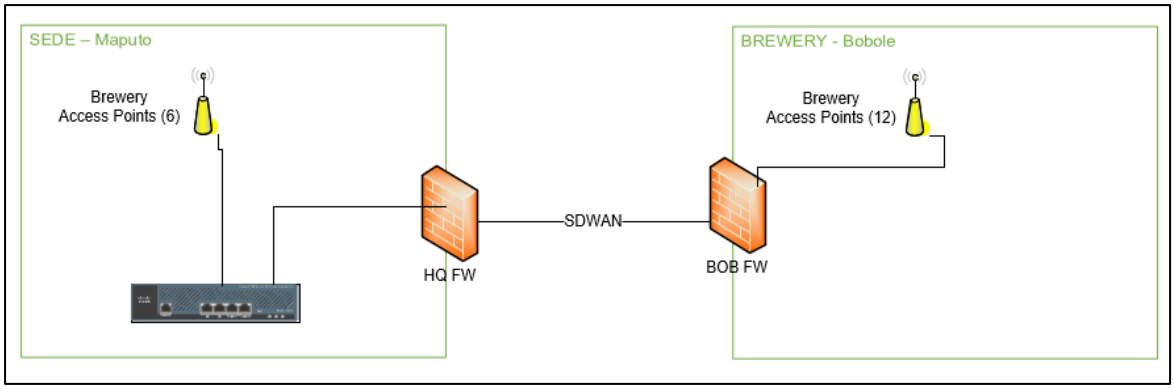


Figura 10: Conexão dos APs antes da mudança. Fonte: Autor

Através do circuito existente entre a firewalls da sede e da fábrica, os APs da fábrica se autenticavam na controladora que se encontrava na sede usando a funcionalidade FlexConnect que estava configurada nos access points da fábrica.

Mas visto que a fábrica contava com mais de 12 AP e a sede tinha somente 6 APs em funcionamento, o primeiro passo consistiu em alocar a controladora Cisco 2500 Series à fábrica e mudar os detalhes de endereçamento IP na mesma e nos access points da fábrica, para reflectir a rede em uso na fábrica, que é diferente da cidade, mas são roteáveis.

De seguida, foi instalada a controladora Cisco 3500 Series na sede e foram atribuídos os detalhes de endereçamento IP que a controladora 2500 Series usava quando funcionava a partir da sede.

No final foram configurados os access points da fábrica de modo a não se autenticarem na controladora da fábrica. Dessa forma, os APs da sede se autenticavam na controladora da sede e os APs da fábrica se autenticavam na controladora da fábrica.

Desta forma, a configuração da controladora e APs teve a estrutura vista na figura abaixo.

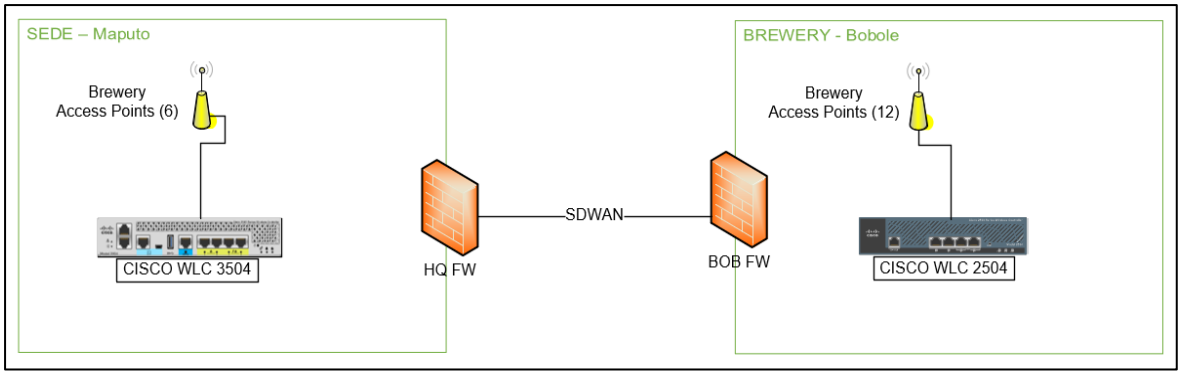


Figura 11: Conexão dos APs depois da mudança. Fonte: Autor

- **Tax Stamp**

O projecto consistiu na implementação de impressoras específicas na área da produção. Essas impressoras fazem a estampagem de "selos fiscais", que devem estar presentes em todas as cervejas e bebidas pronto a consumir (*Ready to Drink* – RTD), que foram impostos pela Autoridade Tributária de Moçambique (MEF, 2022).

A função desempenhada neste projecto esteve ligada à criação e configuração das máquinas virtuais onde estaria instalado o software que descarrega os selos do website fornecido pela Autoridade Tributária. Outra função desempenhada foi garantir que houvesse comunicação entre as impressoras que são usadas na estampagem dos selos e as máquinas virtuais criadas.

- **Operacionalização do Call Center da Sede**

A empresa contava, no passado, com um call center estava localizado na sede e era usado para a gestão de chamadas, mas devido à uma gestão não-satisfatória por parte da empresa contratada para a instalação e manutenção do call center, a HEINEKEN Moçambique cessou o contracto com a empresa e de seguida foi elaborado um concurso para várias empresas onde estas deveriam apresentar uma proposta para deixar o sistema de call center operacional.

A minha contribuição neste projecto esteve ligada à gestão da infra-estrutura, onde tive de garantir tudo o que diz respeito aos servidores (criação e configuração dos mesmos), comunicação entre os servidores e os telefones que seriam fornecidos,

funcionamento dos *voice gateways* (que já existiam e estavam configurados) e a comunicação entre estes e o servidores.

Para além disso outra contribuição esteve na interligação entre o recém-instalado call center e a plataforma Microsoft Customer Relationship Management (CRM) Dynamics onde eu estive responsável por dar suporte nos aspectos que concernem à rede nos casos em que houvesse algum erro que proveniente dos aspectos da rede, como por exemplo bloqueios da firewall.

- **Desactivação do Site Secundário do SCCM**

Desde o início das operações da HEINEKEN Moçambique, a empresa tinha na sua infra-estrutura, dois (2) servidores (virtuais) pertencentes à estrutura do SCCM, cujas funções (*role*) eram de Site Secundário (*Secondary Site*) e Ponto de Distribuição (*Distribution Point*). O servidor de Site Secundário estava instalado na infra-estrutura da sede e o ponto de distribuição estava instalado na infra-estrutura da fábrica.

Depois de quatro (4) anos de operação destes servidores, uma análise foi feita pela equipa Global responsável pelo SCCM e foi determinado que a OpCo tinha um número muito baixo de dispositivos, aproximadamente 171, que estavam registados no site secundário do SCCM que se encontrava na cidade.

Foi determinado que o mais sensato para a OpCo seria ter um ponto de distribuição na cidade também, invés de um site secundário pois os sites secundários suportam até quinze mil dispositivos. Então os pontos de distribuição presentes na sede e na fábrica seriam vinculados à um site secundário na região (África) que não tenha o número de dispositivos próximo ao limite.

Com isto, seria necessário fazer a desactivação do site secundário da OpCo (que seria feito pela equipa Global) e criar uma máquina virtual, que deveria ser feito pela equipa local, que seria o novo ponto de distribuição que irá substituir o site secundário. As especificações da máquina virtual a ser criada foram partilhadas pela equipa Global.

Neste projecto, a minha função foi de garantir que já estava disponível um servidor virtual com as especificações, previamente partilhadas pela equipa Global, onde

pudessem ser instaladas as aplicações necessárias para o comissionamento do novo ponto de distribuição para a sede.

Após o término da instalação do ponto de distribuição, a minha função era de garantir que as instalações dos sistemas operativos nas estações de trabalho funcionavam correctamente e outras funcionalidades relacionadas ao SCCM (como instalação de softwares) também funcionavam sem problemas após esta mudança.

- **Migração do DDI**

DDI é a sigla para **DNS, DHCP, and IPAM (*IP Address Management*)** que é frequentemente usada para descrever a integração desses três componentes principais da rede em uma solução de gerenciamento. Este projecto consistiu na migração do DDI para a plataforma Infoblox.

Antes da execução deste projecto, os servidores de DHCP & DNS eram geridos localmente em todas OpCos. No caso de Moçambique:

- Na sede, o serviço de DHCP foi instalado no servidor que tinha a função de *Domain Controller*; O servidor de DNS era a firewall que tinha o link de internet do provedor.
- Na fábrica, o servidor de DHCP era o *Core Switch*. O servidor de DNS era a firewall que tinha o link de internet do provedor.

Na primeira fase deste projecto as minhas tarefas consistiram em enviar a informação detalhada das redes e VLANs que a empresa usa e o seu propósito. Na segunda e última fase, as minhas tarefas eram de desactivar os servidores DHCP locais tanto na fábrica, como na sede; configurar os parâmetros de DHCP nas controladoras WiFi e nos switches, inserindo nestes o endereço IP dos novos servidores DHCP; configurar nos servidores o endereço do novo DNS; garantir que os dispositivos (laptops, desktops e telefones IP) recebiam o endereçamento IP & DNS a partir do novo DHCP server & DNS server, que é gerido plataforma da Infoblox.

- **Melhoria de performance e backup do computador do Weighbridge**

Outro projecto que foi de grande relevância, foi a melhoria na performance do computador que se encontrava no Weighbridge, uma das áreas da fábrica onde existe um computador que processa as informações de carregamentos (de produtos acabados e materiais) da fábrica. Nesta área existe um computador que os operadores frequentemente reportavam lentidão do mesmo.

Após uma avaliação do computador foi possível determinar o motivo da lentidão do computador. Durante o uso normal do computador o uso da memória RAM no computador estava acima dos 85%, para além disso o computador possuía um disco duro instalado, o que representa a minoria dos computadores da empresa, pois a maior parte dos computadores tinham um SSD instalado.

Com estas constatações e depois de proposta a solução, que seria o aumento da memória RAM e a troca do disco duro por um SSD, foi comunicada a área do Weighbridge e da Logística a informar que seria necessário fazer as alterações supracitadas no computador, o que implicava a paragem de entrada de caminhões.

Pelo facto deste computador possuir alguns softwares de terceiros cujo suporte deve ser agendado e acarreta alguns custos, a solução funcional mais viável encontrada foi da clonagem das informações do disco duro para o SSD. Como forma de contornar estes gastos, a clonagem do disco duro foi a melhor opção encontrada.

Foi proposto um dia, ao longo do final de semana para serem feitas estas alterações, onde foram então efectuadas as seguintes acções

1. Backup das informações existentes no computador para um disco duro externo;
2. Preparação de uma unidade USB para colocar o software de clonagem, “CloneZilla”;
3. Desactivação do *bitlocker* no computador;
4. Clonagem do disco duro inteiro para um SSD de igual capacidade;
5. Conservação do HDD em um local seguro para servir de backup em caso de haver alguma falha do computador actual;
6. Aumento da memória RAM, de 8GB para 16GB;
7. Inicialização do computador a partir do SSD;

8. Activação do *bitlocker* no computador;

Após estas actividades o meu trabalho foi monitorar se surgiam problemas e/ou erros resultantes dessas alterações.

3.3.3. Outras actividades

Para além das actividades acima descritas, outras tarefas eram de desempenhas de forma regular eram:

- Atribuição de equipamentos aos utilizadores – eram da minha responsabilidade atribuir itens como telemóveis, computadores e acessórios, cartões SIM com contracto, pastas de costas, teclados, mouses, entre outros equipamentos concernentes à TI;
- Gestão de licenças – atribuição e remoção de licenças da Microsoft, Adobe, entre outras;
- Troca recorrente da password da rede WiFi *Guest* – que muda mensalmente, em todas as OpCos, num dia predefinido e obedecendo uma lista de passwords previamente partilhada pela equipa do Hub, anualmente;
- Configuração de *switches*, roteadores e pontos de acesso sem fio;
- Documentação de procedimentos (de operações relacionadas com TI) e partilha dos mesmos com a equipa de TI;
- Suporte às diversas funções para o *setup* de eventos e reuniões – prover ajuda em ocasiões em que houvesse a necessidade de projectar a imagem para TVs e também transmitir o vídeo para a plataforma Microsoft Teams, entre outras.

4. CAPÍTULO IV – CASO DE ESTUDO

Neste capítulo, será apresentado o caso de estudo para proporcionar uma compreensão mais clara do tipo de organização onde o trabalho foi desenvolvido.

4.1. Organização da Infra-estrutura de TI no alto nível

A HEINEKEN Moçambique, possui um padrão de operação conforme as empresas de similar função. Onde esta possui um ambiente somente dedicado aos equipamentos e sistemas usados para a produção, o que na empresa é considerado *Process Control Domain* (PCD) ou *Process Control Network* (PCN), e o outro ambiente para usos do escritório que na empresa é considerado “Office”.

Estes ambientes são separados por uma firewall interna que garante que o tráfego dos equipamentos que se encontram no Office somente seja possível a partir de dispositivos específicos (como por exemplo um *Jump Box*) e usando os protocolos autorizados para o tráfego. A firewall que separa os ambientes tem a gestão feita pela equipa Global responsável pelas firewalls implementadas a nível do Grupo HEINEKEN.

Como forma de fornecer uma visão abrangente do ambiente de tecnologia da informação que suporta as operações da HEINEKEN Moçambique, a figura abaixo ilustra de forma geral como a infra-estrutura de TI está organizada e estruturada.

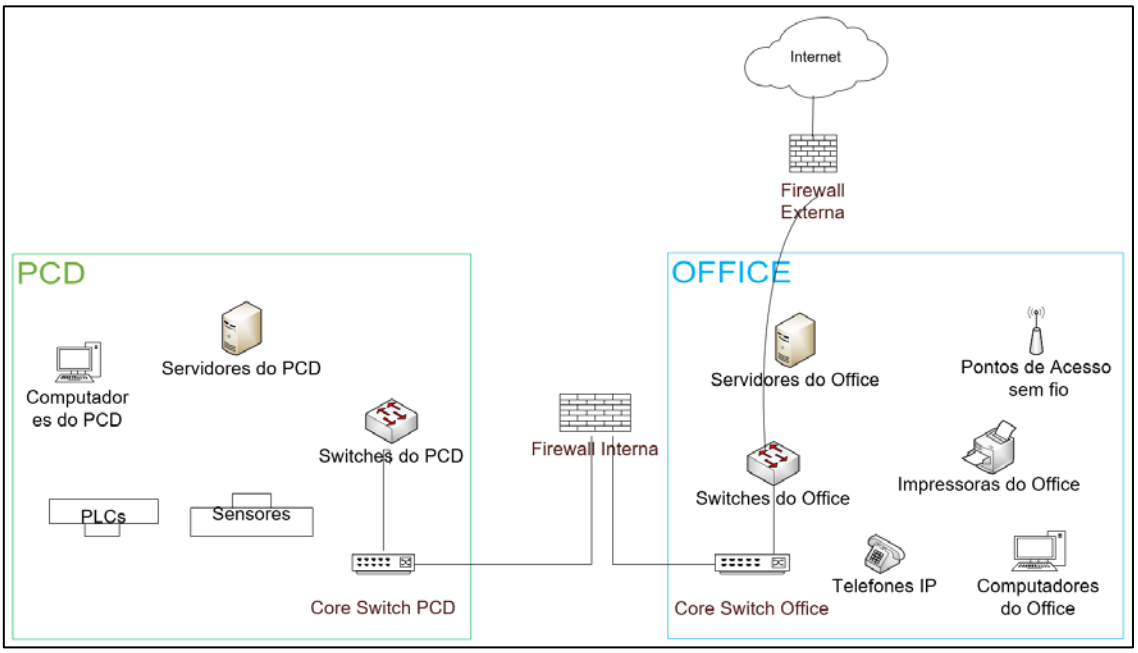


Figura 12:Organização da Infra-estrutura da empresa. Fonte: autor

4.1.1. Office (Escritório)

Do lado do Office existe uma firewall externa que faz o filtro do tráfego da internet para dentro da rede do Office.

Na rede do Office é onde se encontram as impressoras, telefones IP, pontos de acesso, switches e estações de trabalho que são usadas diariamente pelos colaboradores para actividades rotineiras.

Os switches encontrados nesta rede que garantem a comunicação entre os demais dispositivos neste ambiente (Office), garantido também a alimentação de alguns dispositivos como access points que se encontram no mesmo ambiente.

Para os dispositivos com placas sem fio que estão disponíveis neste segmento, os Pontos de Acesso sem fio (*Wireless Access Points* – WAP), são usados tanto em dispositivos móveis pessoas como também nos dispositivos móveis corporativos, tendo a devida separação das redes usadas pelos SSIDs emitidos pelos access points.

Existem também neste ambiente servidores que contém máquinas virtuais que fornecem suporte aos demais serviços disponíveis na infra-estrutura. A rede o Office dispões de um servidor (virtual) que, através de algumas regras da firewall interna, é o elo de comunicação entre a rede do Office e do PCD para actividades como configuração de dispositivos de rede encontrados na rede do PCD, entre outras.

4.1.2. PCD

Desta a garantir haja uma maior segurança, existe uma firewall que separa os ambientes do Office e PCD, conforme explicado em **4.1**, neste segmento (PCD) existem também servidores cujo propósito é somente fornecer suporte às diversas aplicações e dispositivos usados neste ambiente.

Para fazer a interligação dos demais dispositivos existentes no ambiente PCD, como máquinas virtuais, impressoras (específicas da produção), PLCs, sensores, entre outros, existem switches que garantem a comunicação dos mesmos.

Existem também nessa rede, computadores cujo propósito é somente auxiliar na operação dos equipamentos existentes nessa rede. Estes computadores em nenhum momento se conectam à rede do Office e/ou a internet.

4.1.3. Cenário de Actual

A fábrica dispões de um *datacenter* devidamente refrigerado onde estão localizados os demais servidores e dispositivos de rede da infra-estrutura. O datacenter também com a existência de dois (2) sistemas de UPS (*Uninterruptible Power Supply*) com capacidades de Oito Kilovolt-ampere (8KVA) e Vinte Kilovolt-ampere (20KVA), respectivamente que alimentam os racks existentes na sala.

Dentre os equipamentos encontrados no datacenter, importa destacar a existência de dois racks onde o primeiro é de 48U de marca BARPA, destinado para os equipamentos de rede – denominado “Rack 1 (Network)” conforme a figura13. Neste rack encontramos equipamentos como switches, patch panels, controladora WiFi, firewalls entre outros.

O segundo rack de 42U da marca HPE, é destinado para servidores e outros “*appliances*” físicos, mas também pode ser encontrado neste um patch pannel que garante a ligação entre os racks.

Como forma ilustrar os equipamentos existentes na infra-estrutura, as figuras 13 e 14 apresentam o desenho dos equipamentos existentes em ambos racks, seguidos de uma letra do abecedário (pintada a vermelho) para poder distinguir os equipamentos existentes, pois existem equipamentos similares (mesma marca e modelo).

As tabelas que seguem (nomeadamente Tabela 3 e Tabela 4) servem como forma de descrever os equipamentos vistos nos desenhos 13 e 14 respectivamente.

Disposição dos equipamentos no Rack 1 (Network)

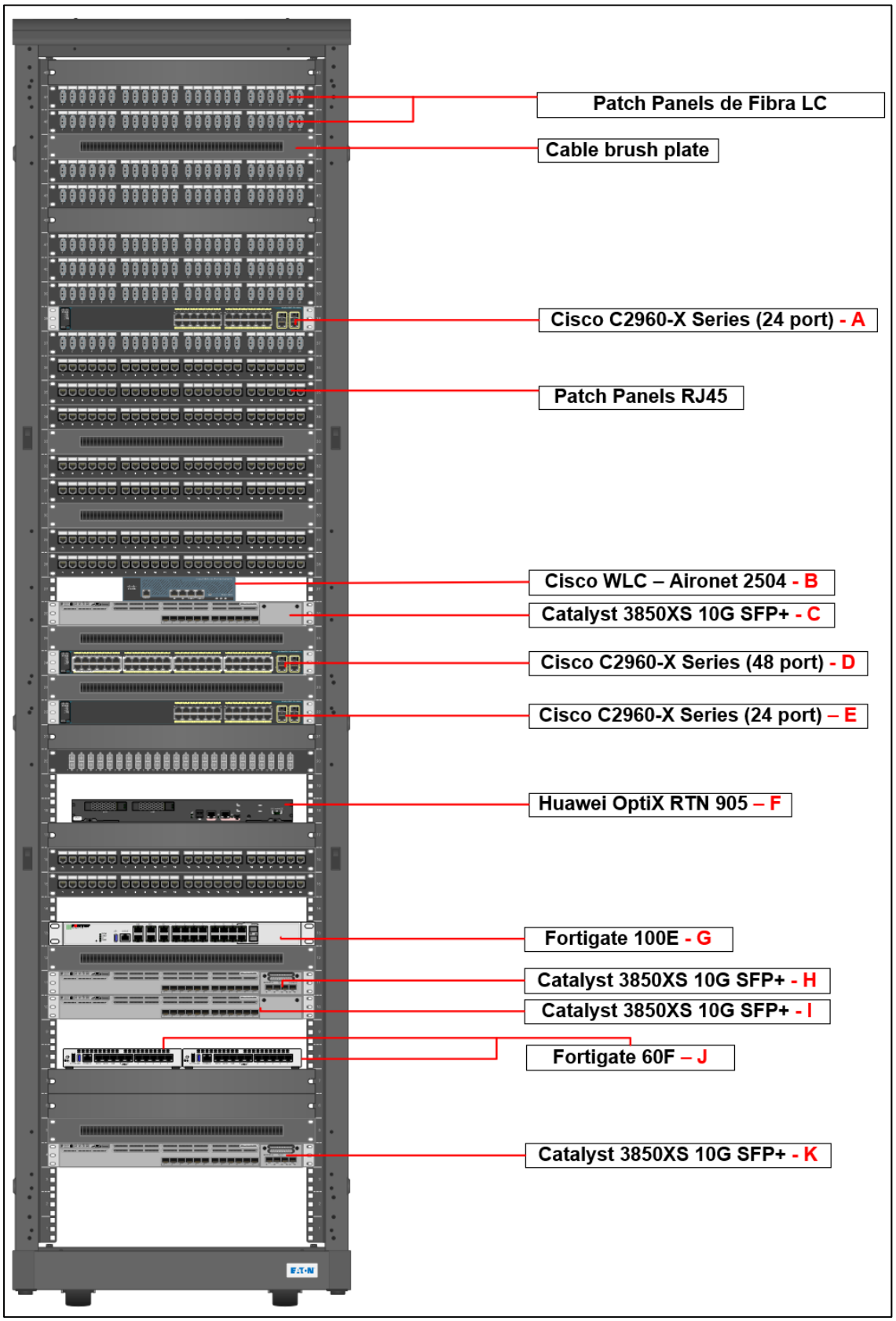


Figura 13: Disposição actual dos dispositivos no Rack 1 (Network) - Fonte: Autor

A tabela abaixo descreve a legenda da figura anterior, mencionando a função dos itens encontrados no rack:

Item	Descrição	Função/Papel
Cisco C2960-X Series (24 port) – A	Switch L2 – Acesso	Switch the accesso (Office Network)
Cisco WLC – Aironet 2504 – B	Cisco Wireless Controller	Controladora dos APs da fábrica
Catalyst 3850XS 10G SFP+ – C	Switch L3 – Distribuição	Switch de distribuição (Office Network)
Cisco C2960-X Series (48 port) – D	Switch L2 – Acesso	Switch the accesso 2 (Office Network)
Cisco C2960-X Series (24 port) – E	Switch L2 – Acesso	Switch the accesso 3 (Office Network)
Huawei OptiX RTN 905 – F	Equipamento de Telecom	
Fortigate 100E – G	Firewall PCD	Firewall interna que separa o ambiente do Office do PCD
Catalyst 3850XS 10G SFP+ – H	Switch L3 – Core PCD	Switch de Core do ambiente PCD
Catalyst 3850XS 10G SFP+ – I	Switch L3 – Core OFC	Core Switch “Principal” da rede do Office Main. Está em stack com o switch Catalyst 3850XS 10G SFP+ – K
Fortigate 60F – J	Firewall SD-WAN	Firewall externa que separa a rede do Office da internet. Ambas firewall idênticas (Fortigate 60F) usam a tecnologia SD-WAN
Catalyst 3850XS 10G SFP+ – K	Switch L3 – Core OFC	Core Switch “Redundante” da rede do Office Main. Está em stack com o switch Catalyst 3850XS 10G SFP+ – I

Tabela 3: Legenda dos equipamentos do Rack 1 (Network) – Fonte: Autor

Disposição dos equipamentos no Rack 2 (Servers)

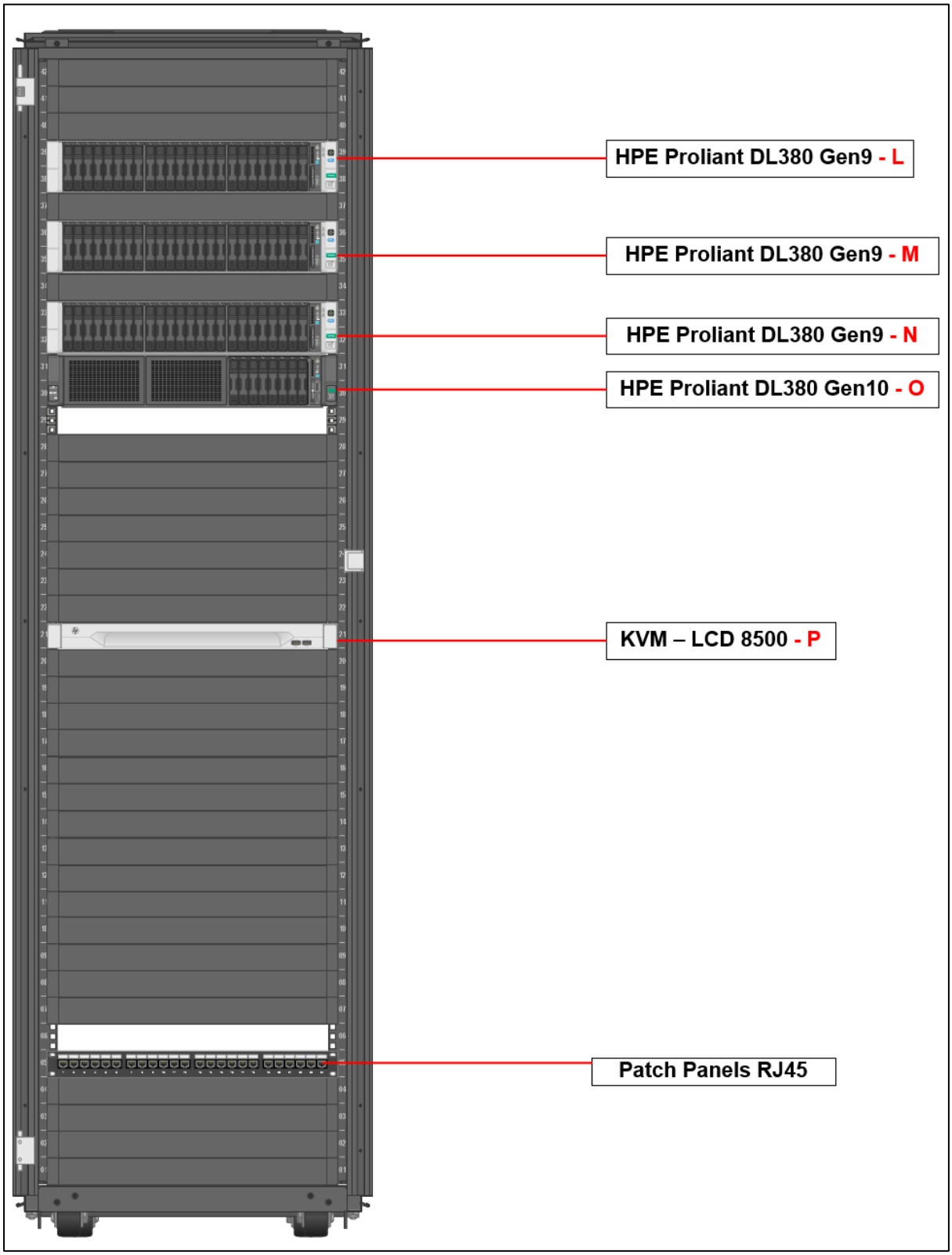


Figura 14: Disposição actual dos dispositivos no Rack 2 (Servers) - Fonte: Autor

A tabela abaixo descreve a legenda da figura anterior, mencionando a função dos itens encontrados no rack:

Item	Descrição	Função/Papel
HPE Proliant DL380 Gen9 – L	Servidor/host com VMware ESXi 6.7U3 – PCD	Hospeda as VMs do ambiente do PCD *Host*
HPE Proliant DL380 Gen9 – M	Servidor/host com VMware ESXi 7.0U3 – Office	Nenhuma
HPE Proliant DL380 Gen9 – N	Servidor com o Software BrewMaxx	Contém a aplicação BrewMaxx
HPE Proliant DL380 Gen10 – O	Servidor/hosts com VMware ESXi 6.7U3 – Office	Hospeda as VMs do ambiente do Office Host
KVM – LCD 8500 – P	Monitor, Teclado & Mouse	Usado para mostrar a saída de vídeo dos servidores

Tabela 4: Legenda dos equipamentos do Rack 2 (Servers) – Fonte: Autor

A figuras 12 mostra no mais alto nível os componentes que fazer parte da infra-estrutura, onde temos a separação das redes. A nível físico, vários dos componentes se encontram no mesmo espaço físico, conforme ilustram as figuras 12 e 13 acima. A nível lógico existe uma separação entre os demais componentes que se encontram nos racks. Esta separação é ilustrada na figura 15 abaixo.

Interligação dos equipamentos

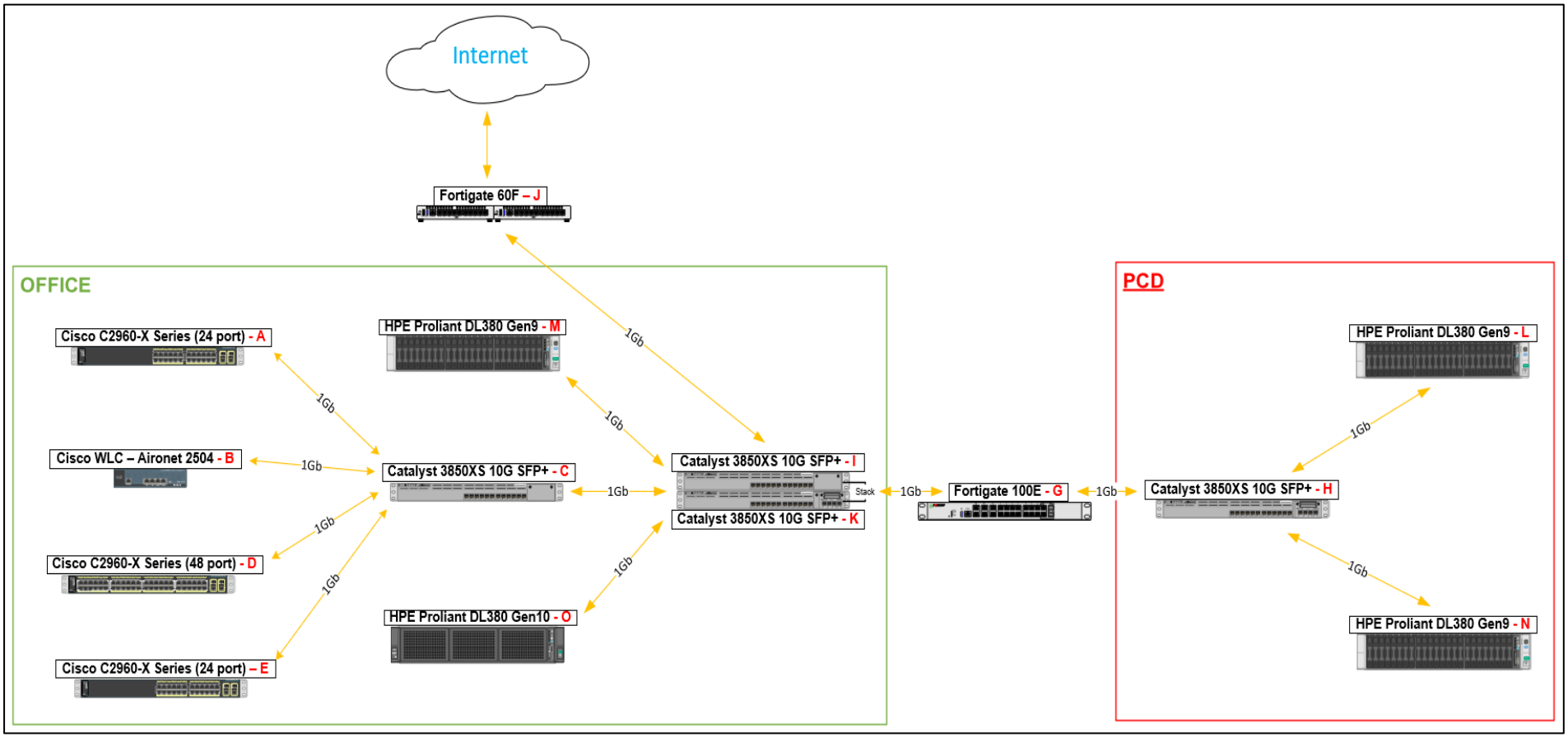


Figura 15: Interligação dos Equipamentos dos Racks. Fonte: Autor

As figuras 16 e 17 abaixo apresentam os sistemas operativos e máquinas virtuais que existem nos servidores que se encontram na infra-estrutura.

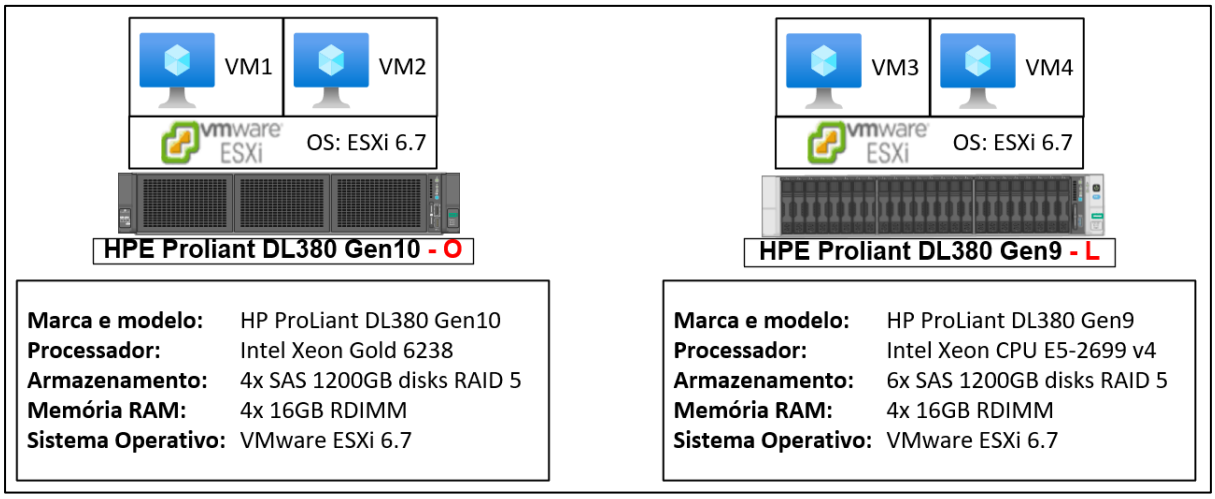


Figura 16: Relação Servidores (O, L) & Máquinas Virtuais existentes. Fonte: Autor

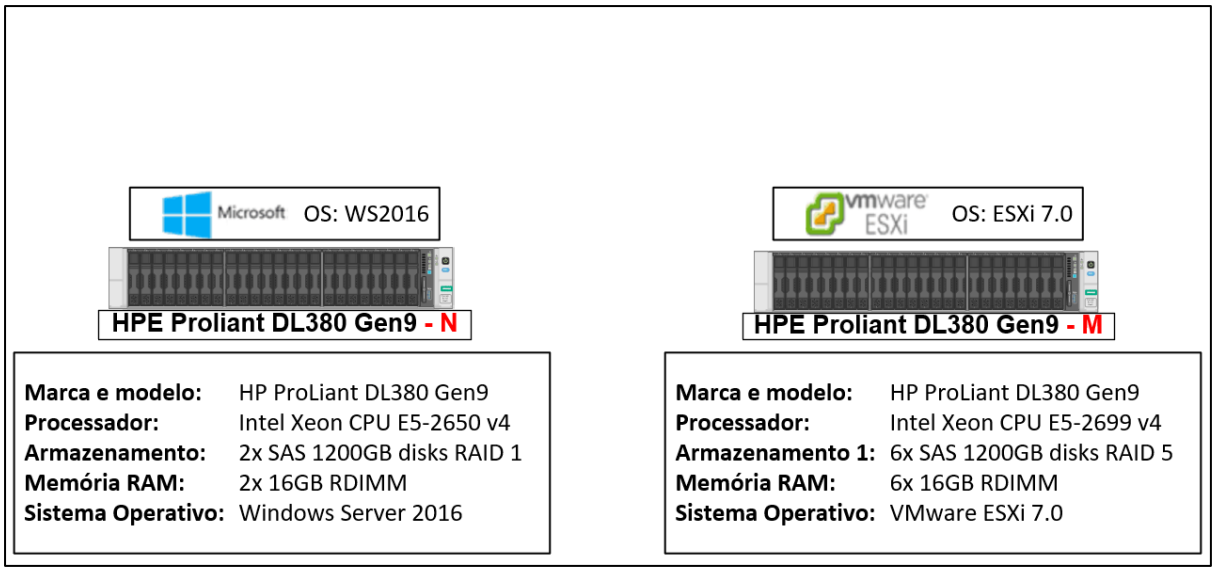


Figura 17: Relação Servidores (N, M) & Máquinas Virtuais existentes. Fonte: Autor

As Máquinas virtuais VM1, VM2, VM3 e VM4, vistas nas figuras acima, são máquinas virtuais que são de alta criticidade para o negócio. Abaixo estão descritas de forma breve as funções de cada uma delas na empresa:

- VM1 – Máquina virtual que contém aplicações & base de dados usadas pela equipa de Produção para descarregar selos que são usados nas garrafas de cerveja produzidas pela empresa. Esta VM está do lado do Office pois os

utilizadores finais precisam, a partir dos seus computadores, se conectam à ela;

- VM2 – Máquina virtual que contém aplicações & base de dados usadas pela equipa da Qualidade para manter registo de amostras. Esta VM está do lado do Office pois os utilizadores finais precisam, a partir dos seus computadores, se conectam à ela;
- VM3 – Máquina virtual que contém aplicações que são usadas em algumas impressoras especializadas (como a impressora de selos digitais), que se encontram nas linhas de produção. Esta VM está do lado do PCD pois a mesma precisa se ligar aos equipamentos encontrados na rede do PCD
- VM4 – Máquina virtual que contém aplicações que fazem backup das configurações existentes nos equipamentos (PLCs, impressoras, etc.) usados na área de produção. Esta VM está do lado do PCD pois a mesma precisa se ligar aos equipamentos encontrados na rede do PCD

Conforme ilustra a figura 17, no cenário actual, o servidor **HPE Proliant DL380 Gen9 – M** tem o **VMware ESXi 7.0U3** instalado, mas não possui nenhuma máquina virtual. Isto deve-se ao facto deste servidor ter sido no passado, usado para hospedar as máquinas virtuais do Office, mas após uma falha dos discos instalados no servidor, foi perdida a maior parte, se não toda, a informação que existia neste.

Durante o tempo em que este servidor esteve indisponível, devido à falha dos discos, foi usado o servidor **HPE Proliant DL380 Gen10 – O** para hospedar as VM do Office que tiveram de ser criadas e configuradas “de zero”.

Depois desse incidente, os discos foram repostos no servidor **HPE Proliant DL380 Gen9 – M** e foi reinstalado o **VMware ESXi 7.0 U3**.

A figura 17, também mostra que o servidor **HPE Proliant DL380 Gen9 – N** também não possui máquinas virtuais e nem o sistema operativo VMware ESXi, mas sim o sistema operativo Windows Server 2016 instalado. Neste servidor está instalado (no Windows) a aplicação BrewMaxx. Este sistema operativo e aplicação foram instalados neste servidor devido à problemas de performance (causados pela utilização do

disco) que eram enfrentavam no passado, quando este servidor era virtual (VM) e estava instalado no servidor **HPE Proliant DL380 Gen9 – L**.

4.2. Problema da Infra-estrutura Actual

Com os pontos apresentados e a ilustração das figuras 16 e 17 surge o problema de não existirem backups na actual infra-estrutura para quase todos estes sistemas.

Foi também verificado que existia uma vulnerabilidade na versão do VMware ESXi 6.7, conforme ilustrado por (VMWARE, 2021). Sendo que esta versão do VMware estava instalada em dois dos servidores da infra-estrutura e a solução recomendada pela equipa Global era de fazer upgrade para pelo menos a versão 7.0 actualizada.

As opções de upgrade disponíveis até à data eram o VMware ESXi 7 e VMware ESXi 8. Dos servidores que existiam na infra-estrutura, somente um é compatível com o VMware ESXi 8, que é o servidor **HPE Proliant DL380 Gen10 – O**. Os restantes servidores suportam até no máximo o VMware ESXi 7 (Ver Anexo 4).

5. CAPÍTULO V – PROPOSTA DE SOLUÇÃO

O presente capítulo irá descrever o processo da escolha e implementação dos problemas descritos em **4.2**, bem como as situações encontradas e aprendizado obtido durante o processo da escolha da solução. Por fim serão apresentados os resultados obtidos após a implementação e os benefícios que foram obtidos com a mesma

5.1. Cenário Pretendido

Como forma de introduzir um sistema de backups que actualmente não existe na infra-estrutura, os pontos a seguir descrevem os diferentes cenários desejados para a existência de backups.

5.1.1. Cenário 1: Usando recursos existentes

Fazendo o uso dos recursos actualmente existentes na infra-estrutura podemos ter um cenário onde o repositório para guardar as réplicas/backups, das máquinas virtuais que actualmente existentes tanto no PCD e do Office, seja o servidor **HPE Proliant DL380 Gen9 – M**.

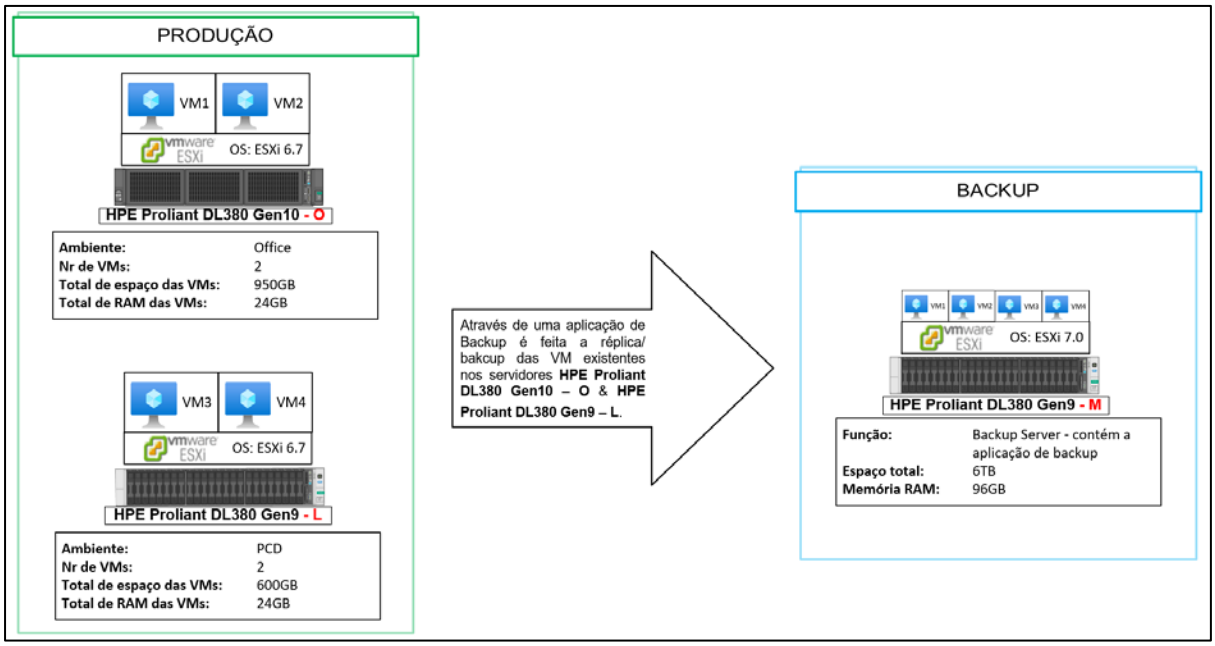


Figura 18: Cenário Pretendido para a existência de Backups. Fonte: Autor

A figura acima mostra um cenário onde poderemos fazer o backup das máquinas virtuais existentes nos servidores **HPE Proliant DL380 Gen9 - L** e **HPE Proliant DL380 Gen10 - O** para o servidor **HPE Proliant DL380 Gen9 – M** que actualmente não possui máquinas virtuais e não está em uso.

Optando por esta solução, haveria o problema de que no servidor de backups, teríamos no mesmo no mesmo Servidor ESXi, máquinas virtuais de ambientes diferentes, o que não deve acontecer pois a interface de gestão do servidor **HPE Proliant DL380 Gen9 – M** teria de estar ligada em apenas um dos switches de Core (que seria PCD ou Office). No caso de ligar-se esta interface à um dos switches teriam de ser abertas portas da firewall para passar o tráfego das máquinas virtuais do ambiente onde o Servidor onde o servidor de backup não estivesse fisicamente ligado o que traria ainda mais complexidade.

Outra preocupação que surgiu com essa ideia foi a longevidade desta solução. Após verificar o ciclo de vida dos produtos da VMware (ver figura 19 e 20), foi possível verificar que o fim do apoio geral (*End of General Support*) do VMware 7 ESXi termina em 2025, comparado com 2027 do VMware ESXi 8.

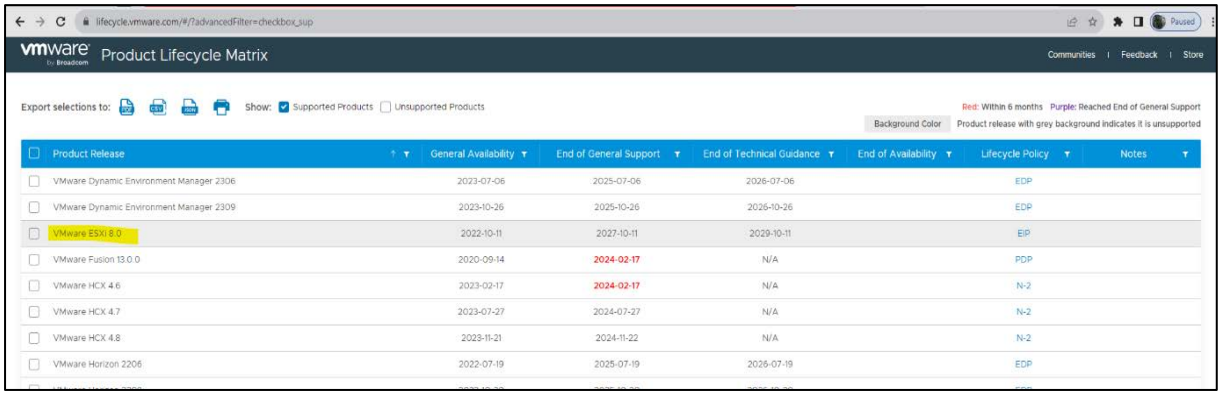


Figura 19: Matriz do Ciclo de Vida dos Produtos VMware. Fonte: VMware (2022)

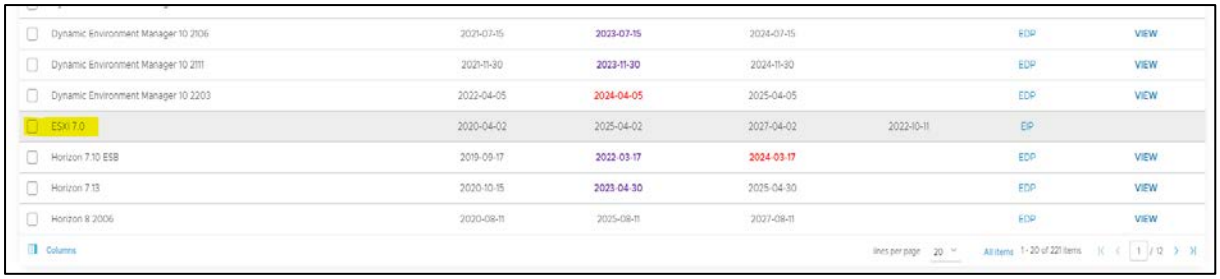


Figura 20: Matriz do Ciclo de Vida dos Produtos VMware. Fonte: VMWare (2022)

5.1.2. Cenário 2: Fazendo a aquisição de um novo servidor

Com estas observações, foi concluído que seria sensato e sairia em conta fazer o "refresh" do Servidor de ESXi do PCD para um novo que suporte o VMware ESXi 8. Foi constatado para um que suportasse o VMware ESXi 8. Com isto o PCD passaria a contar com dois (2) servidores e o Office também contaria com dois (2) servidores, sendo um destinado para a produção e o outro destinado para backup/réplica.

Pelo facto de não existir nenhuma réplica do servidor que tem a aplicação do BrewMaxx (**HPE Proliant DL380 Gen9 – N**), o ideal seria que o novo servidor ESXi do PCD tivesse ou usasse armazenamento baseado em flash, de forma a ter um backup deste servidor em forma virtual como houve no passado. Com este requisito, o problema de performance, mencionado no último parágrafo do **4.1.3**, seria ultrapassado.

Daí teríamos a aplicação BrewMaxx no servidor físico que está actualmente em funcionamento e também no novo servidor (em forma de VM). O servidor do BrewMaxx virtual por sua vez também terá um backup tal como as outras máquinas virtuais que estarão no novo servidor. Então no caso do servidor **HPE Proliant DL380 Gen9 – N** sofrer alguma falha, seria possível dar continuidade das operações com o servidor virtual. E com isso, teríamos um backup completo da infra-estrutura.

Assim o cenário pretendido passa ter a estrutura apresentada na figura 21.

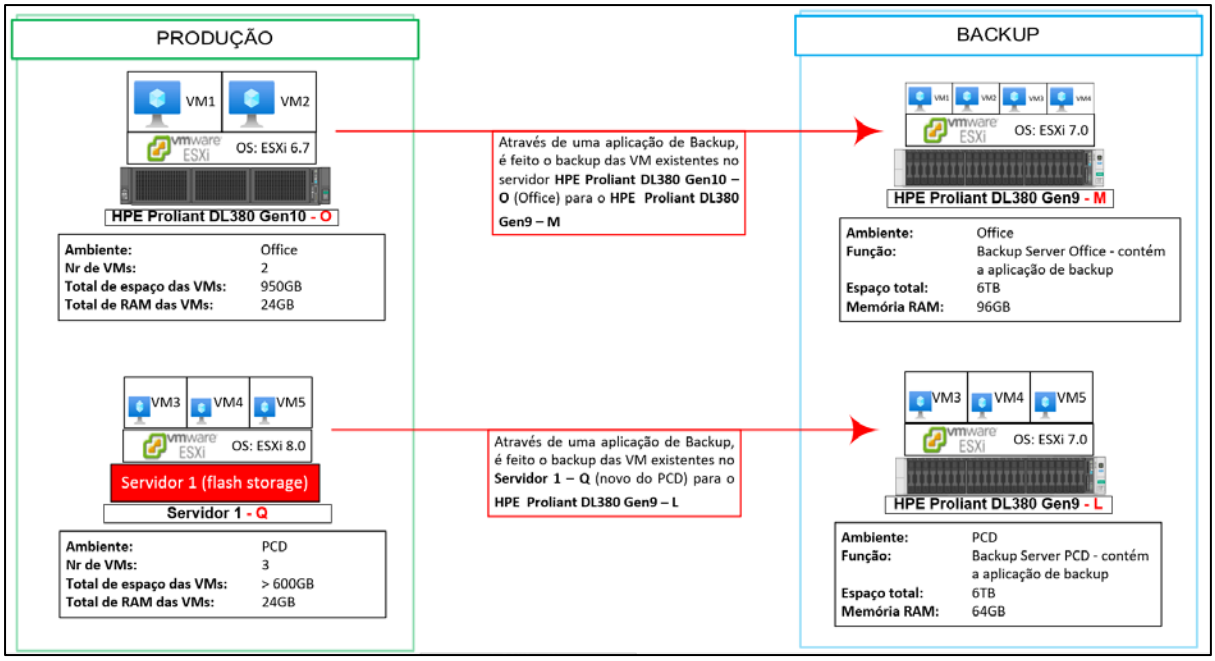


Figura 21: Cenário Pretendido para a existência de Backups com novo servidor do PCD. Fonte: Autor

Da figura acima podemos observar que no servidor o PCD (**Servidor 1 – Q**) passará a contar com uma quinta máquina virtual (VM5), que será a VM de backup do BrewMaxx que actualmente corre no servidor **HPE Proliant DL380 Gen9 – N**. A actividade da criação do servidor (VM5) do BrewMaxx foi uma acção que corria em paralelo enquanto eram discutidas as opções do melhor cenário para a implementação do sistema de backups.

Após algumas sessões de discussão em torno do tópico dos backups com o Gestor do D&T, o mesmo informou que para além do novo servidor para o PCD, existe a possibilidade de comprar mais um servidor. O Gestor do D&T também informou que os servidores **HPE Proliant DL380 Gen9 – L** (actual ESXi do PCD) e **HPE Proliant DL380 Gen9 – M** (actualmente sem nada, mas destinado aos backups do Office) deverão futuramente ser usados para um *site* de Recuperação de Desastres (*Disaster Recovery* – DR).

Com esta nova directriz surgiu a seguinte questão, como garantir que haja backups do PCD e do Office, sendo que os servidores **HPE Proliant DL380 Gen9 – L** e **HPE Proliant DL380 Gen9 - M** serão usados no DR *site*?

5.1.3. Cenário 3: Fazendo a aquisição de dois novos servidores e usando outros recursos existentes

Sendo que a operacionalização do DR implicaria mais custos no meio do actual projecto, foi então olhado para os recursos que até agora fariam parte da solução (excluindo os servidores que farão parte do DR) e alguns itens que existiam em stock e que não estavam em uso. Dos itens em stock, os itens que seriam de grande utilidade para este novo cenário são:

- Um disco duro (HDD) externo de dez (10) TB da marca Seagate Backup Plus Hub
- Um sistema de backup em fita (*Tape Library*) da marca HP StorageWorks 1/8 G2 Tape AutoLoader – LTO 7 (com interface SAS) & tapes.
- Dois discos duro SAS 300GB (para servidores)
- Dois discos duro SAS s1200GB (para servidores)

Com todos estes itens e os que se pretende fazer a aquisição e os itens em stock, o cenário pretendido passou do ilustrado na figura 21 para a figura abaixo, onde poderemos então ter o sistema de backup robusto e a possibilidade de fazer o DR *site* com os servidores **HPE Proliant DL380 Gen9 – L** e **HPE Proliant DL380 Gen9 – M**.

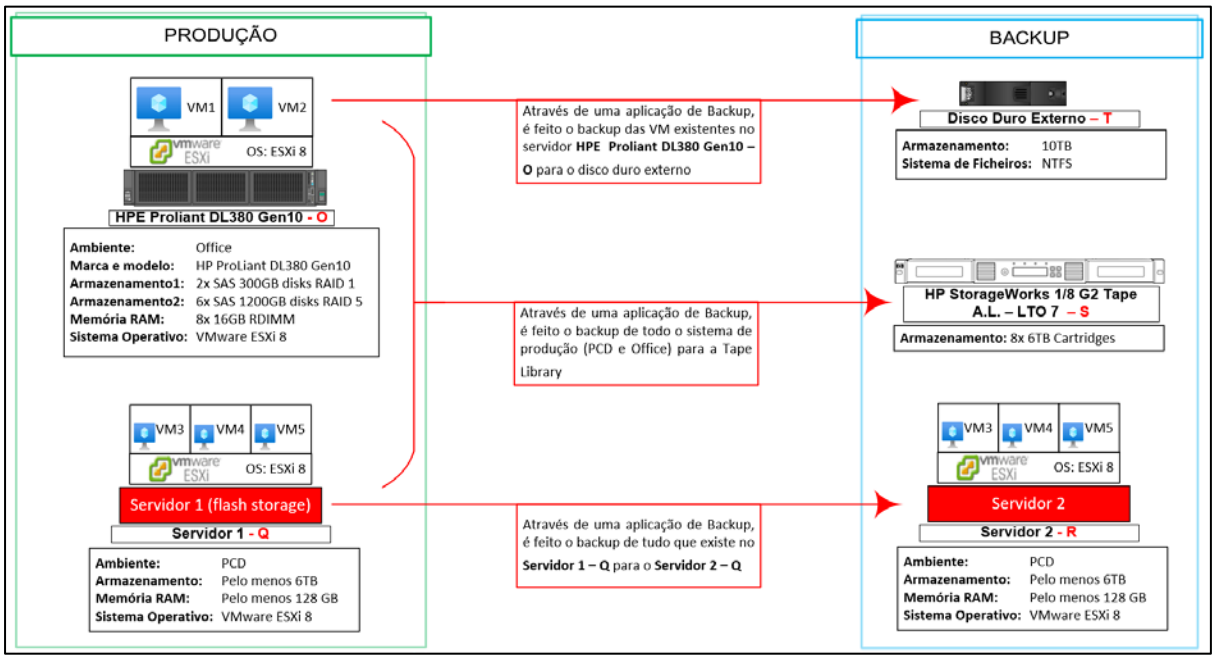


Figura 22: Cenário pretendido mais robusto para a existência de Backups. Fonte: Autor

Da figura acima, para além de observar que os servidores que irão para o DR site saíram da actual solução, e podemos também verificar que o servidor o servidor **HPE Proliant DL380 Gen10 – O** terá um aumento da memória RAM e dos discos. Isto porque futuramente poderá haver a necessidade de aumentar a capacidade das actuais máquinas virtuais ou então o número de máquinas virtuais neste ambiente poderá crescer.

Durante as sessões de discussão, ficou decido que o ambiente do PCD (mais crítico) deve ter uma réplica que pode ser usada para correr os sistemas, pois a paragem de mais de 10 minutos dos sistemas do PCD tem grandes impactos na produção e consequentemente no negócio. Daí que ter uma réplica deste ambiente será de grande vantagem pois irá reduzir o tempo de paragem (*downtime*) significativamente, pois no caso da avaria do servidor principal (**Servidor 1 – Q**) o servidor com a réplica (**Servidor 2 – R**) poderá ser usado para dar continuidade das operações.

Quando comparado com os sistemas do PCD, os sistemas do Office podem ter um *downtime* maior, daí que para o âmbito deste projecto, a existência do backup (para o disco duro externo) ilustrado na figura é minimamente satisfatória pois os sistemas poderão ser repostos a partir dos backups (do disco duro externo).

A figura também mostra que ambos ambientes passarão a ter como backup também, o sistema de tapes (*Tape Library*).

5.2. Selecção da melhor solução e implementação

O cenário apresentado em **5.1.3** mostrou ser o de maior robustez pois garante a existência de pelo menos duas copias de todas máquinas virtuais existentes na infra-estrutura, sem contar que após o comissionamento do DR site irá garantir uma terceira cópia. Para além disso, existem recursos disponíveis para a materialização do cenário proposto. Dito isso, ficou então decido que o cenário apresentado em **5.1.3** seria implementado.

Foi então lançado um concurso público onde as empresas concorrentes teriam de apresentar uma solução para os requisitos apresentados no Anexo 2. Nesta solução deveria estar incluso o fornecimento, configuração e instalação de dois servidores, licenças para o VMware 8 para os servidores que estarão na infra-estrutura principal e um software de backup.

Para esta este projecto, foi escolhido como aplicação de backup, a solução da Veeam pois, aquando da realização deste projecto, o grupo HEINEKEN estava no processo de celebração de um contracto com a empresa (Veeam) e após o término desta, o grupo passaria a dispor de descontos nas renovações das licenças que fossem feitas pelas OpCos. Mas pelo facto do contracto não ter sido concluído, foi colocado nos requisitos o fornecimento da licença do *Veeam Backup & Replication*, para que a empresa adjudicada fornecesse.

Após receber as propostas recolhidas pelo departamento de Procurement, juntamente com o Gestor do D&T, foi feita a análise das propostas técnicas e financeiras de três (3) empresas que concorreram para o fornecimento dos equipamentos e serviços solicitados.

Das empresas concorrentes, a empresa vencedora não só apresentou uma solução que se adequa aos requisitos, mas também foi a empresa com o menor custo comparado com as outras.

A proposta apresentada pela empresa continha o fornecimento dos seguintes itens para além da configuração de alguns dos equipamentos:

- **Servidor 1, com as especificações:**
  - Marca e modelo: Dell PowerEdge R750 Server (2.5"Chassis)
  - CPU: Intel Xeon Silver 4314
  - RAM: 8 x 32GB RDIMM
  - Armazenamento 1: 2x M.2 240GB (RAID 1)
  - Armazenamento 2: 1x 600GB HDD SAS 12Gb (No RAID)

- **Servidor 2, com as especificações:**
  - Marca e modelo: Dell PowerEdge R750 Server (3.5"Chassis)
  - CPU: Intel Xeon Silver 4314
  - RAM: 8 x 32GB RDIMM
  - Armazenamento 1: 2x M.2 480GB (RAID 1)
  - Armazenamento 2: 5x 2TB HDD SAS 12Gbs (RAID 5)
- **Storage Server, com as especificações:**
  - Marca e modelo: Dell Unity XT 380F (25 x 2.5")
  - Armazenamento: 12 x 1.92TB SSD
- **Veeam Data Platform Universal Subscription**
  - Duração: Um ano
- **VMware vSphere 8 Essentials Plus Kit for 3 hosts**
  - Duração: Um ano

A empresa propôs um cronograma onde existiam as datas para as entregas dos itens acima descritos (ver Anexo 1). Com o cronograma partilhado pela empresa e tendo observado as actividades que recaíam sobre a nossa responsabilidade, foi necessário dividir o andamento do projecto em 4 fases.

5.2.1. FASE 1 – Preparação da infra-estrutura

Durante o tempo de espera dos equipamentos, foi a mim incumbida a tarefa de deixar o servidor **HPE Proliant DL380 Gen10 – O** (que nessa época era usado para as máquinas virtuais do Office) pronto para a reinstalação do VMware ESXi 8. Esta tarefa consistia em garantir que as máquinas virtuais que estavam neste servidor passassem com sucesso para o servidor **HPE Proliant DL380 Gen9 – M** (que na época não tinha nenhuma máquina virtual e tinha o VMware ESXi 7.0 instalado – a última versão suportada por este servidor).

A forma recomendada pela VMware para a transferência de máquinas virtuais entre servidores (*Hosts*) que não compartilhem o mesmo esspaço de armazenamento e também não estejam vinculados à um VMware vCenter, que era o caso, é através da exportação da máquina virtual para um ficheiro OVF (*Open Virtualization Format*) e

de seguida a implantação (*deployment*) do OVF no servidor (*Host*) de destino (VMWARE, 2020).

Esta opção não foi escolhida pois requer a existência de espaço livre disponível no computador usado para se conectar aos servidores/hosts envolvidos. Após algumas consultas na internet, de formas alternativas para realizar a transferência, foi possível aprender que é possível copiar máquinas virtuais entre hosts directamente a partir da rede, usando o comando “SCP” (Secure Copy) que é um utilitário de linha de comandos que lhe permite copiar ficheiros e directórios de forma segura entre duas localizações, conforme explicado no artigo de (Rodgers, 2021).

Usando qualquer uma das alternativas, é imperioso que todas as máquinas virtuais estejam desligadas, foi então necessário pedir um tempo de paragem (*downtime*), de 4h para cada uma das máquinas virtuais existentes nos hosts, aos gestores das áreas nas quais são usadas as máquinas virtuais em questão. Após ter sido aprovado o pedido de *downtime*, foi então colocado em prática o conhecimento recém aprendido, sobre o SCP, e dessa forma realizando a cópia das máquinas virtuais do servidor **HPE Proliant DL380 Gen10 – O** para o servidor **HPE Proliant DL380 Gen9 – M**.

Depois de garantir que a migração correu com sucesso, foi dado um período para que os utilizadores fizessem testes para garantir que todos os serviços estavam a correr plenamente, a partir do servidor **HPE Proliant DL380 Gen9 – M**. Depois de ser tido garantido que todos os serviços estava a correr correctamente, foram então feitas as modificações no servidor **HPE Proliant DL380 Gen10 – O**, que consistiram em:

1. Colocar os discos que estavam em stock neste servidor, deixando a configuração:
    a. 2x 300GB SAS (HDD) – colocado em RAID 1 para ser instalado o sistema operativo
    b. 2x 1200GB SAS (HDD) – colocado no servidor, que previamente tinha somente 4x 1200GB SAS (HDD). Com esta adição de discos foi criado drive lógico em RAID 5, que seria o *datastore* onde ficarão as máquinas virtuais e outros dados deste servidor.
2. Remover memórias 4x 16GB de módulos de memória RAM, do servidor **HPE Proliant DL380 Gen9 – L**, de modo a deixar o actual servidor com 128GB de memória RAM.

Após a modificação das especificações do servidor, foi instalado o VMware ESXi 8 no mesmo. E aguardava-se a chegada dos equipamentos que iriam albergar as máquinas virtuais do ambiente PCD.

5.2.2. FASE 2 – Montagem e ligação dos equipamentos à infra-estrutura

Depois da chegada dos equipamentos na fábrica, a equipa fez a montagem dos servidores no Rack (ver Anexo 7). De salientar que a maior parte dos equipamentos chegou pré-configurado, graças ao pedido da partilha antecipada (por parte da empresa adjudicada) de detalhes, como endereçamento IP, *hostnames*, VLAN, etc., que foram necessários durante a configuração dos servidores enquanto ainda estavam no *workshop* da empresa adjudicada.

Por volta do mesmo tempo já havia sido instalada a máquina virtual para o BrewMaxx, mas a mesma estava em fase de testes pela equipa da Produção. Por este motivo o servidor físico (HPE Proliant DL380 Gen9 - N) continuava ligado à infra-estrutura e como o servidor principal da aplicação.

A montagem dos equipamentos foi feita no rack a estrutura passou a contar com os os equipamentos vistos na figura a seguir.

Disposição dos equipamentos no Rack 2 (Servers) após a montam dos novos equipamentos

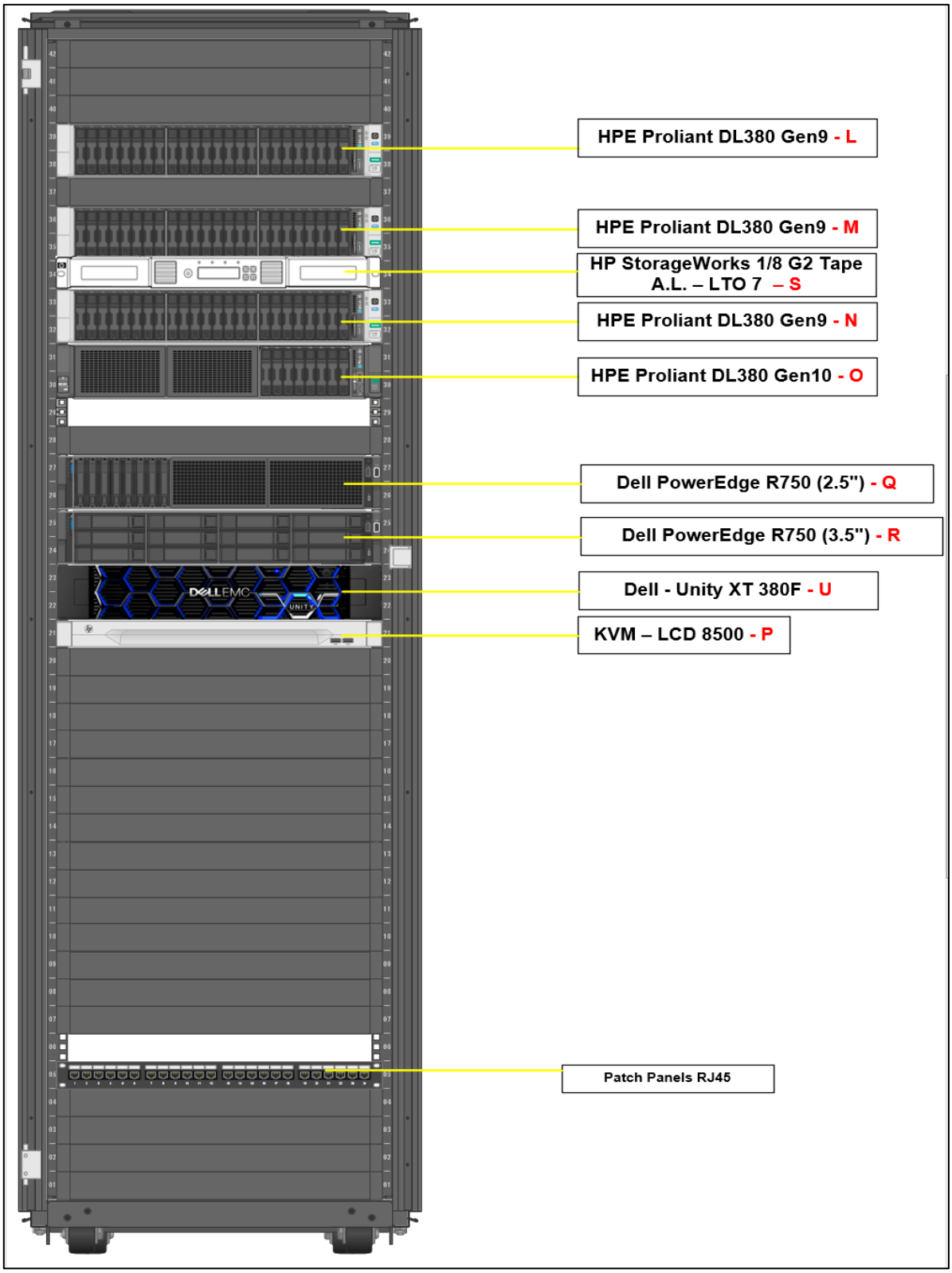


Figura 23: Disposição dos dispositivos no Rack 2 (Servers) após a chegada dos equipamentos - Fonte: Autor

A tabela abaixo descreve a legenda da figura anterior, mencionando a função dos itens encontrados no rack:

Item	Descrição	Função/Papel
HPE Proliant DL380 Gen9 – L	Servidor com VMware ESXi 6.7U3 – PCD	Desligado – Por ser usado no DR site
HPE Proliant DL380 Gen9 – M	Servidor com VMware ESXi 7.0U3 – Office	Desligado – Por ser usado no DR site
HPE Proliant DL380 Gen9 – N	Servidor com o Software BrewMaxx	Contém a aplicação BrewMaxx
HPE Proliant DL380 Gen10 – O	Servidor com VMware ESXi 8.0U2 – Office	Hospeda as VMs do ambiente do Office Host
Dell PowerEdge R750 (2.5") - Q	Servidor com VMware ESXi 8.0 U2 – Server principal do PCD	Contém os recursos de computação das VMs do ambiente do PCD
Dell PowerEdge R750 (3.5") – R	Servidor com VMware ESXi 8.0 U2 – PCD – Server secundário do PCD	Contém a réplica das VM que correm no servidor Dell PowerEdge R750 (2.5") - Q
HP StorageWorks 1/8 G2 Tape A.L. – LTO 7 – S	Tape Library/Sistema de backup em fita	Mantém os backups das VMs do PCD e do Office
Dell - Unity XT 380F - U	Storage do PCD	Contém os recursos de armazenamento das VM que correm no servidor Dell PowerEdge R750 (2.5") - Q

Tabela 5: Legenda dos equipamentos do Rack 2 (Servers) após a chegada dos novos equipamentos - Fonte: Autor

Da unidade Dell - Unity XT 380F – U foram retirados dois discos para ter como *spares* (sobra) e com os remanescentes discos criou-se um *storage pool* de aproximadamente quinze (15) terabytes (TB). Dos quinze (15) TB, dez (10) TB são destinados para o backup e cinco para o armazenamento das máquinas virtuais em serviço (ver Anexo 10).

O passo a seguir foi então ligar os equipamentos à rede onde no final a interligação dos equipamentos ficou com a seguinte estrutura:

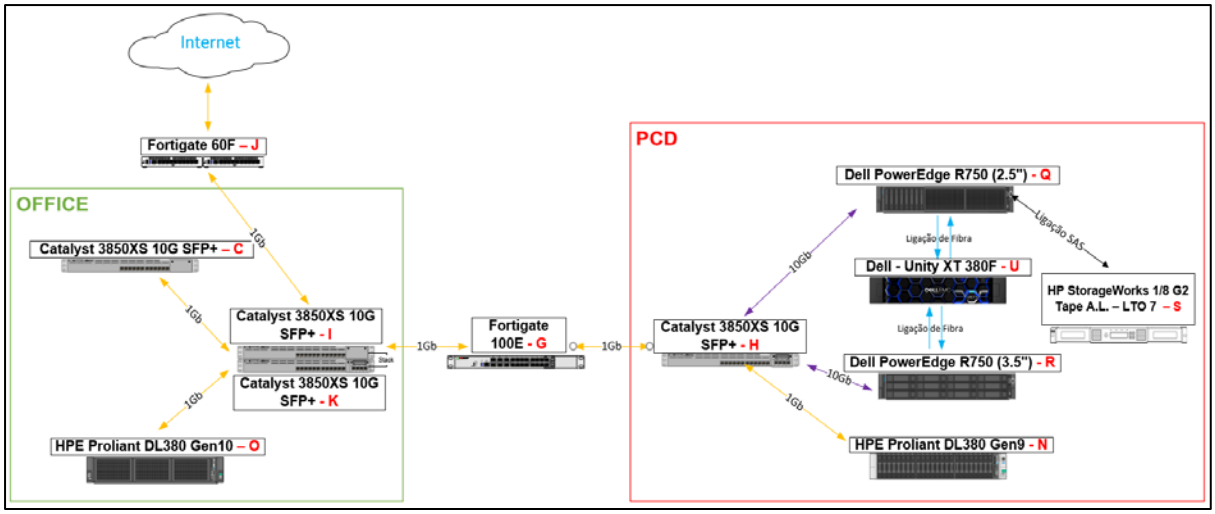


Figura 24: Interligação dos Equipamentos dos Racks após a chegada dos novos equipamentos. Fonte: Autor

5.2.3. FASE 3 – Instalação e configuração

Na figura 24 vemos que as ligações para o servidor de armazenamento (*storage*) estão ligados directamente por fibra aos dois novos servidores. A ligação do Tape Library é directamente ligada ao Servidor **Dell PowerEdge R750 (2.5") – Q**, usando um cabo SAS. Isto porque a máquina virtual onde está a aplicação de backup (Veeam) ter sido instalada neste servidor, e é na aplicação de backup onde será configurada a conexão com o *Tape Library*.

Depois de ser garantido o funcionamento das ligações recém feitas, o passo a seguir foi a instalação do vCenter (que está incluso na licença *VMware vSphere 8 Essentials Plus Kit for 3 hosts*) foi por nós decidido que deveria ser instalado no servidor principal do PCD (**Dell PowerEdge R750 (2.5") – Q**). A equipa da empresa adjudicada conseguiu realizar a instalação com sucesso, usando informações previamente fornecidas para o efeito.

De seguida se procedeu com a integração dos 3 *hosts* (**Dell PowerEdge R750 (2.5") – Q**, **Dell PowerEdge R750 (3.5") – R** e **HPE Proliant DL380 Gen10 - O**) ao vCenter, seguido do licenciamento dos mesmos através do vCenter.

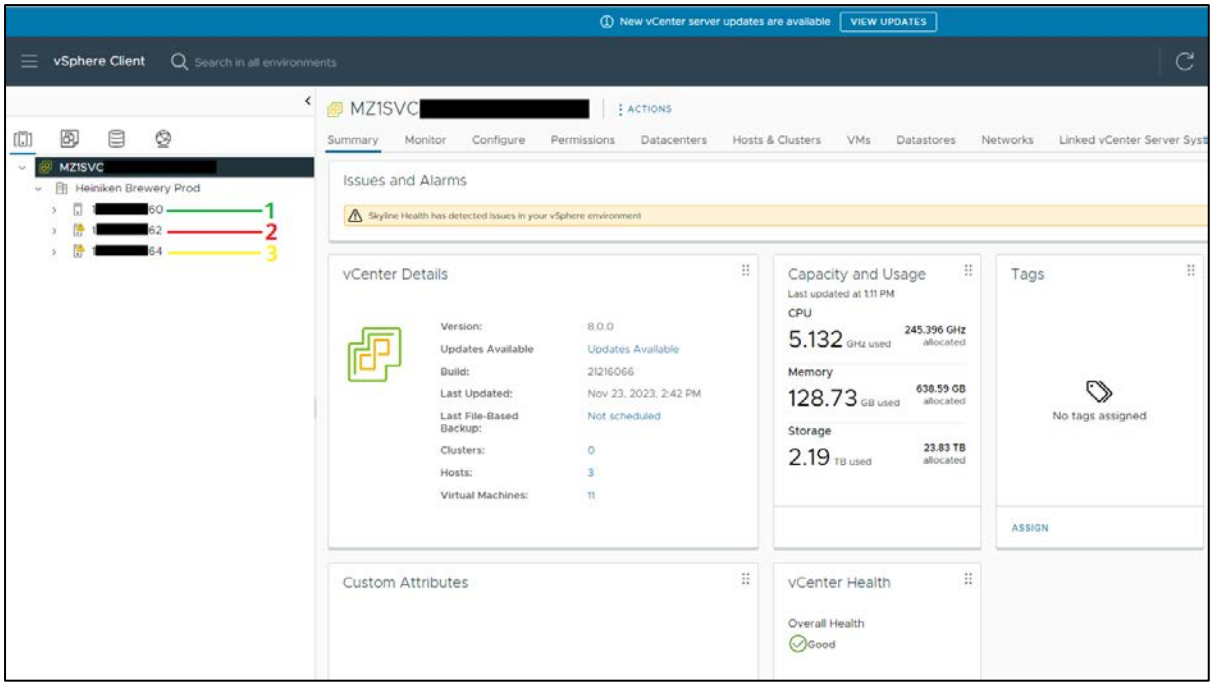


Figura 25: 3 servidores integrados ao virtual datacenter do vCenter. Fonte: Autor

Legenda

1. **HPE Proliant DL380 Gen10 – O**
2. **Dell PowerEdge R750 (2.5") – Q**
3. **Dell PowerEdge R750 (3.5") – R**

O passo a seguir foi criar uma VM onde foi de seguida instalada a aplicação de backup, Veeam Backup & Replication. Depois de ser instalada a aplicação, foi feita a conexão entre a aplicação de backup e o vCenter previamente instalado. Com esta conexão integração, a aplicação Veeam Backup & Replication Console já tinha visibilidade de todos os *hosts* que existiam na infra-estrutura e consequentemente as máquinas virtuais existentes nos *hosts*.

Depois desta integração, o passo a seguir foi de garantir que as máquinas virtuais que até então estavam no momento a correr a partir dos servidores **HPE Proliant DL380 Gen9 – M** e **HPE Proliant DL380 Gen9 – L** passassem para a nova infra-estrutura, nos servidores **HPE Proliant DL380 Gen10 – O** e **Dell PowerEdge R750 (2.5") – Q** respectivamente.

Para este efeito foi usada a funcionalidade de *Replicação* da aplicação VEEAM Backup & Replication Console que consistiu em:

a. **Adição dos hosts na Infra-estrutura virtual do Veeam:**

Na Interface da aplicação, navegou-se para o **Inventory** > **Virtual Infrastructure** > **VMware vSphere** > **Standalone Hosts**, onde fez a adição dos *hosts standalone* (**HPE Proliant DL380 Gen9 - M** e **HPE Proliant DL380 Gen9 - L**)

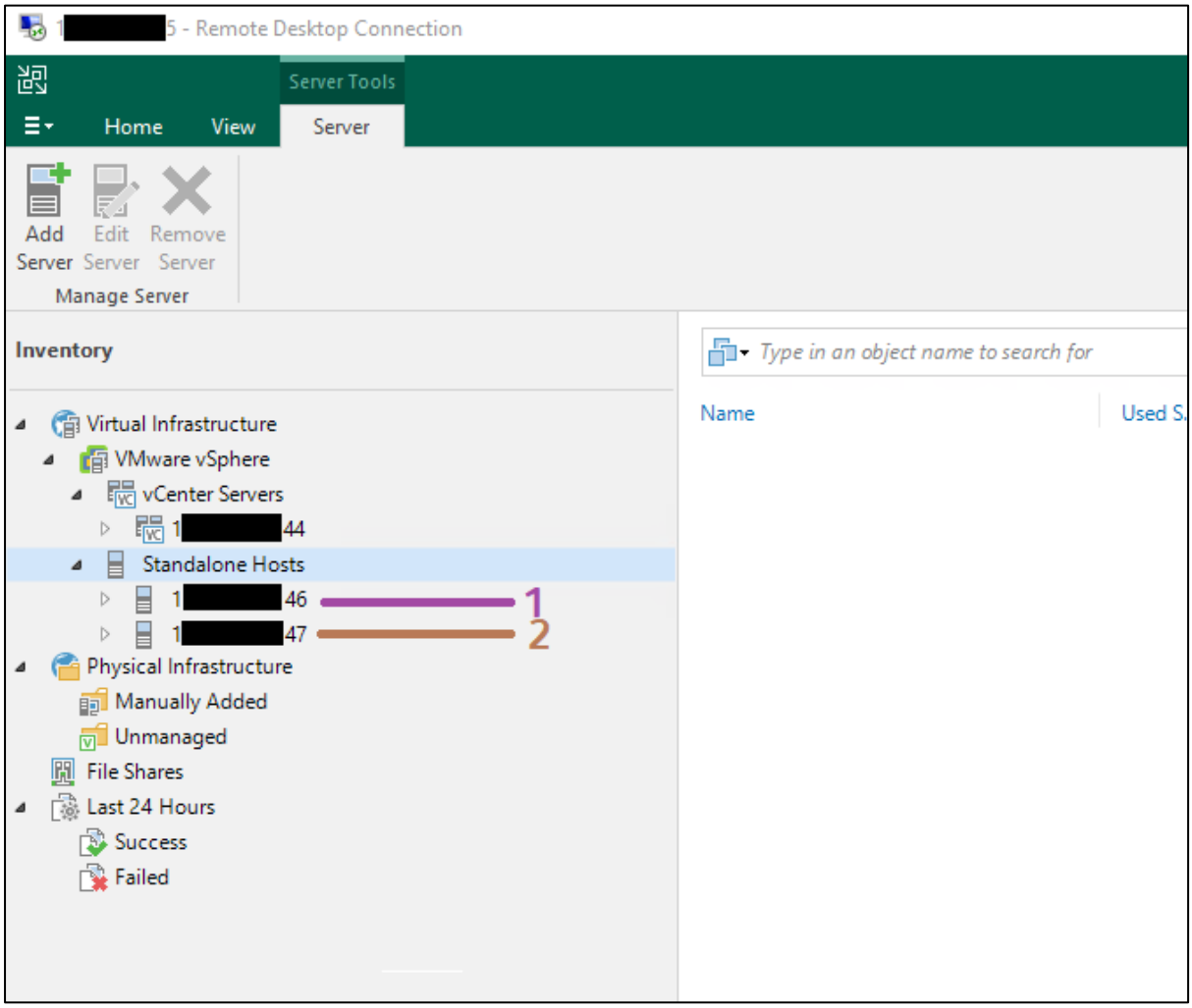


Figura 26: Hosts Standalone do PCD e do Office adicionados no Veeam B&R Console. Fonte: Autor

Legenda

1. **HPE Proliant DL380 Gen9 - M**
2. **HPE Proliant DL380 Gen9 - L**

Depois de serem adicionados os servidores foi possível ter, a partir da aplicação, visibilidade das máquinas virtuais existentes nos hosts, a partir da aplicação de backup.

b. Replicação das máquinas virtuais, dos servidores standalone para os servidores integrados no vCenter

Na Interface da aplicação, navegou-se para o **Home** > **Jobs** > **Replication**, onde fez a adição de tarefas de replicação (*Replication Jobs*) que tivessem como finalidade a concretização do cenário descrito no ambiente da *Produção* da figura 22.

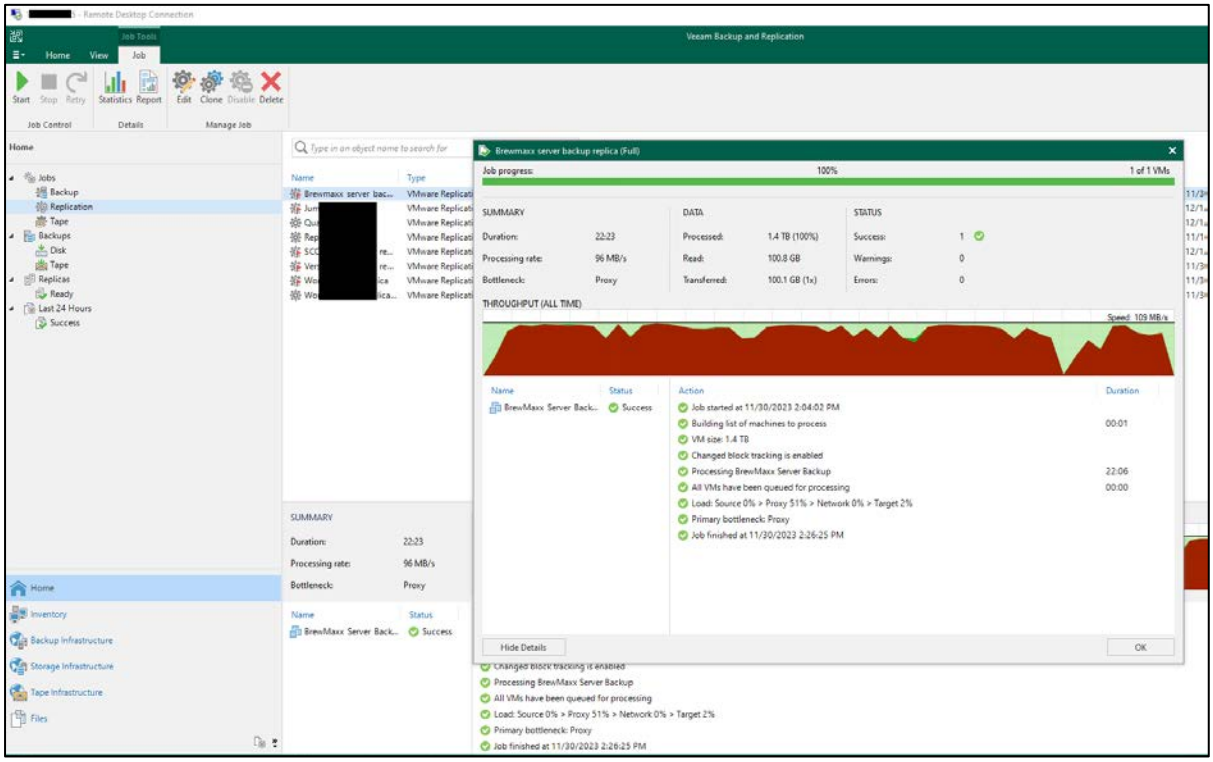


FIgura 27: Conclusão da tarefa de replicação do servidor (virtual) do BrewMaxx. Fonte: Autor

Adicionalmente foram configurados outros aspectos da aplicação de backup como por exemplo os alertas por email e os repositórios de backup que consistem dos dispositivos vistos na figura 23. Dos dispositivos que fazem parte do repositório, a tape library (HP StorageWorks 1/8 G2 Tape AutoLoader - LTO 7 – S) também faz parte, mas o mesmo se encontra numa outra secção da aplicação, quando comparado com os outros tipos de armazenamento presentes na solução.

Conforme ilustra a figura abaixo, na aplicação de backup a tape library pode ser vista nas livrarias (Libraries) da secção *Tape Infrastructure* da aplicação de backup (ver figura 28).

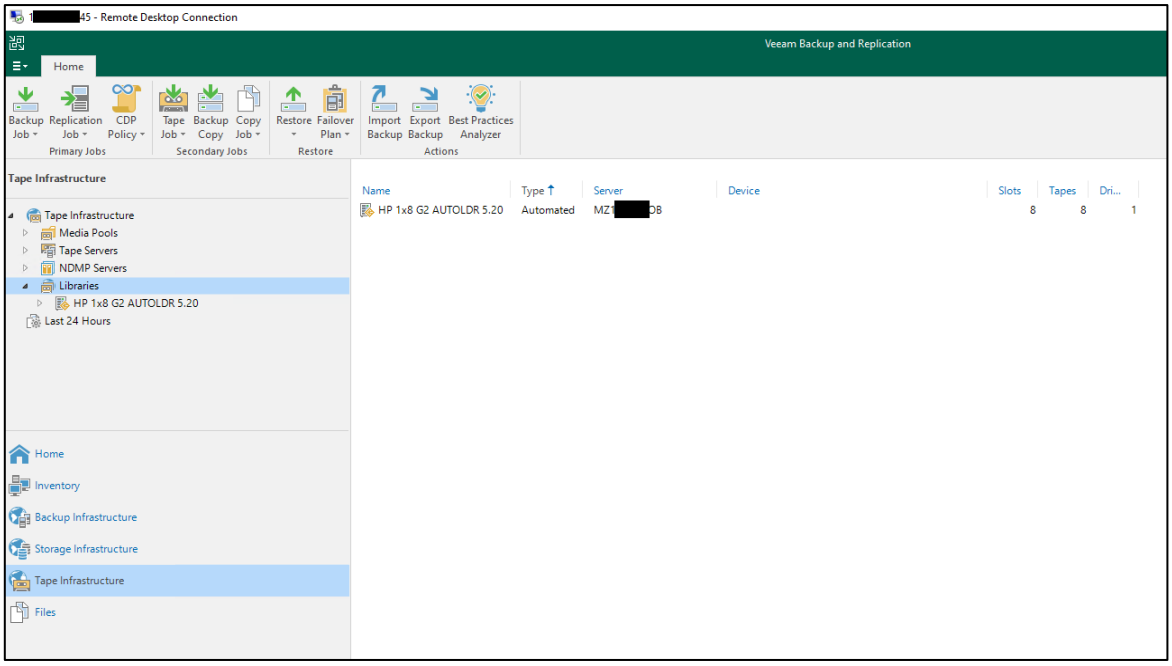


Figura 28: Ilustração do Autoloader na infraestrutura do Veaam B.&R. Console

O Anexo 5 mostra as máquinas virtuais enquanto corriam a partir do servidor **HPE Proliant DL380 Gen9 - L**. A figura abaixo mostra as mesmas máquinas virtuais enquanto correm na nova infra-estrutura, onde estas já se encontram no servidor **Dell PowerEdge R750 (2.5") – Q**.

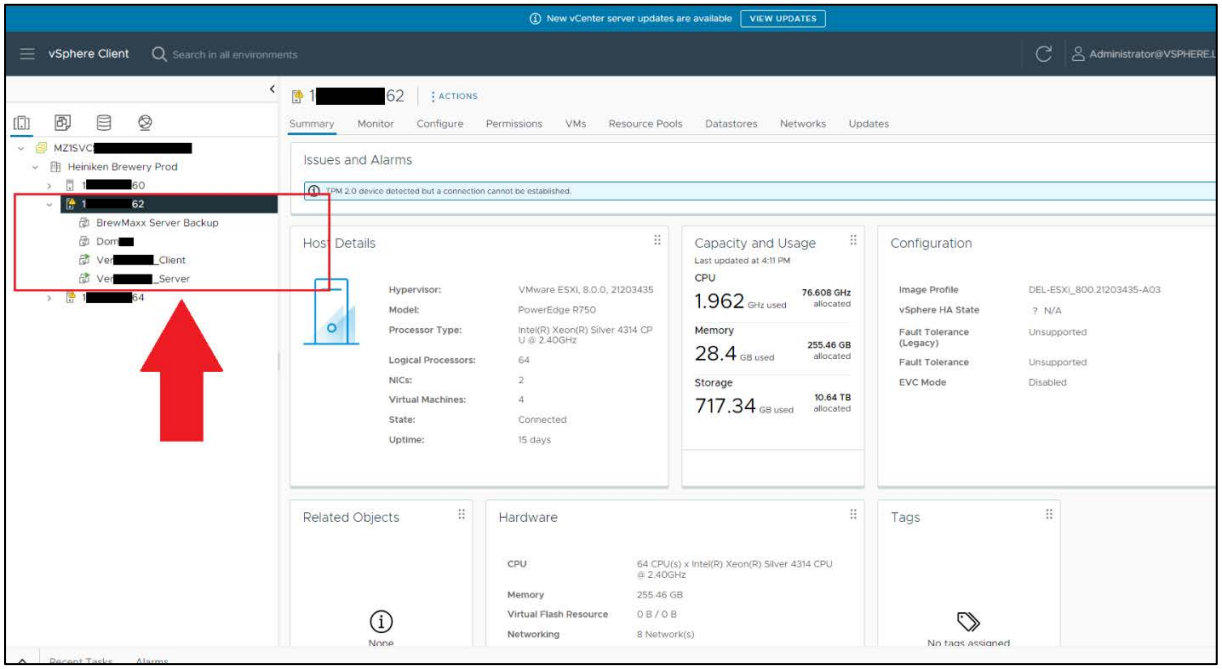


Figura 29: Máquinas virtuais correndo no novo host. Fonte: Autor

Com isto, foi dada como terminada a tarefa de passagem das máquinas virtuais dos servidores standalone para a os servidores integrados ao vCenter, podendo então deixar os servidores standalone prontos para futura infra-estrutura do DR site.

5.2.4. FASE 4 – Configuração dos backups e execução dos backups

Tendo assim os novos dispositivos integrados na infra-estrutura e os dispositivos destinados ao DR desconectados (conforme ilustra o cenário da figura 24) o passo a seguir foi de configurar a aplicação de backup tendo em conta os dispositivos actualmente ligados.

Visto que o vCenter tem a visibilidade de todos os hosts e máquinas virtuais que estão na infra-estrutura, e o vCenter por sua vez está interligado à aplicação de backup, dando visibilidade das máquinas virtuais que farão parte do backup, a figura 30 ilustra a forma como serão feitos os backups na aplicação.

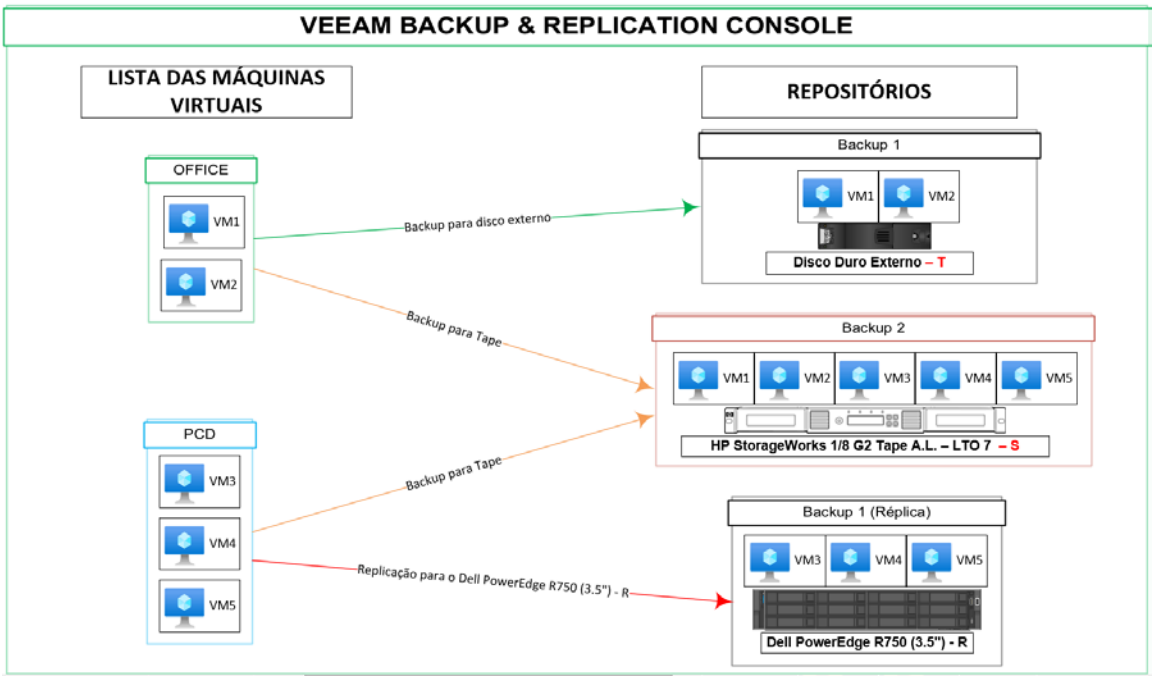


Figura 30: Topologia de backups da infra-estrutura. Fonte: Autor

De forma a tornar este cenário uma realidade, foram configuradas na aplicação Veeam Backup & Replication Console as tarefas de backup (backup jobs). Este passo não diferiu muito da tarefa de replicação, sendo que para esta actividade foi usada a Tabela 6 como base para serem agendados os backups.

VM	Tipo de backup	Retenção	Frequência	Repositório
VM1	Full	60 dias	Mensal	Disco Duro Externo – T
VM1	Full	365 dias	Mensal	Tape Library
VM1	Incremental	15 dias	Diário	Disco Duro Externo – T
VM2	Full	60 dias	Mensal	Disco Duro Externo – T
VM2	Full	365 dias	Mensal	Tape Library
VM2	Incremental	15 dias	Diário	Disco Duro Externo – T
VM3	Full	365 dias	Mensal	Tape Library
VM3	Réplica	n/a	Diário	Dell PowerEdge R750 (3.5") - R
VM4	Full	365 dias	Mensal	Tape Library
VM4	Réplica	n/a	Diário	Dell PowerEdge R750 (3.5") - R
VM5	Full	365 dias	Mensal	Tape Library
VM5	Réplica	n/a	Diário	Dell PowerEdge R750 (3.5") - R

Tabela 6: Modalidade de backup. Fonte: Autor

De salientar que esta tabela foi elaborada de acordo com a criticidade dos servidores e a quantidade de alterações que ocorrem diariamente.

Na figura 31 temos um exemplo de três trabalhos de backup que foram agendados (linhas 2, 6 e 7, pintados de amarelo na segunda coluna) para que corresse diariamente, na hora descrita na coluna *Next Run*, de acordo com a tabela 6 acima.

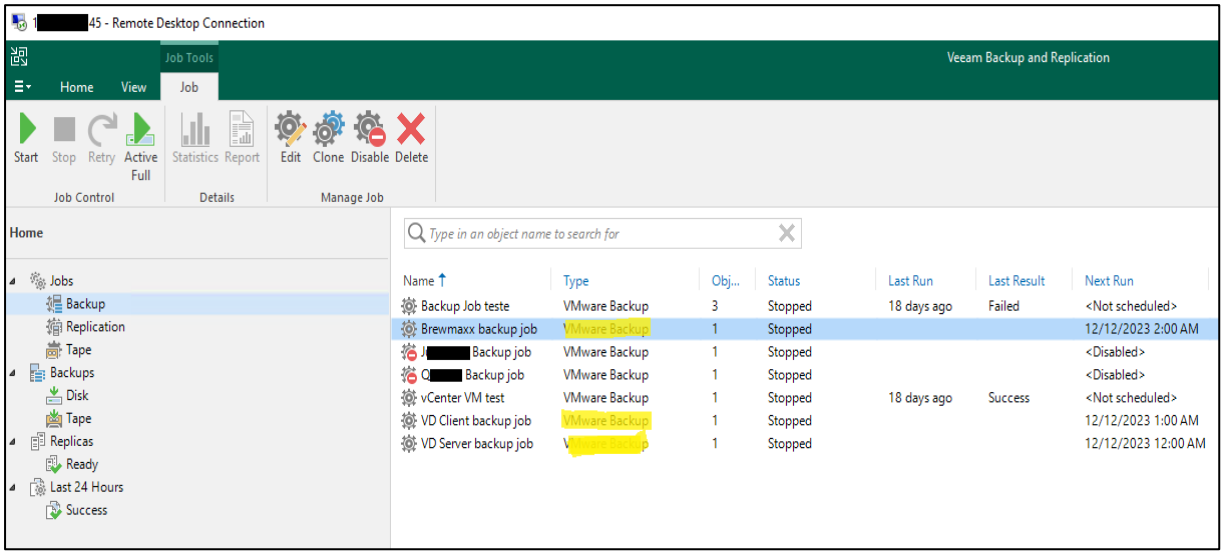


Figura 31: Backups agendados no Veeam B.&R. Console - antes de ser executado. Fonte: Autor

A figura 32 abaixo ilustra, em forma de exemplo, uma das tarefas de backup anteriormente agendadas depois de ter corrido com sucesso na hora agendada.

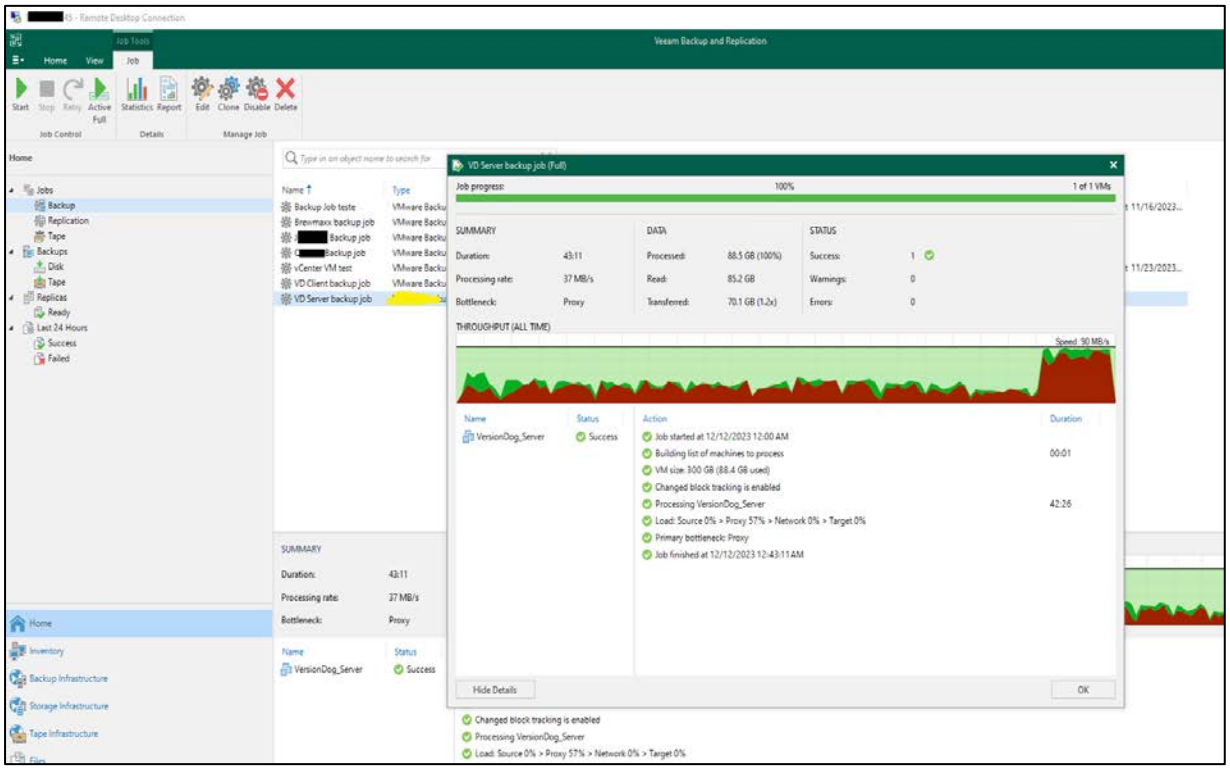


Figura 32: Trabalho de backup terminado com sucesso. Fonte: Autor

Adicionalmente os alertas por email também estão completamente funcionais conforme visto nas figuras 33 e 34, onde o segundo foi feito com sucesso para o sistema de tapes.

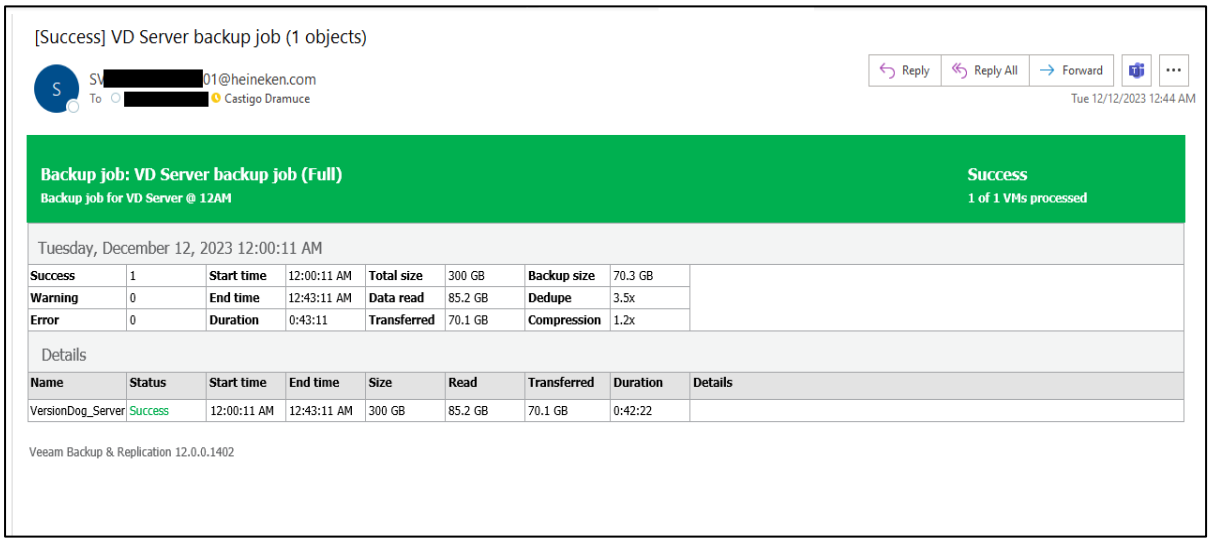
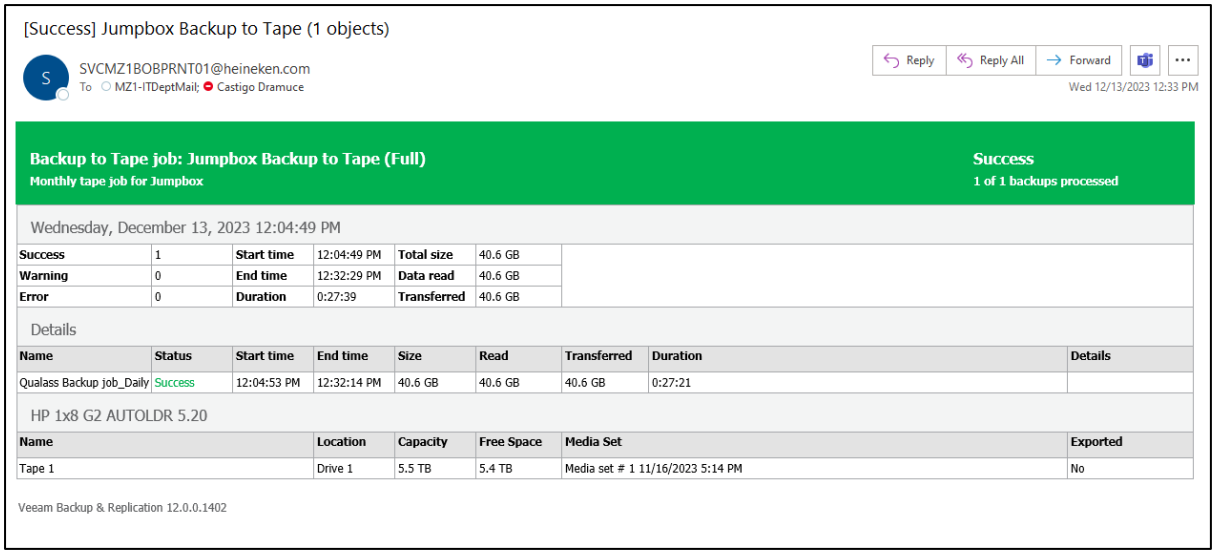


Figura 33: Alerta de email do trabalho de backup que correu com sucesso para o armazenamento de backup. Fonte: Autor



[Success] Jumpbox Backup to Tape (1 objects)

SVCMZ1BOBPRNT01@heineken.com
To MZ1-ITDeptMail; Castigo Dramuce

Reply | Reply All | Forward

Wed 12/13/2023 12:33 PM

Backup to Tape job: Jumpbox Backup to Tape (Full)
Monthly tape job for Jumpbox

Success
1 of 1 backups processed

Wednesday, December 13, 2023 12:04:49 PM

Success	1	Start time	12:04:49 PM	Total size	40.6 GB
Warning	0	End time	12:32:29 PM	Data read	40.6 GB
Error	0	Duration	0:27:39	Transferred	40.6 GB

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
Qualass Backup job_Daily	Success	12:04:53 PM	12:32:14 PM	40.6 GB	40.6 GB	40.6 GB	0:27:21	

HP 1x8 G2 AUTOLDR 5.20

Name	Location	Capacity	Free Space	Media Set	Exported
Tape 1	Drive 1	5.5 TB	5.4 TB	Media set # 1 11/16/2023 5:14 PM	No

Veeam Backup & Replication 12.0.0.1402

Figura 34: Alerta de email do trabalho de backup que correu com sucesso para Tape

Diante destes resultados pode dar-se como concluída com sucesso a instalação do sistema de backups. Restando desta forma a fase de igual importância que seria o teste de restauração.

Tendo os backups em todos os repositórios vistos na figura 30, o próximo foi fazer a restauração de:

1. Restauração de uma VM a partir da tape

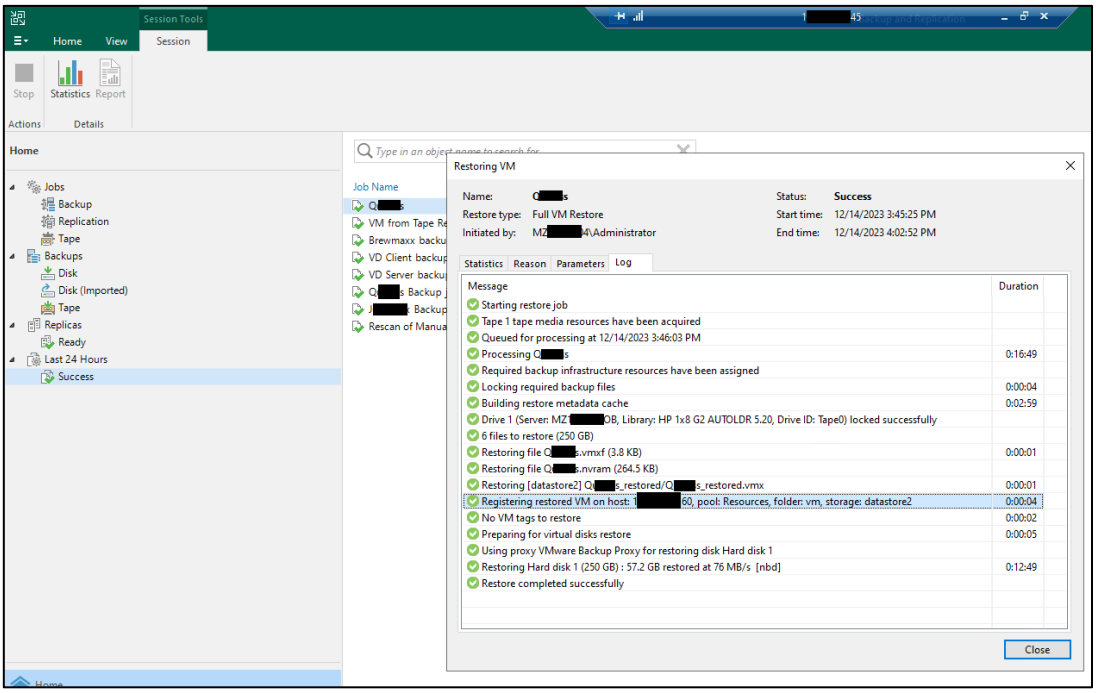


Figura 35: Restauração com sucesso de uma VM a partir da Tape. Fonte: Autor

2. Restauração de uma VM a partir das outras mídias de armazenamento (Disco duro externo)

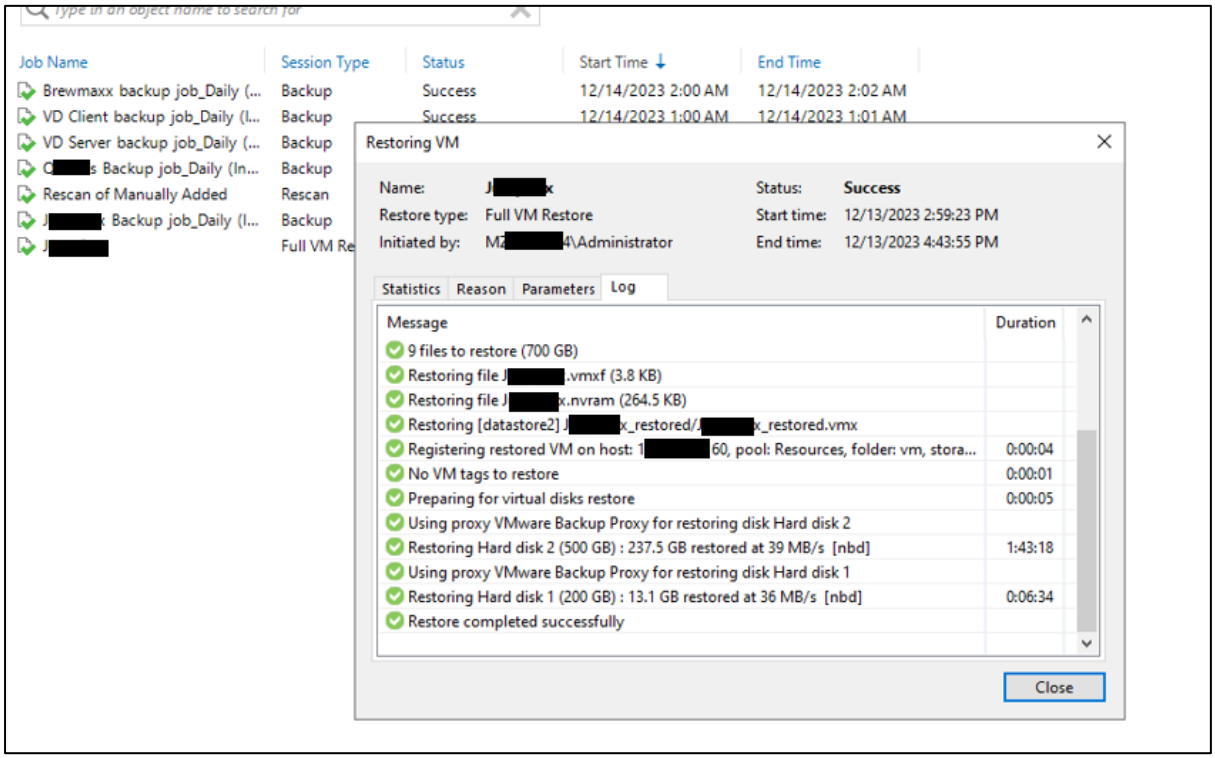


Figura 36: Restauração com sucesso de uma VM a partir do disco externo. Fonte: Autor

5.1. Desafios e lições aprendidas

Durante a execução de algumas tarefas descritas em **5.2**, surgiram alguns desafios que puderam servir de aprendizado. Como forma de advertir o leitor e partilhar o conhecimento obtido perante esses desafios, abaixo estão descritas as situações encontradas e as soluções encontradas para a sua resolução.

5.1.1. Problema da cópia de uma VM de um host para o outro

No decorrer do projecto, durante a primeira fase, descrita em **5.2.1**, a solução optada para a migração das máquinas virtuais de um host para o outro teve como consequência a mudança do MAC address da VM no novo host, o que também aconteceria com a solução sugerida pela (VMWARE, 2020) para as circunstâncias específicas da infra-estrutura na altura, isto é, sem armazenamento compartilhado entre os servidores e não a não existência de um vCenter server.

Por causa deste facto, no segundo dia após o a migração das máquinas virtuais para o novo servidor, a equipa de produção enfrentou um problema com um dos softwares

que fazem uso para descarregar selos digitas que são estampados nas garrafas de cerveja produzidas pela empresa.

O software apresentava um erro que a equipa de produção reportou ao fabricante do software. O fabricante por sua vez informou que o erro se devia a alguma alteração no hardware do computador (VM) onde está instalado o Software. Depois de ser sido à mim reportado o problema e a razão, a primeira ideia tentada foi de verificar se o MAC address da VM era o mesmo em ambos hosts, pois o artigo da VMware também informa que o MAC address da VM deve ser manualmente alterado.

Após definir o MAC address da VM em questão no novo host, para que seja igual ao endreço que a VM tinha no antigo host, foi pedido que fizessem o teste e continuassem a monitorar e logo depois desta troca do MAC address, a equipa notificou que o software já estava em funcionar na sua plenitude.

De salientar que fazendo o uso da funcionalidade de replicação do Veeam Backup & Replication, o problema do MAC address não chega a ocorrer pois o MAC address é também replicado neste processo.

5.1.2. Comunicação entre vCenter, aplicação de backup e hosts do Office

No primeiro parágrafo do **5.2.3**, foi dito que o servidor **Dell PowerEdge R750 (2.5") – Q** teria na sua estrutura a VM que contém a aplicação de Backup e o vCenter instalados no mesmo. Mas observando a figura 24 pode-se notar que este servidor está no lado do PCD e existe uma firewall que separa ambos ambientes, e sendo que os hosts do Office (antigo e novo) deve ser alcançável a partir do vCenter e da aplicação de backup para efeitos de replicação, há a necessidade de garantir que esse tráfego passe pela firewall.

Para que isso fosse possível foram feitas pesquisas onde fez-se o registo das portas e protocolos que são necessário permitir o tráfego na firewall, entre o IP dos hosts do Office e o vCenter (vice-versa), e também entre os IP dos hosts do Office e a VM que contém a aplicação de backup (vice-versa), conforme descrito em (VEEAM, 2023).

A implementação dessa actividade não é possível ser feita a nível da OpCo e por esse motivo, foi necessário abrir um *ticket* no Service Now para a equipa Global (explicado em **3.2**) responsável pela gestão das Firewalls.

Depois de aberto o ticket, foi preenchido o formulário onde devem ser descritas as alterações que deverão ser feitas na firewall e depois de aproximadamente cinco dias as alterações foram feitas e a rede estava pronta para receber os servidores.

5.1.3. Incompatibilidade da Placa para 10Gb

Com o Anexo 9 podemos verificar, a partir do endereço de gestão do *BMC* – designado neste servidor como iLO (Integrated Lights-Out), as propriedades do servidor **HPE Proliant DL380 Gen10 – O**, e os diversos componentes que o compõem e o estado dos mesmos.

A figura 37 mostra o mesmo servidor na secção das propriedades da rede e é possível que existe uma placa HBA "***HP Ethernet 10G 2-port 546SFP+ Adapter***" de rede 10Gb.

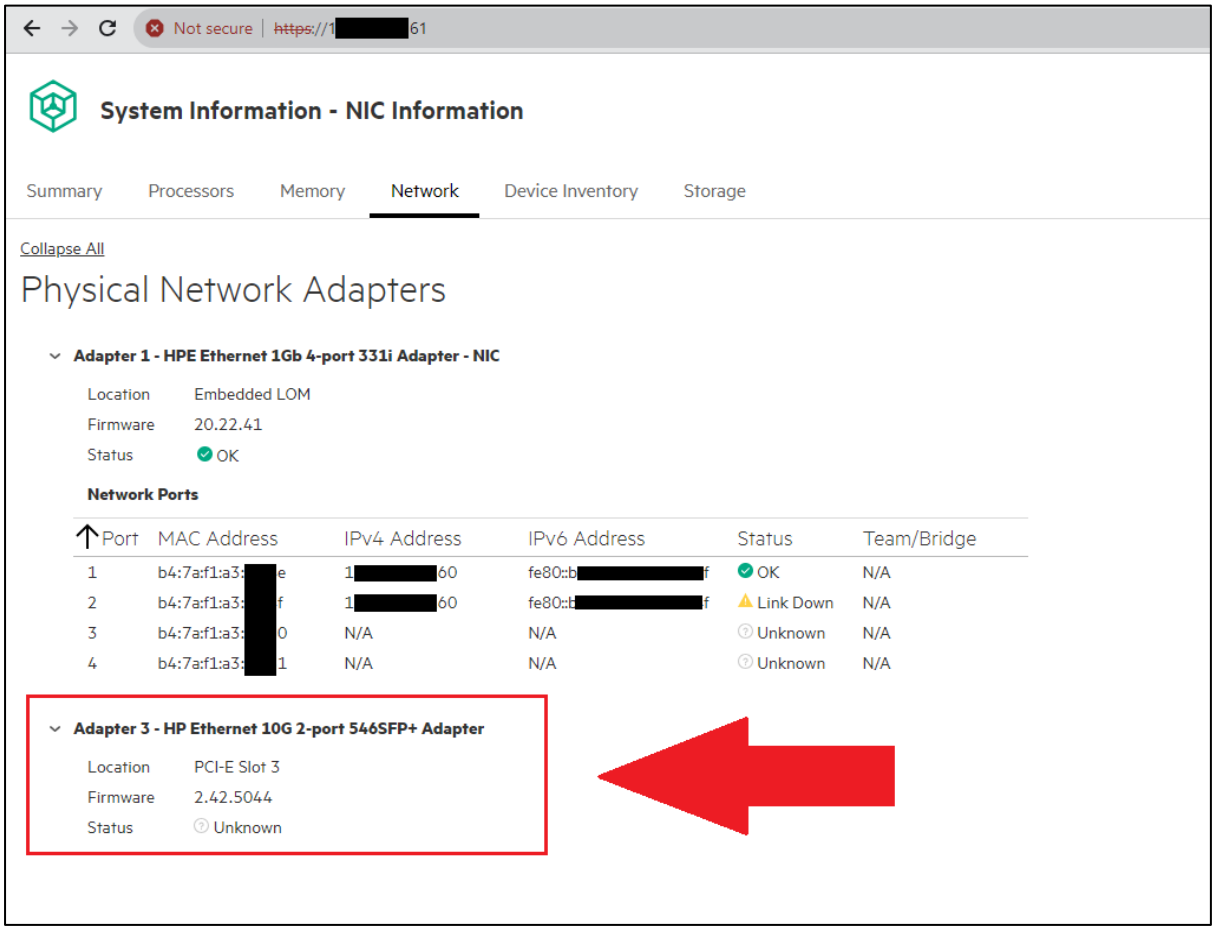


FIgura 37: Placa HBA de 10Gb no servidor HPE Proliant DL380 Gen10 – O

A figura 38 mostra as placas de rede do mesmo servidor, vistos a partir do sistema operativo, VMware ESXi 8, e a placa HBA "***HP Ethernet 10G 2-port 546SFP+ Adapter***" não aparece. Após pesquisas em torno do tópico foi possível ficar a saber que a placa não é suportada no VMware 8, conforme descrito por (Micanek, 2023).

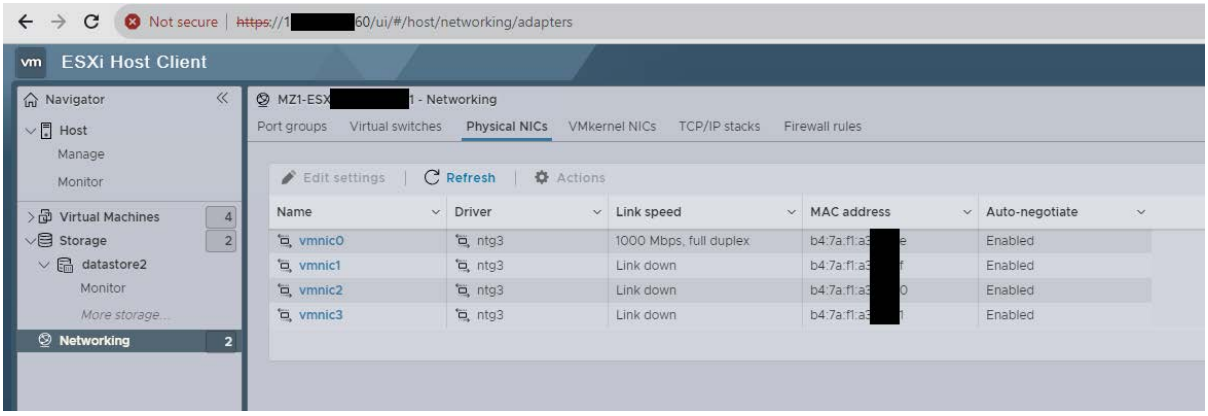


FIgura 38: Placa de rede no servidor HPE Proliant DL380 Gen10 – O a partir do VMware

Com isso dito, a única forma de poder ter um link de 10Gb neste servidor seria com a aquisição de um outro adaptador suportado, como por exemplo o "**HP Ethernet 10G 2-port 548SFP+ Adapter**" conforme descrito por (VMWARE, 2023)

5.2. Resultados obtidos e benefícios

Com a implementação até aqui feita, a fábrica da HEINEKEN Moçambique passou de um cenário onde praticamente não existiam backups, para o presente cenário onde existem pelo menos duas cópias dos sistemas usados no ambiente de produção do Office e do PCD.

As demais capturas de ecrã apresentadas no relatório, servem como forma de ilustrar partes do que foi implementado, servindo com evidência da implementação bem-sucedida dos eventos relatados.

Com a ilustração dos backups agendados e que foram executados com êxito, pode-se concluir que de agora em diante o trabalho a ser feito deverá ser de monitoramento destes e/ou a atenção dos relatórios que são enviados. Pois graças a estes, medidas atempadas podem ser tomadas no caso do não sucesso dos backups, garantido

assim que a infra-estrutura continue com um sistema de backups actualizado e possa responder no caso de desastres e/ou perda de informação.

Ainda mais importante que a execução dos backups, é a restauração bem-sucedida dos backups, a partir dos repositórios onde estes vão. Conforme ilustrado nas figuras 35 e 36, foram executados testes restauração e estes correram com sucesso, tornando o sistema de backups implementados na fábrica da HEINEKEN Moçambique completamente funcionais e pronto para responder à desastres.

De salientar que testes como estes devem ser feitos regularmente de forma a garantir que os backups que são executados serão úteis para a empresa no caso de perda da de dados ou no caso de um eventual desastre.

Graças a essa implementação, no caso de acontecer alguma falha de um dos sistemas ou então um desastre, diferente da outra vez, o dano desta vez não será da mesma magnitude graças aos sistemas implementados como replicação dos servidores do PCD, sistema de tape e futuramente com o DR, existirá sempre um ponto de restauro, garantindo que a situação de perda total de dados que aconteceu no passado não volte a acontecer. Diferente da outra vez, não será necessário começar “do zero”.

Um dos benefícios obtidos com a actual implementação está no facto de existir o sistema de tape que graças ao mesmo, no caso da ocorrência de um ataque por um malware que atinja a maior parte dos servidores que estão ligados a rede, todos os sistemas poderão ser restaurados, graças ao facto de este não estar ligado a rede.

Pelo facto de actualmente todos estes sistemas se encontrarem no mesmo espaço físico, ficou a directriz de se enviar as tapes com os backups mensais para a sede assim que estes terminarem, de forma a ter um backup off-site. Desta forma garantimos que no caso do acontecimento de um desastre como incêndio, haja uma forma de restaurar as informações a partir de uma mídia que não se encontra no mesmo espaço que os sistemas danificados.

Um dos grandes benefícios que a empresa teve na aquisição dos dois novos servidores foi a longevidade que estes trazem tanto no suporte à última versão do VMware ESXi, como também por estes serem servidores serem recentes, terão suporte do fabricante por mais tempo comparado com os que a empresa activamente operava antes.

Pelo facto de terem sido adquiridos dois servidores ESXi para o ambiente PCD, no caso da paragem do servidor principal (Dell PowerEdge R750 (2.5") - Q):

- **Por falha de hardware**: o servidor secundário (de backup) poderá iniciar as máquinas virtuais exactamente de onde havia parado (no momento da falha), graças ao facto do storage usado no servidor principal estar também ligado ao servidor secundário (conforme ilustra a figura 24).
- **Por falha de storage**: O servidor secundário também pode iniciar as máquinas virtuais a partir do seu armazenamento interno, pois este possui a réplica das máquinas virtuais que correm no servidor principal (conforme apresentado na Tabela 6).

Deve-se também contar que para além dos servidores actuais, existem também os servidores cujo propósito é fazer o comissionamento do DR site, fazendo assim com que a informação seja salvaguardada em mais um local além do actual.

Graças ao projecto foi possível identificar alguns pontos de melhor que podem ser de grande utilidade aos administradores da infra-estrutura, como é o caso da melhoria dos links que os servidores actualmente usam. Também ligado à este ponto, seria também a melhoria no dispositivo que interliga os ambientes PCD e Office, a firewall interna, que actualmente é um gargalo para o tráfego entre alguns dados do ambiente PCD e do Office.

Pela escolha da solução Veeam, a empresa futuramente terá benefícios dessa escolha pois futuramente passará a contar com descontos nas renovações das licenças da solução. Graças as tantas funcionalidades dessa solução, como agendamento das tarefas de backup e alertas por email, será possível ter os backups a serem feitos de forma automática e os relatórios (de sucesso ou não) destes backups serão enviados para os administradores dos sistemas.

6. CAPÍTULO VI – CONCLUSÕES E RECOMENDAÇÕES

Para responder os objectivos propostos no Introdução, o presente capítulo irá apresentar as conclusões obtidas após a elaboração do trabalho, bem como deixar ficar as recomendações para trabalhos futuros em torno da infra-estrutura com vista na melhoria e optimização da mesma.

6.1. Conclusão

Para além do aprendizado tido no desenvolvimento do trabalho, foi possível ir ao encontro dos objectivos definidos no Capítulo I, onde no final do projecto foi possível conforme detalhado ao longo do trabalho, instalar um sistema de backups na infra-estrutura fábrica da empresa HEINEKEN Moçambique, em Bobole.

Conforme inicialmente proposto, foi também descrita a situação em que a empresa se encontrava a nível da infra-estrutura de virtualização, onde através do de figuras e tabelas foram descritos os componentes que existem na infra-estrutura e o propósito de cada um deles. E com base no que a infra-estrutura dispunha foi possível desenhar uma proposta para a existência e operacionalização de um sistema de backups, onde a partir da mesma foram analisados os pontos de falha e melhorias que poderiam ser feitas.

Com base nessas melhorias de cada proposta foi então escolhida a proposta que mais agrega valor e também satisfaz o objectivo geral do trabalho, que é a instalação de um sistema de backups na infra-estrutura, trazendo maior robustez para a solução.

No final deste processo foi possível implementar uma solução que responde ao que foi proposto como solução para o problema, onde para além de garantir que através da infra-estrutura de backups consiga se fazer a salvaguarda da informação, mas também seja possível, a partir dos backups restaurar a informação e sistemas existentes.

O trabalho foi também uma oportunidade de ver em primeira mão a importância da existência de backups para uma organização e que o investimento no mesmo, apesar de não ser linear, traz retornos para uma empresa na evitação nas paragens de produção o que também evita perda de lucros, nos casos de empresas como a HEINEKEN Moçambique. Foi possível aprender através das pesquisas feitas que a

existência de um sistema de backup deve sempre estar acompanhado de um plano sólido de testes de restauração, pois sem este não há garantia de que os backups poderão ser úteis para o ambiente onde este se encontra.

6.2. Recomendações

Em forma de recomendação para próximos projectos fica a implementação do DR site pois dessa forma será possível ter a partir de uma outra localização, ter uma réplica da infra-estrutura no caso de acontecer algum desastre na actual localização da infra-estrutura.

Para além do ponto anterior, a actual firewall que está instalada na infra-estrutura desde 2018, Fortinet Fortigate 100E, que separa os ambientes Office e PCD somente tem portas cuja velocidade não alcançam 10Gbps. Por esse motivo, esta poderá futuramente ser trocada por um modelo de firewall que tenha portas que permitam o tráfego de 10Gbps, de forma a não causar o gargalo (*bottleneck)* entre os dois ambientes.

O modelo recomendado seria a firewall da mesma categoria, de entrada (*entry-level*), Fortinet FortiGate 100F pois esta suporta 10Gbps em duas portas, através do uso de *transceivers* SPF+ (*Small Form-factor Pluggable*). A vantagem deste modelo é que tem o número de portas necessárias para o cenário da empresa e ainda não tem data definida para o fim de suporte técnico.

Com a implementação projecto, o tráfego entre as redes do PCD e do Office irá aumentar o que fortalece ainda mais a necessidade da troca desta firewall, para uma que permita mais largura entre as redes, sem contar que o suporte para a actual firewall termina em 2026.

Outra recomendação, que de certa forma está ligada a recomendação anterior é a melhoria nos links entre os hosts e o switch onde estes se ligam. Os switches onde estão ligados os servidores possuem portas de 10Gbps e estas não estão a ser

usadas na sua total capacidade pois os servidores HP não têm placas HBA compatíveis com o VMware.

Conforme visto no Anexo 8, pode-se ver uma grande quantidade de cabos no rack dos dispositivos de rede. Aquando da montagem e ligação dos equipamentos na infra-estrutura foi possível encontrar cabos de rede (fibra e UTP) que estavam desligados em ambos terminais. Para além disso, para alguns dispositivos cujos cabos haviam sido por mim identificados, foi feita a troca de cabos com mais de três metros, que ligavam equipamentos no mesmo rack, por cabos de um à três metros. Desta forma reduzindo a quantidade de cabos faziam voltas ao longo do organizador de cabos lateral do rack. Com isto deixo ficar a recomendação de fazer uma organização dos cabos, de modo a aliviar o organizador de cabos lateral e melhorar o aspecto do rack no geral.

BIBLIOGRAFIA

Brandão, P. R. (2018). *Virtualização: fundamentos.* ISTEC – Departamento de Estudos e Investigação em Tecnologias de Informação e Sociedade . Evora: Kriativ Tech. Obtido em 03 de Outubro de 2003, de http://www.kriativ-tech.com/wp-content/uploads/2018/02/02PEDROBRANDao.pdf

Chaubal, C. (24 de Outubro de 2008). *The Architecture of VMware ESXi*. Obtido em 30 de Novembro de 2023, de VMWARE: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/ESXi_architecture.pdf

Controle Net. (2023). *O que é HBA (Host Bus Adapter)*. Obtido em 01 de Novembro de 2023, de Controle Net: https://www.controle.net/faq/o-que-e-hba-host-bus-adapter-e-qual-a-importancia-dessas-controladoras

Dell Technologies. (2023). *Integrated Dell Remote Access Controller (iDRAC)*. Obtido em 30 de Novembro de 2023, de Dell Technologies: https://www.dell.com/en-us/lp/dt/open-manage-idrac

Đorđević, B., Jovičić, I., Kraljević, N., & Timčenko, V. (2022). Comparison of type-2 hypervisor performance on the example of VirtualBox, VMware Workstation player and MS Hyper-V., (p. 6). Serbia. Obtido em 29 de Novembro de 2023, de https://www.etran.rs/2022/zbornik/ICETRAN-22_radovi/066-RTI2.4.pdf

Gupta, J. (25 de Janeiro de 2018). *Top hypervisor comparison 2019 - HyperV vs vSphere vs XenServer vs KVM*. Obtido em 30 de Novembro de 2023, de ZNetLive Blog: https://www.znetlive.com/blog/server-virtualization-software-comparison-microsoft-hyper-v-vs-vmware-vsphere-vs-citrix-xenserver-vs-kvm/

Hewlett Packard Enterprise (HPE). (s.d.). *What is Integrated Lights-Out (iLO)?* Obtido em 30 de Novembro de 2023, de Hewlett Packard Enterprise (HPE): https://www.hpe.com/us/en/what-is/ilo.html

Indeed Editorial Team. (19 de Dezembro de 2022). *What Is a Process Control System? (With Benefits and Types)*. Obtido em 14 de Setembro de 2023, de Indeed.com: https://www.indeed.com/career-advice/career-development/process-control-system

Infoblox. (s.d.). *What is DDI - (Secure DNS, DHCP, IPAM)*. Obtido em 15 de Novembro de 2023, de Infoblox: https://www.infoblox.com/glossary/ddi/

KVM. (2023). *KVM*. Obtido em 30 de Novembro de 2023, de KVM: https://linux-kvm.org/page/Main_Page

Lavoie, S. (11 de Maio de 2023). *Baseboard Management Controller (BMC)*. Obtido em 02 de Novembro de 2023, de The OnLogic Blog: Edge Computing Articles & Insights: https://www.onlogic.com/company/io-hub/baseboard-management-controller/

Lopes, J. (15 de Setembro de 2015). *VMWARE - Arquitetura Tradicional x Virtualização*. Obtido em 12 de Outubro de 2023, de Jovino IT: http://jovinoit.blogspot.com/2015/09/vmware-arquitetura-tradicional-x.html

McCrory, D., Reynolds , W., & Marshall , D. (2006). *VMware and Microsoft Platforms in the Virtual Data Center.* (T. &. Group, Ed.) Florida: Auerbach Publications.

McDonald, G., Papadopoulos, P., Ahmad , J., Pitropakis, N., & Buchanan, W. (26 de Janeiro de 2022). Ransomware: Analysing the Impact on Windows Active. *Sensors*, p. 26. Obtido em 30 de Novembro de 2023, de https://www.mdpi.com/1424-8220/22/3/953

MEF. (03 de Novembro de 2022). *AT Reforça Controlo Fiscal e Aduaneiro, Com a Entrada em Vigor da Selagem de Cervejas e RTD's*. Obtido de Ministério da Economia e Finanças: https://www.mef.gov.mz/index.php/imprensa/noticias/693-at-reforca-controlo-fiscal-e-aduaneiro-com-a-entrada-em-vigor-da-selagem-de-cervejas-e-rtd-s

Mell , P., & Grance , T. (2011). *The NIST Definition of Cloud Computing.* Obtido em 21 de Agosto de 2023, de National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Meyler, K., Holt, B., Oh, M., & Sandys, J. (2012). *System Center 2012 Configuration Manager (SCCM) Unleashed.* United States of America: Sams Publishing.

Micanek, D. (15 de Agosto de 2023). *ESXi 8.0 – Deprecated and unsupported devices*. Obtido em 30 de Novembro de 2023, de vDan: https://vdan.cz/esxi-8-0-deprecated-and-unsupported-devices/

Nelson, S. (2011). *Pro Data Backup and Recovery.* New York: Apress.

Porwal, K. M., Yadav, A., & Charhate, S. (2008). Traffic Analysis of MPLS and Non MPLS Network including MPLS Signaling Protocols and Traffic Distribution in OSPF and MPLS. *First International Conference on Emerging Trends in Engineering and Technology* (p. 6). Nagpur: IEEE. Obtido de https://ieeexplore.ieee.org/document/4579892/authors#authors

ProLeiT Group. (2023). *BrewMaxx - The industry solution for breweries*. Obtido em 10 de Novembro de 2023, de ProLeiT: https://www.proleit.com/brewmaxx/

Rajagopalan, S. (2020). An Overview of SD-WAN Load Balancing for WAN Connections. *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (p. 4). Coimbatore: IEEE. Obtido de https://ieeexplore.ieee.org/document/9297574

Rittinghouse, J. W., & Ransome, J. F. (2009). *Cloud Computing: Implementation, Management, and Security* (1st ed.). Boca Raton: CRC Press.

Rodgers, M. (21 de Setembro de 2021). *Copying ESXi VMs to New Host Using SCP*. Obtido em 10 de Novembro de 2023, de Medium: https://medium.com/@mjrod/copying-esxi-vms-to-new-host-using-scp-d1e266c1d3c1

SenthilKumar, P., & Muthukumar, M. (2018). A Study on Firewall System, Scheduling and. *2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW)* (p. 4). Erode, India: IEEE. Obtido de https://ieeexplore.ieee.org/document/8997167

Servile, V. (21 de Janeiro de 2021). *Jumping SSH Hosts*. Obtido em 22 de Novembro de 2023, de oooops.dev – DevOps is hard: https://oooops.dev/2021/01/31/jumping-ssh-hosts/

SolarWinds. (s.d.). *What is a DDI_ - IT Glossary _ SolarWinds*. Obtido em 15 de Novembro de 2023, de SolarWinds: https://www.solarwinds.com/resources/it-glossary/ddi

Stallings, W. (2017). *Computer Security: Principles and Practice.* New Jersey: Pearson Education, Inc. Obtido de https://ds.amu.edu.et/xmlui/bitstream/handle/123456789/17468/Computer_Security_Principles_and_Practice_%283rd_Edition%29.pdf?sequence=1&isAllowed=y

Steffen, C. (Novembro de 2017). network SECURITY. *Network Security Newsletter*, 20. Obtido em 02 de Novembro de 2023, de http://digpath.co.uk/wp-content/uploads/2017/11/NESE_2017-11_Nov.pdf

VEEAM. (12 de Julho de 2023). *Ports - User Guide for VMware vSphere*. Obtido em 25 de Novembro de 2023, de Veeam Technical Documentation: https://helpcenter.veeam.com/docs/backup/vsphere/used_ports.html?ver=120

VMWARE. (14 de Maio de 2020). *Moving a virtual machine between ESXi hosts with different processor types (2058684)*. Obtido em 10 de Novembro de 2023, de VMware Customer Connect: https://kb.vmware.com/s/article/2058684

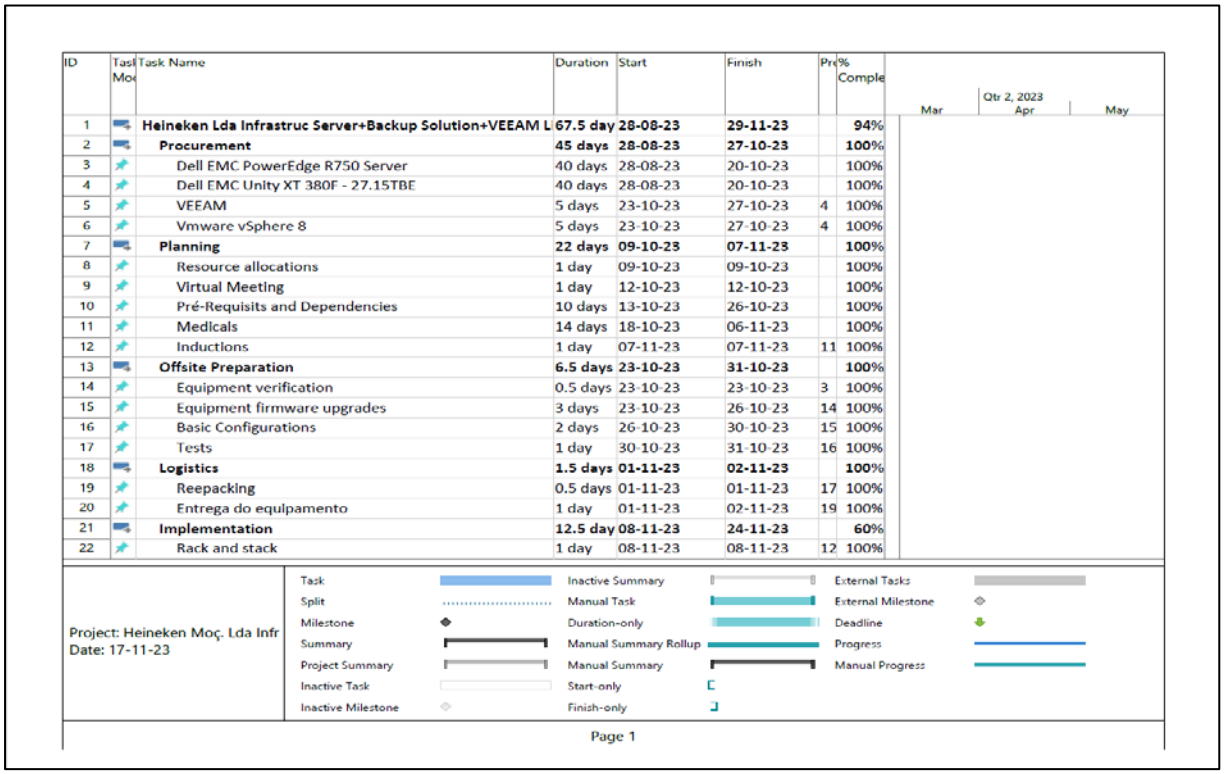
VMWARE. (24 de Agosto de 2021). *VMSA-2021-0014.1*. Obtido em 30 de Novembro de 2023, de VMware: https://www.vmware.com/security/advisories/VMSA-2021-0014.html

VMWARE. (Novembro de 2023). *VMware Compatibility Guide - I_O Device Search*. Obtido em 30 de Novembro de 2023, de VMware: https://www.vmware.com/resources/compatibility/detail.php?deviceCategory=io&productid=49626

VMWARE. (2023). *What is ESXi - Bare Metal Hypervisor*. Obtido em 20 de Outubro de 2023, de VMWARE: https://www.vmware.com/products/esxi-and-esx.html

ANEXOS

Anexo 1 – Cronograma Inicial de actividades do Projecto de Implementação de Sistema de Backups

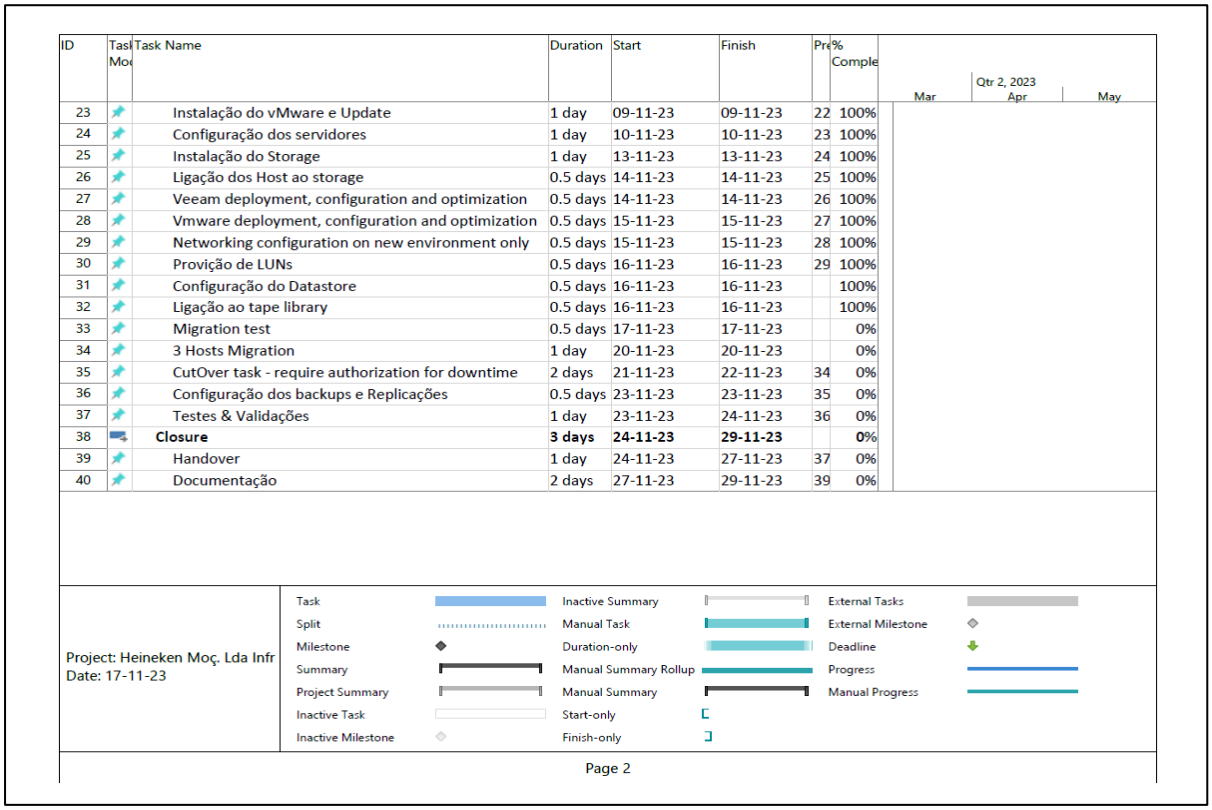


ID	Task Mo	Task Name	Duration	Start	Finish	Pre	% Comple
1		**Heineken Lda Infrastruc Server+Backup Solution+VEEAM L**	**67.5 day**	**28-08-23**	**29-11-23**		**94%**
2		**Procurement**	**45 days**	**28-08-23**	**27-10-23**		**100%**
3		Dell EMC PowerEdge R750 Server	40 days	28-08-23	20-10-23		100%
4		Dell EMC Unity XT 380F - 27.15TBE	40 days	28-08-23	20-10-23		100%
5		VEEAM	5 days	23-10-23	27-10-23	4	100%
6		Vmware vSphere 8	5 days	23-10-23	27-10-23	4	100%
7		**Planning**	**22 days**	**09-10-23**	**07-11-23**		**100%**
8		Resource allocations	1 day	09-10-23	09-10-23		100%
9		Virtual Meeting	1 day	12-10-23	12-10-23		100%
10		Pré-Requisits and Dependencies	10 days	13-10-23	26-10-23		100%
11		Medicals	14 days	18-10-23	06-11-23		100%
12		Inductions	1 day	07-11-23	07-11-23	11	100%
13		**Offsite Preparation**	**6.5 days**	**23-10-23**	**31-10-23**		**100%**
14		Equipment verification	0.5 days	23-10-23	23-10-23	3	100%
15		Equipment firmware upgrades	3 days	23-10-23	26-10-23	14	100%
16		Basic Configurations	2 days	26-10-23	30-10-23	15	100%
17		Tests	1 day	30-10-23	31-10-23	16	100%
18		**Logistics**	**1.5 days**	**01-11-23**	**02-11-23**		**100%**
19		Reepacking	0.5 days	01-11-23	01-11-23	17	100%
20		Entrega do equipamento	1 day	01-11-23	02-11-23	19	100%
21		**Implementation**	**12.5 day**	**08-11-23**	**24-11-23**		**60%**
22		Rack and stack	1 day	08-11-23	08-11-23	12	100%

Project: Heineken Moç. Lda Infr
Date: 17-11-23

Task, Split, Milestone, Summary, Project Summary, Inactive Task, Inactive Milestone, Inactive Summary, Manual Task, Duration-only, Manual Summary Rollup, Manual Summary, Start-only, Finish-only, External Tasks, External Milestone, Deadline, Progress, Manual Progress

Page 1



ID	Task Mo	Task Name	Duration	Start	Finish	Pre	% Comple
23		Instalação do vMware e Update	1 day	09-11-23	09-11-23	22	100%
24		Configuração dos servidores	1 day	10-11-23	10-11-23	23	100%
25		Instalação do Storage	1 day	13-11-23	13-11-23	24	100%
26		Ligação dos Host ao storage	0.5 days	14-11-23	14-11-23	25	100%
27		Veeam deployment, configuration and optimization	0.5 days	14-11-23	14-11-23	26	100%
28		Vmware deployment, configuration and optimization	0.5 days	15-11-23	15-11-23	27	100%
29		Networking configuration on new environment only	0.5 days	15-11-23	15-11-23	28	100%
30		Provição de LUNs	0.5 days	16-11-23	16-11-23	29	100%
31		Configuração do Datastore	0.5 days	16-11-23	16-11-23		100%
32		Ligação ao tape library	0.5 days	16-11-23	16-11-23		100%
33		Migration test	0.5 days	17-11-23	17-11-23		0%
34		3 Hosts Migration	1 day	20-11-23	20-11-23		0%
35		CutOver task - require authorization for downtime	2 days	21-11-23	22-11-23	34	0%
36		Configuração dos backups e Replicações	0.5 days	23-11-23	23-11-23	35	0%
37		Testes & Validações	1 day	23-11-23	24-11-23	36	0%
38		**Closure**	**3 days**	**24-11-23**	**29-11-23**		**0%**
39		Handover	1 day	24-11-23	27-11-23	37	0%
40		Documentação	2 days	27-11-23	29-11-23	39	0%

Project: Heineken Moç. Lda Infr
Date: 17-11-23

Task, Split, Milestone, Summary, Project Summary, Inactive Task, Inactive Milestone, Inactive Summary, Manual Task, Duration-only, Manual Summary Rollup, Manual Summary, Start-only, Finish-only, External Tasks, External Milestone, Deadline, Progress, Manual Progress

Page 2

Anexo 2 – Descrição dos serviços e equipamentos a serem fornecidos

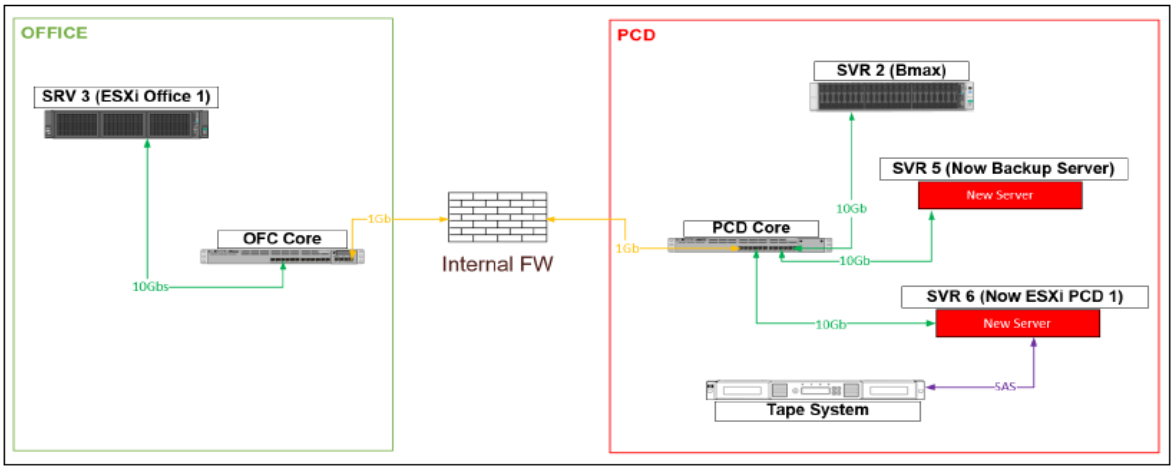
Cenário Desejado

No cenário desejado, o servidor **SVR 6** (com memória baseada em Flash – especificações no final do documento), irá desempenhar o papel do actual **SVR 1 (Actual ESXi PCD)** no sentido de que todas as das VM do PCD passarão a correr a parir deste último servidor para o novo servidor (**SVR6**).

O **SVR 6** deverá ser o backup do **SVR 5**, no sentido de que as VMs que existem no **SVR 6** deverão ter o seu backup no **SVR 5**.

Todos servidores nesse cenário deverão estar ligados à velocidade de 10Gbps, com excepção do **SVR 2 (BMax)**.

Deve também ser configurado o sistema de réplica para a Tape Library que actualmente não está ligado à infra-estrutura



Escopo do Trabalho

1. Fornecimento de dois (2) Servidores.
   a. O primeiro servidor (Backup Server – SRV 5) será o servidor de backup. Especificações no final da página
   b. O segundo servidor (ESXi PCD 1 – SRV 6) será o novo servidor de ESXi do PCD. Especificações no final da página
2. Fornecimento de outros equipamentos que garantam a conexão descrita no desenho (como cabos e os respectivos adaptadores/transceivers & HBAs), de forma a substituir a maior parte das ligações que no **Cenário Actual** são de 1Gb (somente para o PCD)
3. Instalação e configuração do VMware ESXi 8 e o VCenter.
4. Instalação e configuração do VEEAM Backup & Replication.
5. Instalação e configuração da Tape Library

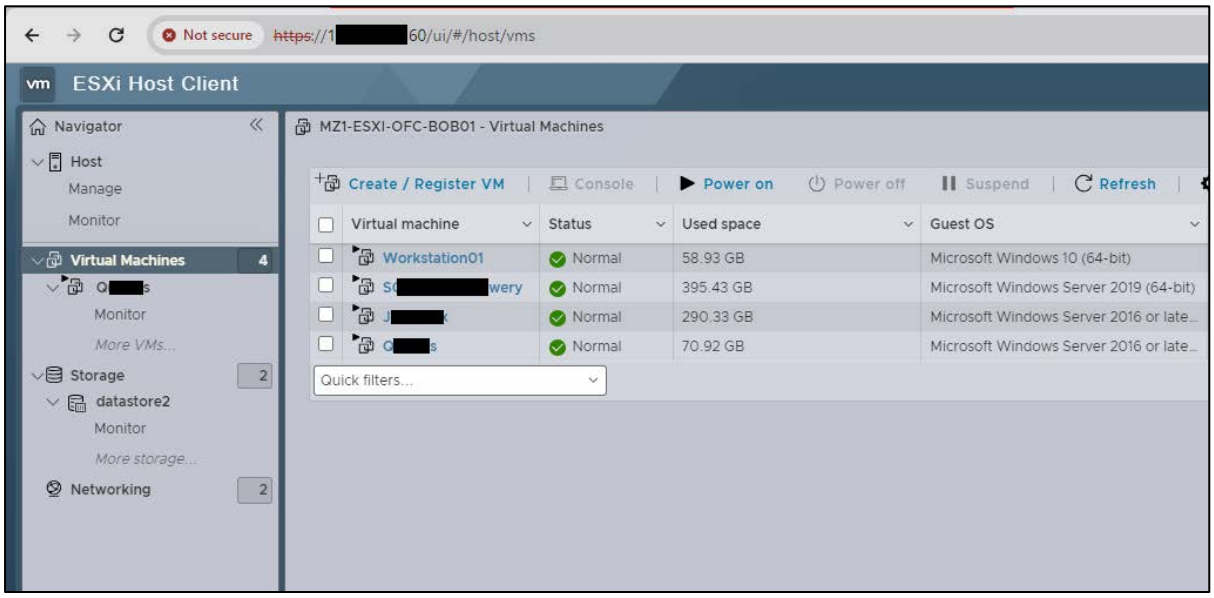
Notas:

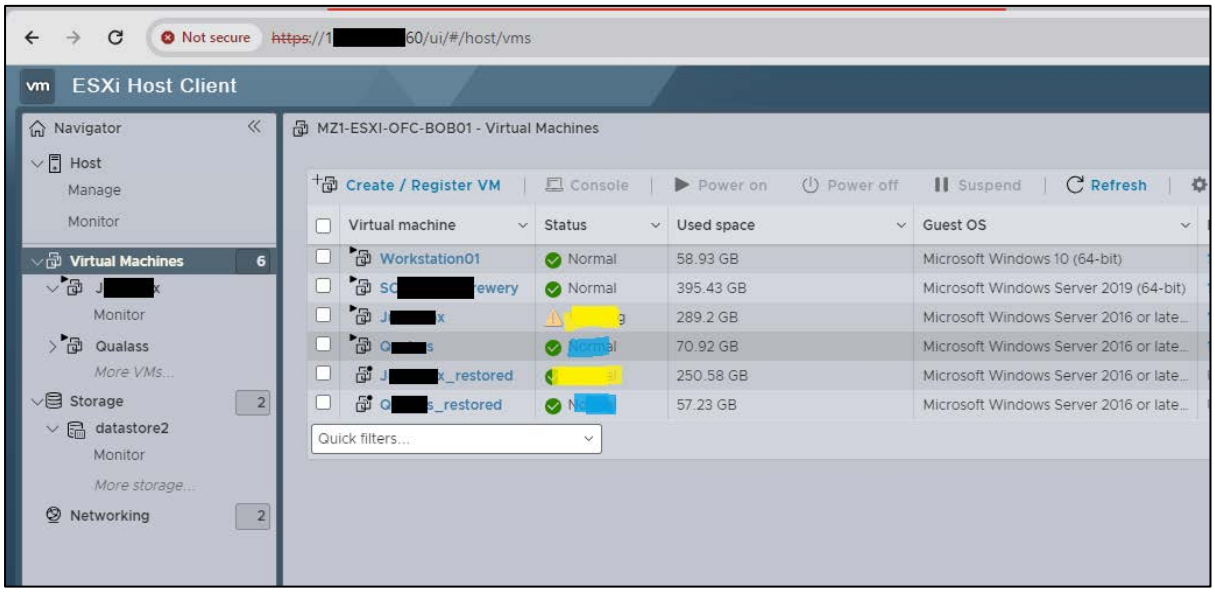
1. O Sistema de "Tape System" e os cabos já existem no nosso inventário e não será necessário o fornecimento.

Por ser fornecido:

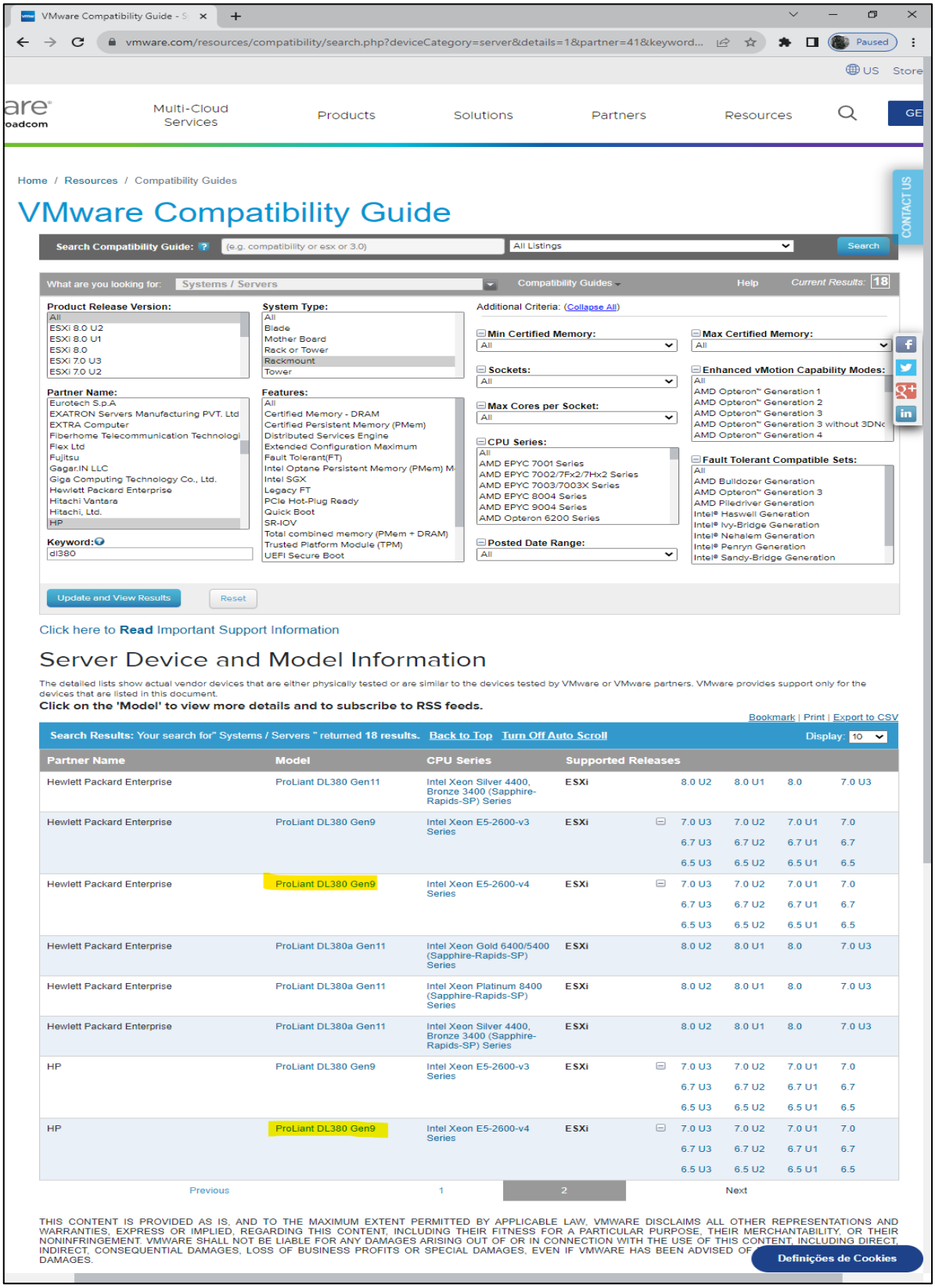
1. Licenças:
   a. VEEAM B&R
   b. VMware ESXi 7.0 (3) + VCenter
2. Discos:
   a. 5un **1.2TB 10K SAS – Model: EG001200JWJNQ | PN: 1XH200-035**
3. Memórias RAM
   a. 4un de 16GB RAM para o modelo HP ProLiant DL380 Gen10
   b. 6 un de 16GB RAM para o modelo HP ProLiant DL380 Gen9
4. 2x Servidores:
   a. **Ports:** at least 4x 10GbE Ports + SAS Ports or HBA
   b. **RAID Options:** 0, 1, 5, 6
   c. **RAM:** pelo menos 128GB
   d. **Storage:** a least 8TB each

Anexo 3 – Antes e depois da restauração das máquinas virtuais





Anexo 4 – Guia de compatibilidade do HPE DL380 Gen 9 com o VMware



VMware Compatibility Guide - S

vmware.com/resources/compatibility/search.php?deviceCategory=server&details=1&partner=41&keyword...

Paused

US Store

are loadcom

Multi-Cloud Services | Products | Solutions | Partners | Resources | GE

Home / Resources / Compatibility Guides

VMware Compatibility Guide

CONTACT US

Search Compatibility Guide: (e.g. compatibility or esx or 3.0) All Listings Search

What are you looking for: Systems / Servers Compatibility Guides Help Current Results: 18

Product Release Version:
All
ESXi 8.0 U2
ESXi 8.0 U1
ESXi 8.0
ESXi 7.0 U3
ESXi 7.0 U2

System Type:
All
Blade
Mother Board
Rack or Tower
Rackmount
Tower

Additional Criteria: (Collapse All)

Min Certified Memory: All

Max Certified Memory: All

Sockets: All

Enhanced vMotion Capability Modes:
All
AMD Opteron™ Generation 1
AMD Opteron™ Generation 2
AMD Opteron™ Generation 3
AMD Opteron™ Generation 3 without 3DN
AMD Opteron™ Generation 4

Partner Name:
Eurotech S.p.A
EXATRON Servers Manufacturing PVT. Ltd
EXTRA Computer
Fiberhome Telecommunication Technologi
Flex Ltd
Fujitsu
Gagar.IN LLC
Giga Computing Technology Co., Ltd.
Hewlett Packard Enterprise
Hitachi Vantara
Hitachi, Ltd.
HP

Features:
All
Certified Memory - DRAM
Certified Persistent Memory (PMem)
Distributed Services Engine
Extended Configuration Maximum
Fault Tolerant(FT)
Intel Optane Persistent Memory (PMem) M
Intel SGX
Legacy FT
PCIe Hot-Plug Ready
Quick Boot
SR-IOV
Total combined memory (PMem + DRAM)
Trusted Platform Module (TPM)
UEFI Secure Boot

Max Cores per Socket: All

CPU Series:
All
AMD EPYC 7001 Series
AMD EPYC 7002/7Fx2/7Hx2 Series
AMD EPYC 7003/7003X Series
AMD EPYC 8004 Series
AMD EPYC 9004 Series
AMD Opteron 6200 Series

Fault Tolerant Compatible Sets:
All
AMD Bulldozer Generation
AMD Opteron™ Generation 3
AMD Piledriver Generation
Intel® Haswell Generation
Intel® Ivy-Bridge Generation
Intel® Nehalem Generation
Intel® Penryn Generation
Intel® Sandy-Bridge Generation

Posted Date Range: All

Keyword: dl380

Update and View Results | Reset

Click here to **Read** Important Support Information

Server Device and Model Information

The detailed lists show actual vendor devices that are either physically tested or are similar to the devices tested by VMware or VMware partners. VMware provides support only for the devices that are listed in this document.

Click on the 'Model' to view more details and to subscribe to RSS feeds.

Bookmark | Print | Export to CSV

Search Results: Your search for" Systems / Servers " returned **18 results.** Back to Top Turn Off Auto Scroll Display: 10

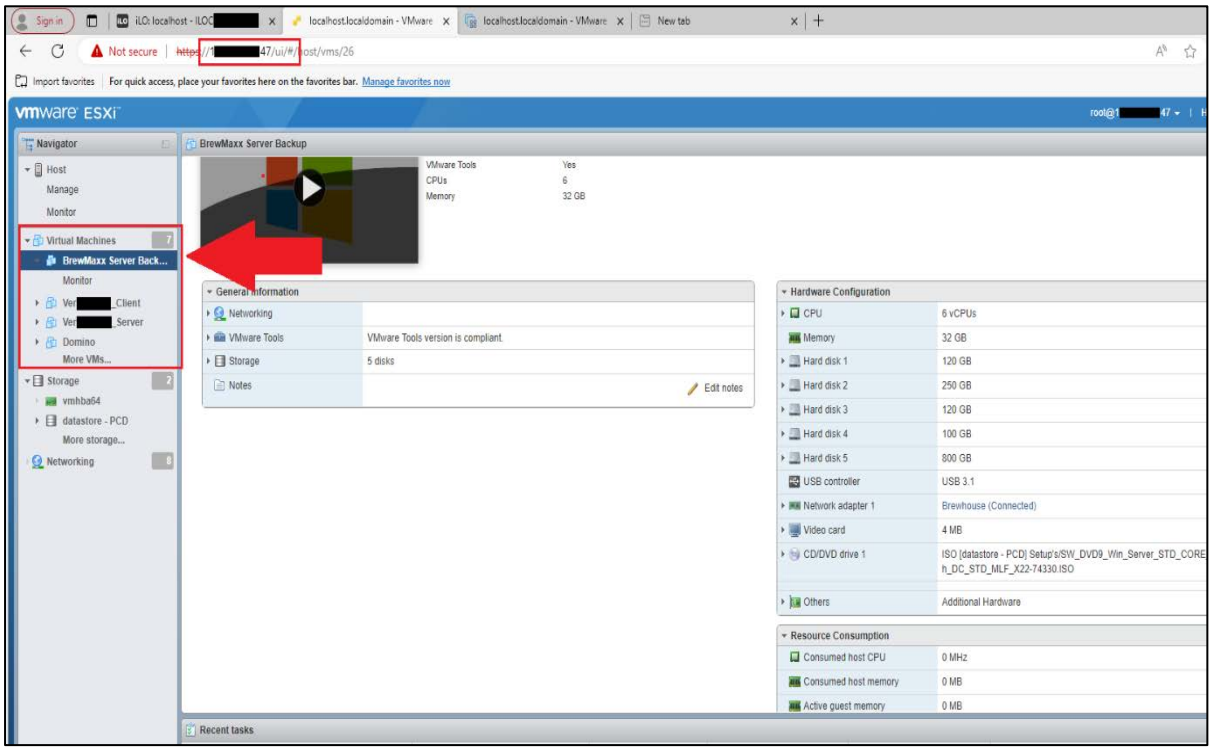
Partner Name	Model	CPU Series	Supported Releases				
Hewlett Packard Enterprise	ProLiant DL380 Gen11	Intel Xeon Silver 4400, Bronze 3400 (Sapphire-Rapids-SP) Series	ESXi	8.0 U2	8.0 U1	8.0	7.0 U3
Hewlett Packard Enterprise	ProLiant DL380 Gen9	Intel Xeon E5-2600-v3 Series	ESXi	7.0 U3	7.0 U2	7.0 U1	7.0
				6.7 U3	6.7 U2	6.7 U1	6.7
				6.5 U3	6.5 U2	6.5 U1	6.5
Hewlett Packard Enterprise	ProLiant DL380 Gen9	Intel Xeon E5-2600-v4 Series	ESXi	7.0 U3	7.0 U2	7.0 U1	7.0
				6.7 U3	6.7 U2	6.7 U1	6.7
				6.5 U3	6.5 U2	6.5 U1	6.5
Hewlett Packard Enterprise	ProLiant DL380a Gen11	Intel Xeon Gold 6400/5400 (Sapphire-Rapids-SP) Series	ESXi	8.0 U2	8.0 U1	8.0	7.0 U3
Hewlett Packard Enterprise	ProLiant DL380a Gen11	Intel Xeon Platinum 8400 (Sapphire-Rapids-SP) Series	ESXi	8.0 U2	8.0 U1	8.0	7.0 U3
Hewlett Packard Enterprise	ProLiant DL380a Gen11	Intel Xeon Silver 4400, Bronze 3400 (Sapphire-Rapids-SP) Series	ESXi	8.0 U2	8.0 U1	8.0	7.0 U3
HP	ProLiant DL380 Gen9	Intel Xeon E5-2600-v3 Series	ESXi	7.0 U3	7.0 U2	7.0 U1	7.0
				6.7 U3	6.7 U2	6.7 U1	6.7
				6.5 U3	6.5 U2	6.5 U1	6.5
HP	ProLiant DL380 Gen9	Intel Xeon E5-2600-v4 Series	ESXi	7.0 U3	7.0 U2	7.0 U1	7.0
				6.7 U3	6.7 U2	6.7 U1	6.7
				6.5 U3	6.5 U2	6.5 U1	6.5

Previous 1 2 Next

THIS CONTENT IS PROVIDED AS IS, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VMWARE DISCLAIMS ALL OTHER REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, REGARDING THIS CONTENT, INCLUDING THEIR FITNESS FOR A PARTICULAR PURPOSE, THEIR MERCHANTABILITY, OR THEIR NONINFRINGEMENT. VMWARE SHALL NOT BE LIABLE FOR ANY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS CONTENT, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF VMWARE HAS BEEN ADVISED OF

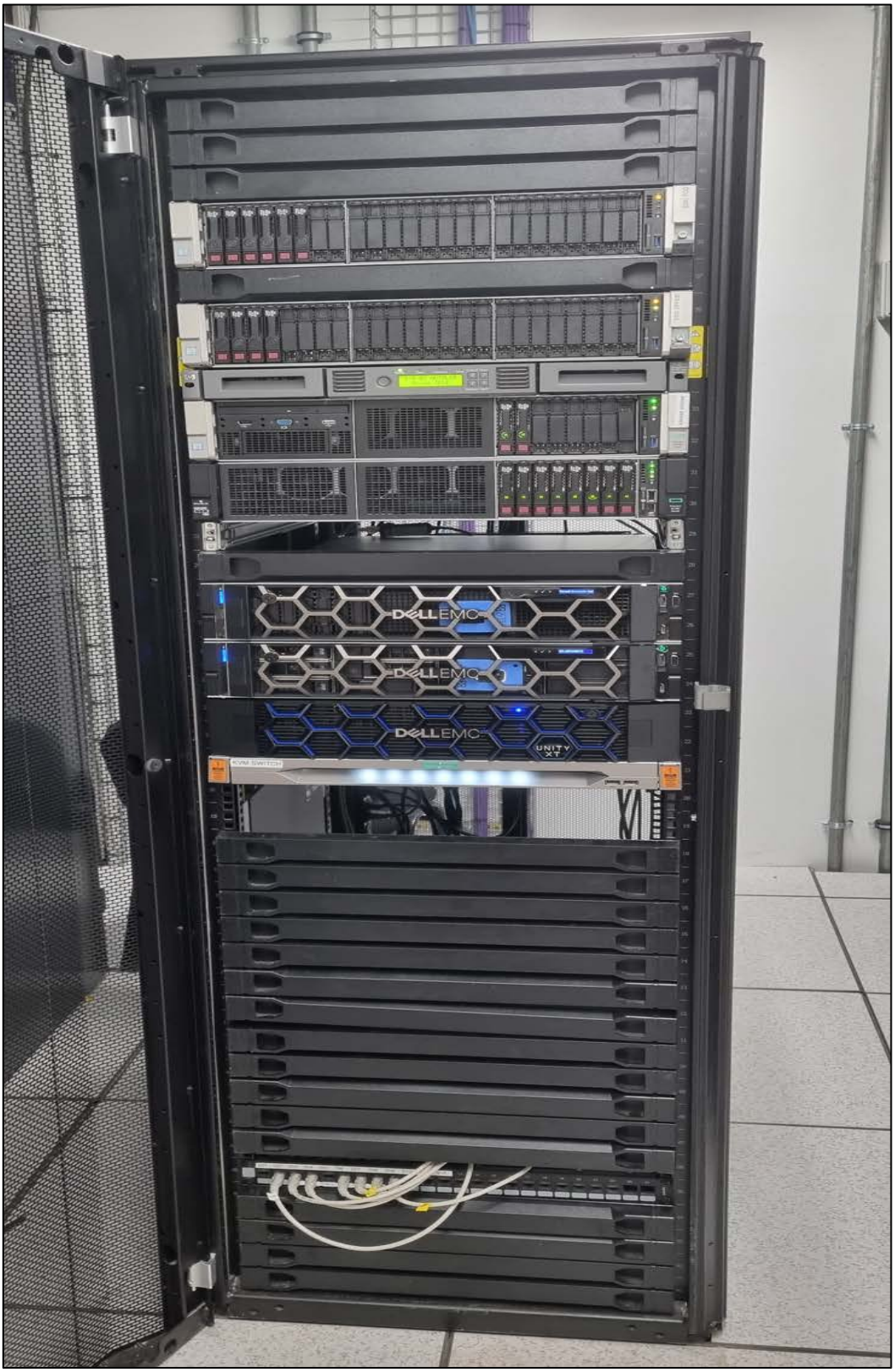
Definições de Cookies

Anexo 5 – Máquinas virtuais no servidor HPE ProLiant DL380 Gen9-L

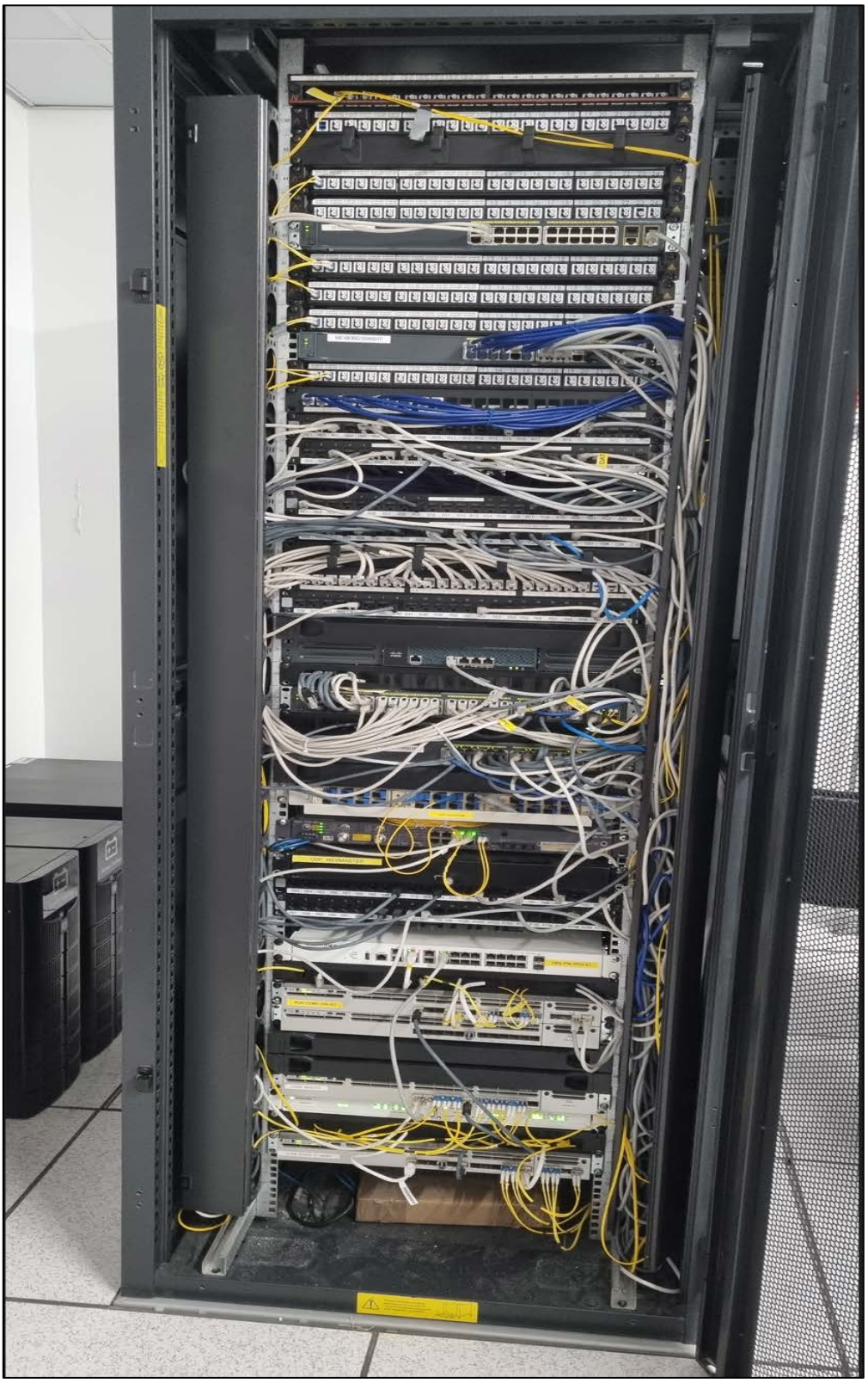


Anexo 6 – Foto do rack dos servidores antes da instalação dos novos servidors (frente)

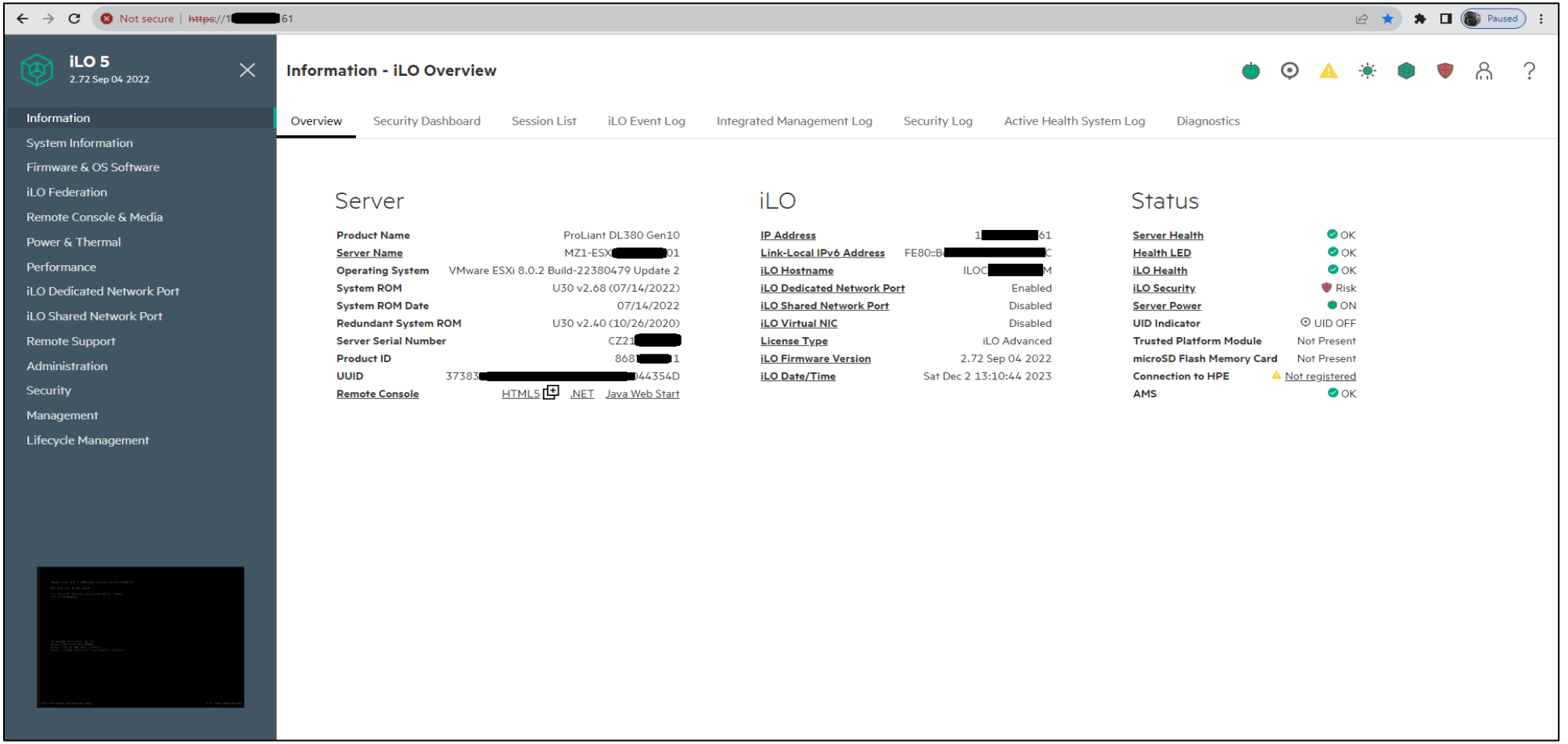
Anexo 7 – Foto do rack dos servidores depois da instalação dos novos servidores (frente)



Anexo 8 – Foto do rack dos dos dispositivos de rede (frente)



Anexo 9 – Informações do servidor HPE Proliant DL380 Gen10 – O visto a partir do BMC (Integrated Lights-Out – iLO)



Anexo 10 – LUN (Logical Unit Number) criadas no Dell - Unity XT 380F - U