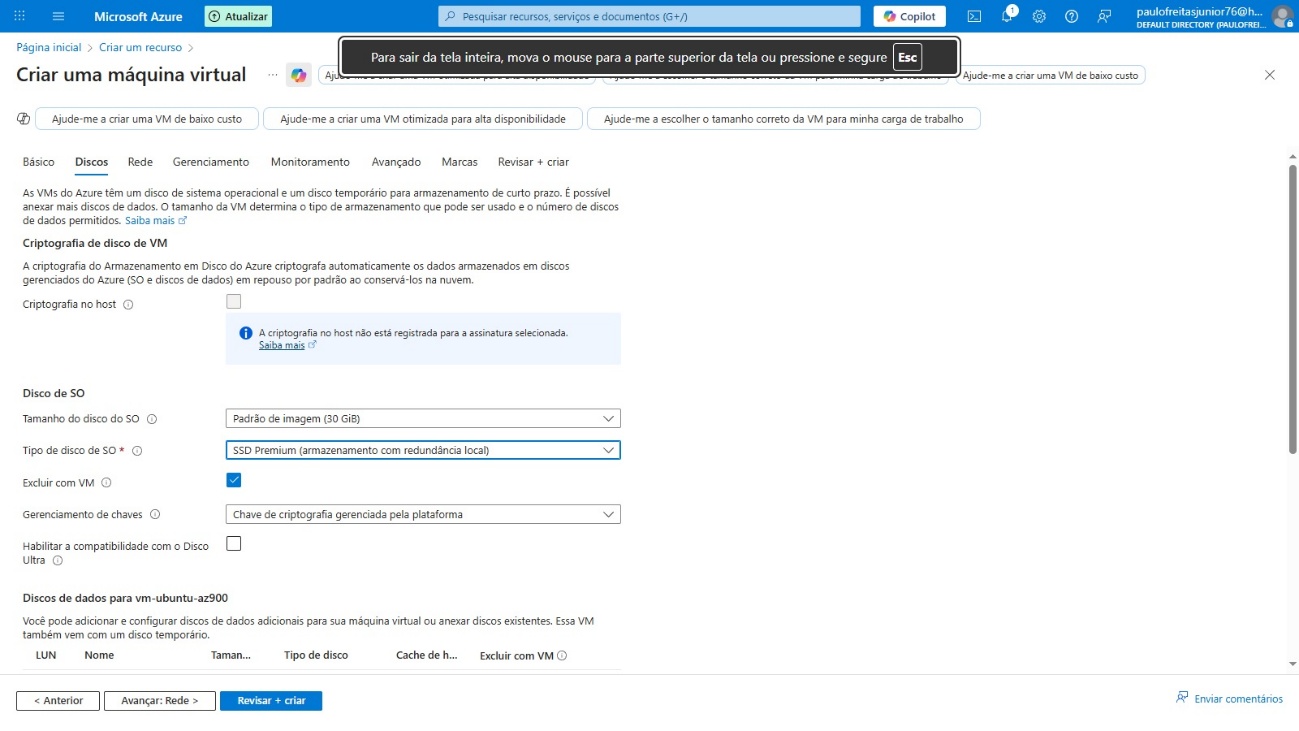
**ANÁLISE DE CONFIGURAÇÃO DE DISCOS E CRIPTOGRAFIA**

Este relatório complementa a análise de provisionamento da Máquina Virtual Spot, focando-se exclusivamente nas escolhas de **Armazenamento (Discos)** e nas implicações de segurança e desempenho resultantes das configurações apresentadas.

**I. Imagem 1: Configuração de Criptografia e Armazenamento Persistente**

****

A Imagem 1 detalha as escolhas de disco gerenciado (Managed Disk) para o Sistema Operacional, a redundância e a abordagem de criptografia de dados em repouso.

**1.1. Configuração e Desempenho do Disco de SO**

O disco do Sistema Operacional (SO) foi configurado com os seguintes atributos:

* **Tamanho do Disco de SO:** Padrão de imagem (30 GiB).
* **Tipo de Disco de SO:** SSD Premium (armazenamento com redundância local).

**Análise:**

A seleção de **Premium SSD** é uma escolha de alto desempenho, ideal para cargas de trabalho que exigem alta taxa de transferência (throughput) e baixa latência. Embora o uso de VMs Spot sugira uma intenção de baixo custo, o Premium SSD garante o melhor desempenho de I/O para as operações do sistema operacional e do sistema de arquivos, o que é crucial para o tempo de inicialização da VM e a responsividade geral do SO.

O disco utiliza **Armazenamento com Redundância Local (LRS)**. O LRS armazena três cópias dos dados dentro de um único datacenter, protegendo contra falhas de hardware local, mas não contra um desastre em nível de datacenter (que é mitigado pela Zona de Disponibilidade, configurada no passo inicial).

**1.2. Gerenciamento de Criptografia de Dados em Repouso**

A configuração define o nível de proteção para os dados em repouso (dados armazenados no disco).

* **Gerenciamento de Chaves:** Chave de criptografia gerenciada pela plataforma.
* **Criptografia no Host (Encryption at Host):** **Desativada (caixa desmarcada)**.

**Análise de Segurança (Server-Side Encryption vs. Encryption at Host):**

1. **Chaves Gerenciadas pela Plataforma (PMKs):** Esta é a configuração padrão e mais básica de segurança do Azure. Todos os Managed Disks são **automaticamente criptografados em repouso** (Server-Side Encryption – SSE) usando chaves gerenciadas pela Microsoft (PMKs). A SSE protege os dados quando persistem nos clusters de armazenamento do Azure.
2. **Criptografia no Host (Encryption at Host):** Ao deixar esta opção desmarcada, o usuário opta por não habilitar uma camada de segurança aprimorada. A Criptografia no Host garante que os dados sejam criptografados no nível do host da Máquina Virtual *antes* de serem armazenados no Storage Cluster. Embora o disco principal já use SSE, a Criptografia no Host é crucial para:
   * Criptografar o **cache do disco de SO e de dados**.
   * Assegurar o fluxo de dados criptografado de ponta a ponta entre a VM e o armazenamento.
   * Criptografar discos temporários (embora a VM Standard\_D2ls\_v3 seja de "Low Cost Storage" e não tenha disco temporário, a proteção do cache permanece relevante).

A recomendação de segurança para ambientes que manipulam dados sensíveis é habilitar a Criptografia no Host para fornecer o máximo de proteção de ponta a ponta.

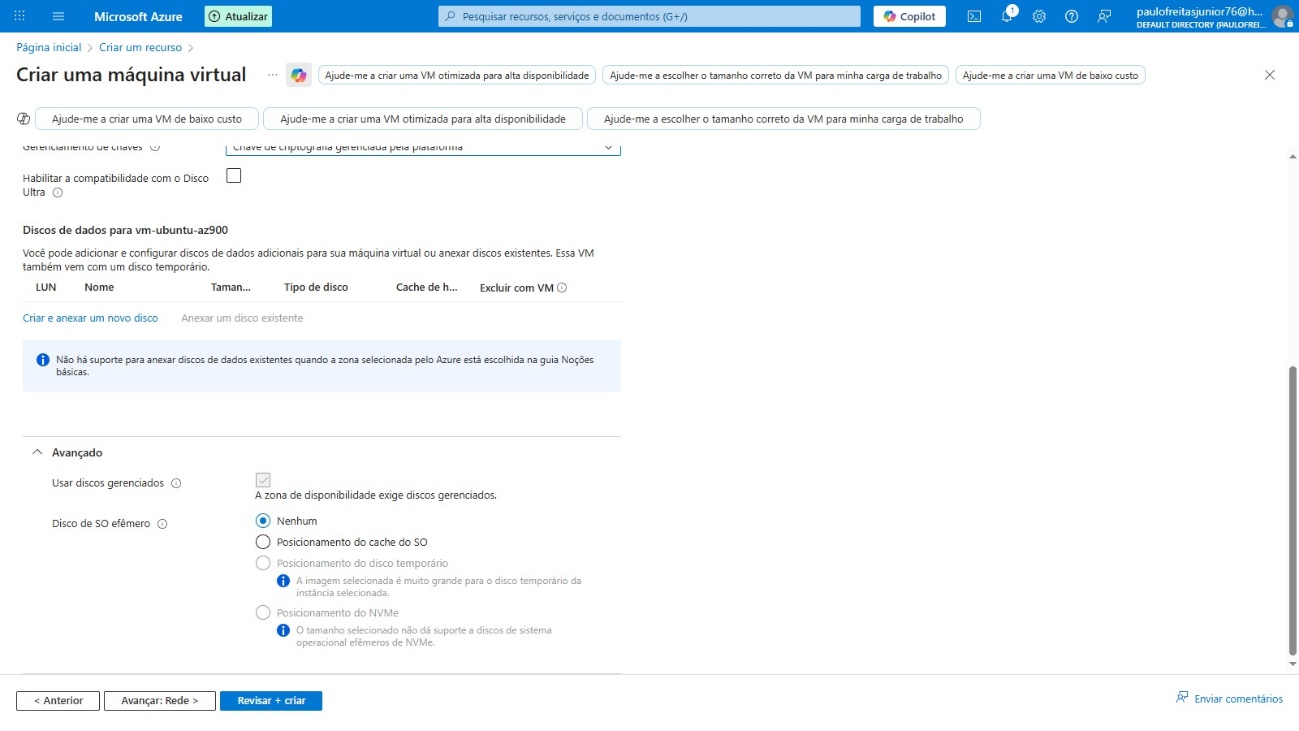
**1.3. Política de Ciclo de Vida do Disco**

A opção **Excluir com VM** está **marcada**.

**Análise de Custo e Operação:**

Esta configuração é uma prática recomendada para VMs voláteis, como as Instâncias Spot. Ao marcar esta caixa, o disco de SO será **automaticamente excluído** quando a Máquina Virtual for excluída (por remoção Spot ou exclusão manual). Isso garante que não haja custos persistentes de armazenamento para discos órfãos após a interrupção da VM, alinhando-se com a estratégia de custo otimizado da Instância Spot.

**II. Imagem 2: Gerenciamento Avançado de Discos e Cache**

****

A Imagem 2 exibe o gerenciamento de discos de dados e as configurações de cache para o disco de SO.

**2.1. Discos Gerenciados e Zonas de Disponibilidade**

O resumo da seção Avançado confirma que a opção **Usar discos gerenciados** está ativada.

**Análise:**

A opção confirma uma restrição arquitetônica fundamental: **"A zona de disponibilidade exige discos gerenciados"**. Como a VM foi configurada em uma Zona de Disponibilidade, o uso de Discos Gerenciados é obrigatório, pois eles são o pré-requisito para o modelo de alta disponibilidade zonal no Azure.

**2.2. Disco de SO Efêmero**

Foi selecionada a opção **Nenhum** para o Disco de SO efêmero.

**Análise:**

Discos de SO Efêmeros usam o disco temporário local da VM (se houver) para hospedar o SO, o que oferece latência ultrabaixa, mas torna o disco ***não persistente*** em caso de reinicialização ou desalocação. A seleção Nenhum significa que o disco de SO persistente (Premium SSD LRS) será usado, garantindo a **durabilidade** do SO e do sistema de arquivos, o que é preferível para a maioria das cargas de trabalho, incluindo as que utilizam Instâncias Spot, pois o estado do SO será retido após uma expulsão seguida de re-provisionamento.

**2.3. Configuração de Cache do Disco de SO**

O posicionamento do cache do SO (Posicionamento do cache do SO) está selecionado, o que, por padrão para discos de SO, define o **Caching do Host** para **Leitura/Escrita (Read/Write)**.

**Análise de Desempenho:**

O Caching do Host permite que a VM utilize a memória local do host para armazenar dados usados recentemente, o que pode aumentar significativamente o desempenho de leitura.

* **Disco de SO:** O padrão de cache Leitura/Escrita é geralmente recomendado para discos de SO, pois o SO realiza operações balanceadas de leitura e escrita.
* **Limitação:** O Caching do Host é suportado apenas para discos com tamanho inferior a 4 TiB. O disco de 30 GiB se enquadra facilmente neste requisito, garantindo o benefício do cache para o desempenho do SO.

A configuração de cache contribui para um ambiente operacional de alta velocidade, complementando a escolha do Premium SSD para o disco de SO.