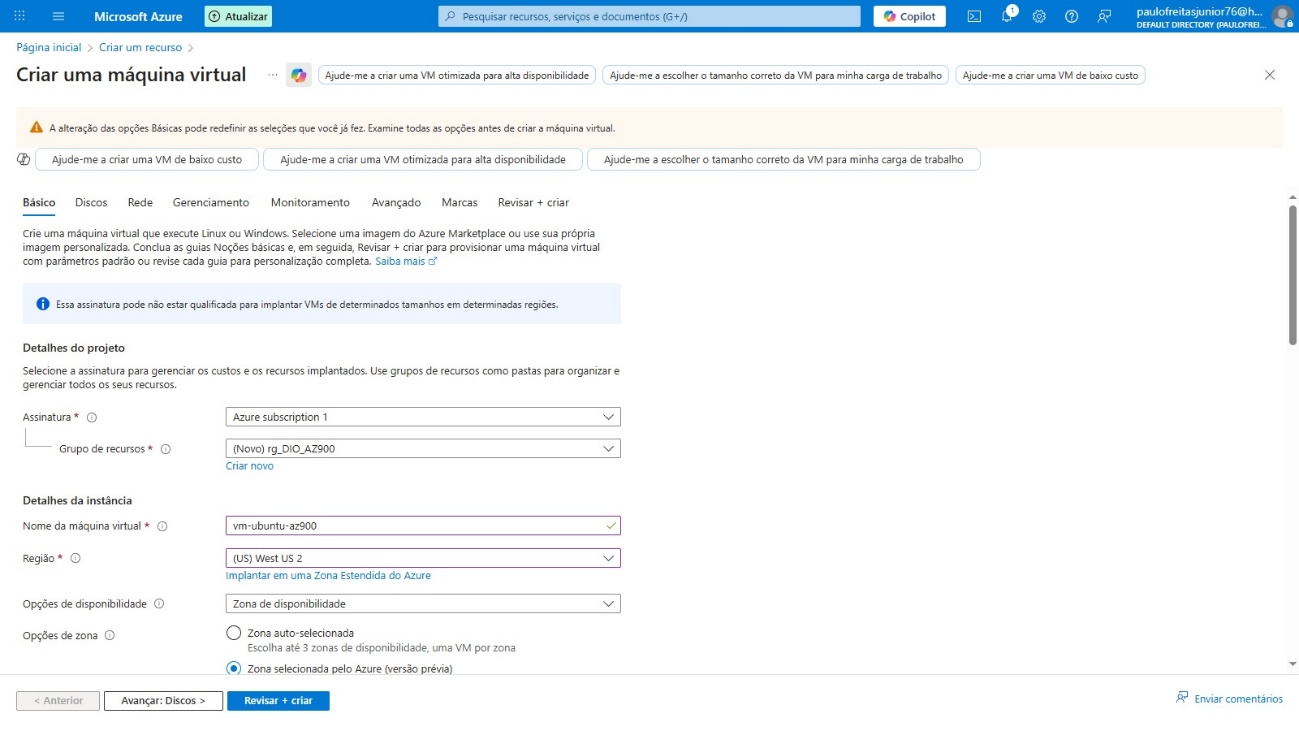
**RELATÓRIO TÉCNICO DE IMPLEMENTAÇÃO DE INFRAESTRUTURA AZURE (IAAS): ANÁLISE DE PROVISIONAMENTO DE MÁQUINA VIRTUAL UBUNTU SPOT**

**I. Introdução Executiva e Contextualização do Cenário de Implantação**

Este relatório técnico oferece uma análise detalhada do processo de provisionamento de uma Máquina Virtual (VM) Linux no portal Azure. A implantação é marcada pela estratégia dupla de otimizar custos operacionais por meio de Instâncias Spot, enquanto se mantém a alta resiliência regional pela seleção de Zonas de Disponibilidade.

A análise se concentra em examinar as implicações arquitetônicas, de custo e, crucialmente, de segurança de cada seleção. O objetivo principal combinar esses elementos, parece ser hospedar uma carga de trabalho que seja inerentemente *tolerante à interrupção* (adequada para Spot) — como processamento em lote ou desenvolvimento/teste— mas que exija proteção contra a falha total de um datacenter, garantindo a continuidade do serviço em nível regional.

**II. Passo 1: Configuração Fundamental do Projeto e Resiliência Regional (imagem 1)**

****

A primeira fase da criação da VM estabelece o escopo administrativo e a fundação geográfica e resiliente da instância.

**2.1. Detalhes do Projeto e Gerenciamento de Recursos**

A máquina virtual está sendo provisionada sob a Azure subscription 1, que atua como o principal limite de faturamento e governança para a alocação de recursos.

Para o gerenciamento, foi criado um novo **Grupo de Recursos** (RG) denominado rg-DIO\_AZ900. Um Grupo de Recursos funciona como um **contêiner lógico crucial para gerenciar recursos** que compartilham o mesmo ciclo de vida. A adoção da nomenclatura padronizada, como sugerido pela estrutura rg-DIO\_AZ900, demonstra uma aderência a boas práticas de governança. O valor dessa prática reside na coordenação do gerenciamento: quando a solução associada ao projeto (AZ-900) for concluída, a exclusão do Resource Group garantirá que todos os componentes relacionados — incluindo a VM, discos, interfaces de rede e IPs— sejam removidos simultaneamente, prevenindo a persistência de recursos órfãos e os consequentes custos indesejados.

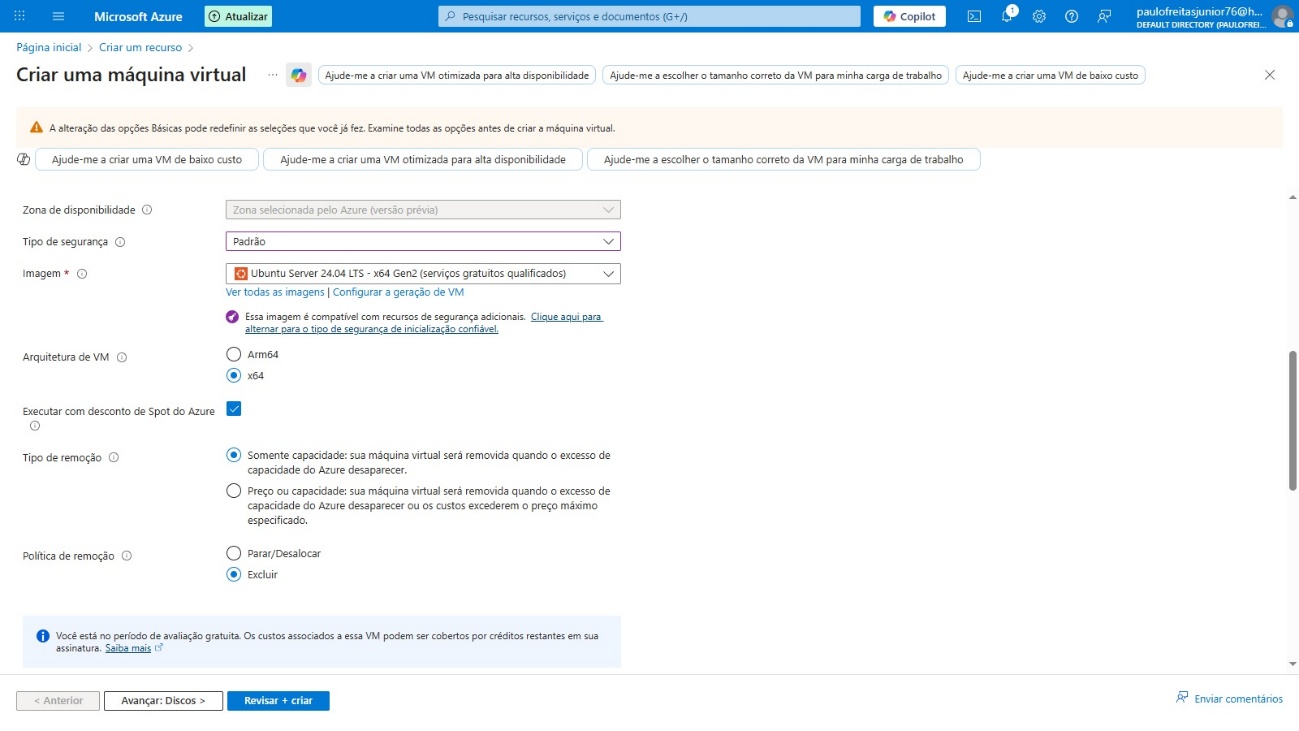
**2.2. Detalhes da Instância e Configuração de Resiliência**

A VM foi nomeada vm-ubuntu-az900 e implantada na região **(US) West US 2**. A escolha crítica de infraestrutura é a configuração das **Opções de Disponibilidade**, onde foi selecionada a "Zona selecionada pelo Azure (versão prévia)".

**As Zonas de Disponibilidade (AZs)** representam datacenters física e logicamente separados dentro de uma região, cada um com energia, resfriamento e rede independentes, projetados para proteger aplicações e dados contra falhas de datacenter. Ao escolher uma Zona (ou permitir que o Azure selecione uma), a VM é implantada como um ***serviço zonal***, significando que o recurso está "fixado" a uma zona específica. A resiliência total da aplicação, neste modelo, requer que o **cliente** replique ativamente o aplicativo e os dados entre uma ou mais zonas.

A combinação de uma **VM Spot** (baixo custo, alta volatilidade) e uma **Zona de Disponibilidade** (alta resiliência regional) levanta uma consideração arquitetônica importante. O uso de Spot indica uma tolerância à falha em nível de instância, mas a seleção de uma Zona de Disponibilidade (AZ) demonstra uma preocupação com a resiliência contra falhas regionais de grande escala. Essa arquitetura sugere uma estratégia de risco mitigado: buscar máxima economia de custo por meio de VMs descartáveis, mas garantir que a infraestrutura fundacional seja robusta o suficiente para resistir a desastres geográficos maiores.

**III. Passo 2: Imagem, Segurança e Otimização de Custos Spot (imagem 2)**

****

Objetivo é detalhar as escolhas do sistema operacional e a ativação da estratégia de otimização de custos através da Instância Spot.

**3.1. Configurações de Sistema Operacional e Geração**

A seleção do **Tipo de Segurança** Padrão e a **Imagem** Ubuntu Server 24.04 LTS - x64 Gen2, que é uma imagem Linux robusta, utilizando a arquitetura de 64 bits (x64) com Geração 2 (baseada em UEFI). A escolha da imagem é compatível com recursos de segurança adicionais, embora o tipo de segurança inicial tenha sido definido como Padrão.

**3.2. Implementação e Análise Estratégica da Instância Spot**

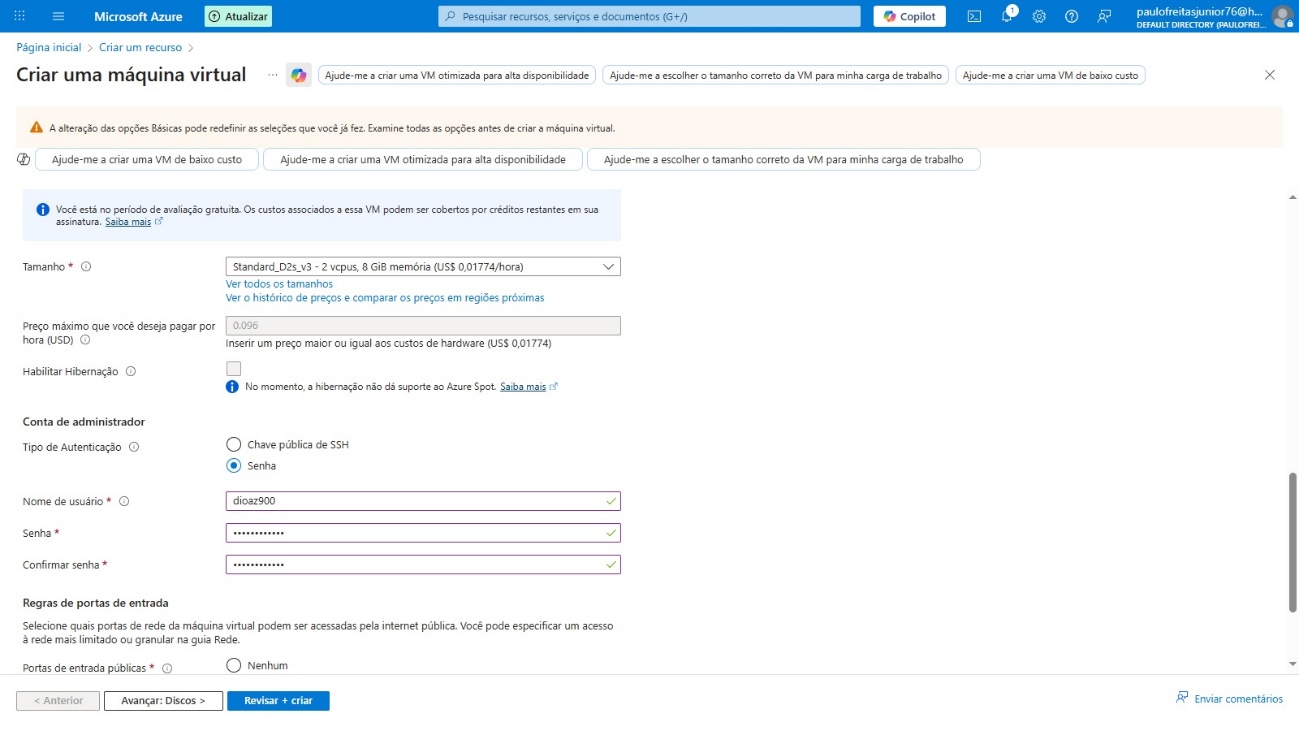
Foi selecionada a execução com **Desconto de Spot do Azure**, confirmando a intenção de utilizar a capacidade de computação não utilizada do Azure a um custo significativamente reduzido.

A configuração da política de remoção é crucial para o gerenciamento de risco e custo:

* **Tipo de Remoção (Eviction Type):** Selecionado Preço ou capacidade. Esta opção é mais rigorosa no controle de custos do que a opção "Somente capacidade". Ela permite que a VM seja removida se o preço Spot exceder o limite máximo definido pelo usuário *ou* se o Azure precisar da capacidade para instâncias Pay-as-you-go.
* **Política de Remoção (Eviction Policy):** Selecionado Excluir. Esta política determina que, no caso de remoção (expulsão), a instância da VM e seus discos efêmeros (se existissem) serão **excluídos permanentemente**. Embora os Discos Gerenciados persistentes sejam retidos, a instância VM deve ser recriada a partir do zero quando a capacidade estiver disponível novamente.

A seleção da política Excluir implica diretamente que a carga de trabalho sendo executada é considerada ***stateless*** ou depende inteiramente de mecanismos de persistência de dados externos. O modelo de aplicação deve ser capaz de lidar com a interrupção abrupta e com a necessidade de re-provisionamento completo da instância, o que é um fator de design essencial para arquiteturas baseadas em VMs Spot.

**IV. Passo 3: Dimensionamento, Preços e Credenciais de Administrador (Imagem 3)**

****

Objetivo é fornecer detalhes essenciais sobre o perfil de desempenho da VM, a estratégia de controle de custos e o acesso inicial.

**4.1. Dimensionamento da Máquina Virtual (Standard\_D2ls\_v3)**

O tamanho da VM selecionado é Standard\_D2ls\_v3, com 2 vCPUs e 8 GiB de memória, ao preço Spot inicial de US$ 0,01774 por hora.

Essa VM pertence à família D de Uso Geral, que oferece um equilíbrio entre CPU e memória. O sufixo 'ls' no nome (Standard\_D2ls\_v3) é indicativo da série Low Cost Storage. Uma característica chave dessa série é a **ausência de armazenamento temporário local** (disco efêmero), o que contribui para um preço de entrada mais baixo da instância. Consequentemente, o sistema operacional e quaisquer operações de cache ou swap dependerão inteiramente do desempenho e da latência dos Discos Gerenciados persistentes anexados, que são cobrados separadamente.

**4.2. Detalhes de Custo Spot e Estratégia de Preço**

O preço máximo que o usuário está disposto a pagar por hora (Preço máximo que você deseja pagar por hora) foi definido em 0,096 USD.

Esta definição do preço máximo é uma mitigação de risco deliberada. O preço Spot atual (US$ 0,01774) é significativamente mais baixo do que o teto de gastos definido (US$ 0,096). Ao estabelecer um teto elevado, foi sinalizado que ***a prioridade é a estabilidade do tempo de atividade***, minimizando a probabilidade de expulsão da VM baseada puramente na flutuação do preço Spot. A instância só será expulsa por preço se o custo subir dramaticamente (mais de 5 vezes o preço atual) ou se a capacidade for requerida pelo Azure. (*Obs: Valores relacionados ao período de Setembro/2025)*

A hibernação da VM está desativada.

**4.3. Configuração da Conta de Administrador**

Para a configuração da conta de administrador Linux, foi definido o **Tipo de Autenticação** como Senha e o **Nome de usuário** como ***dioaz900***.

Embora a autenticação por senha seja funcional, a recomendação de segurança padrão da Microsoft para VMs Linux é sempre priorizar o uso de **Chaves Públicas SSH**. Chaves SSH oferecem um mecanismo de autenticação criptográfica superior, essencial para mitigar o risco de ataques de força bruta, especialmente quando as portas administrativas são expostas publicamente.

(imagem 4)

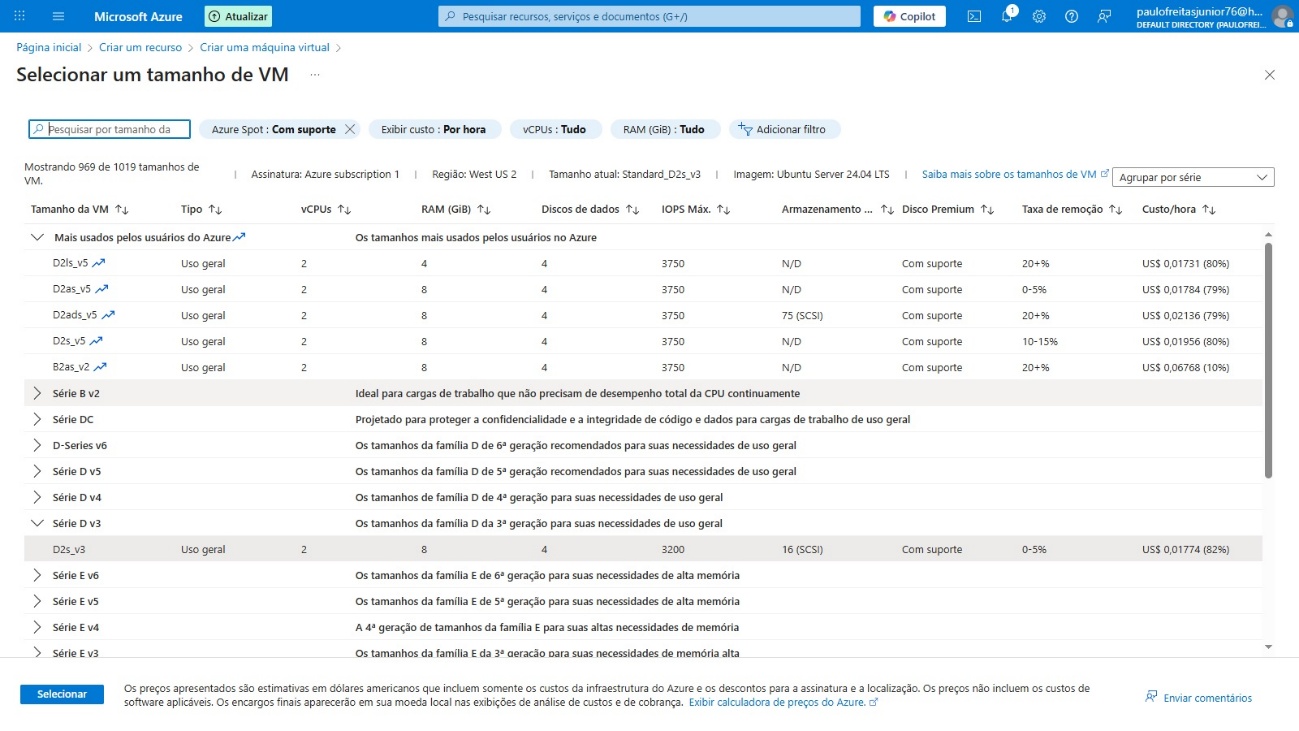
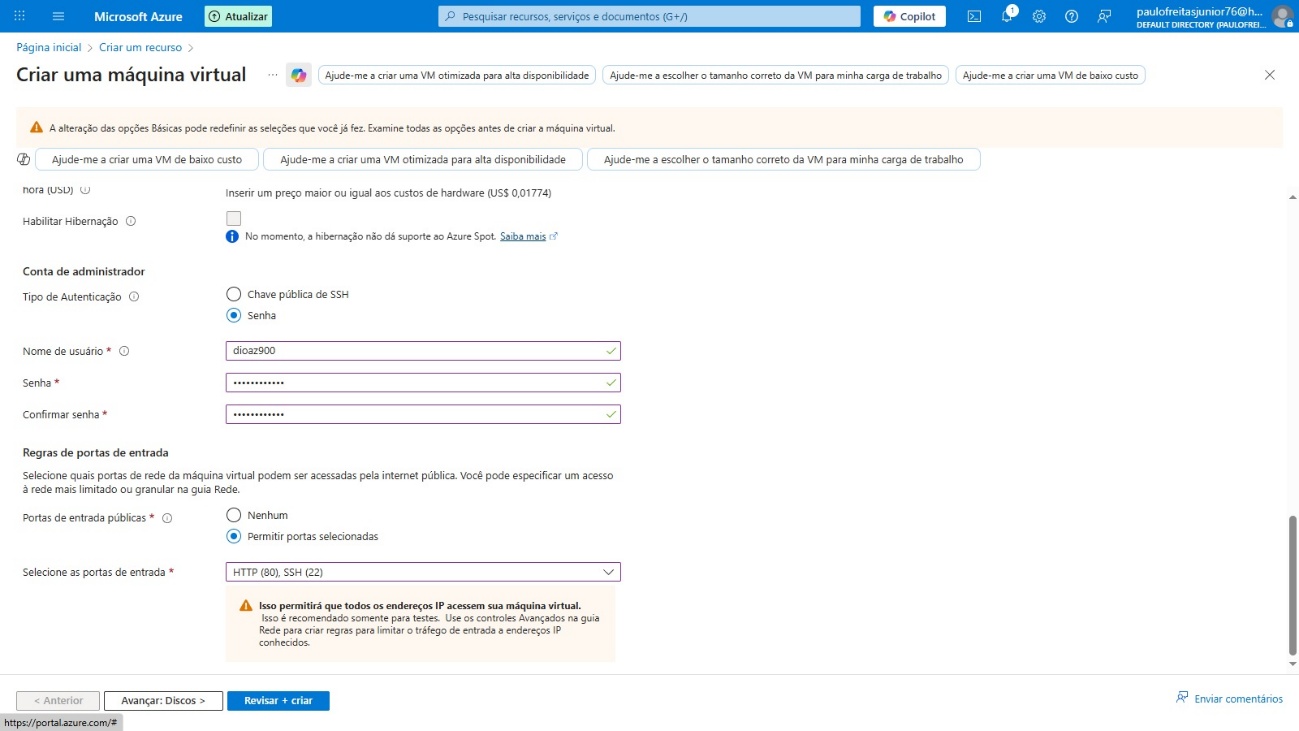


Table 1: Detalhamento do Tamanho e Perfil de Desempenho da VM Standard\_D2ls\_v3

| **Métrica** | **Valor** | **Série VM** | **Análise de Custo/Desempenho** |
| --- | --- | --- | --- |
| Tamanho | Standard\_D2ls\_v3 | Uso Geral (D-family) | Otimizada para custo (low cost storage). |
| vCPUs | 2 | Balanceado. | Performance base suficiente para o SO e aplicações leves. |
| RAM (GiB) | 8 | Proporção 1:4 (CPU:Memória). | Adequado para aplicações que demandam mais memória por núcleo. |
| Armazenamento Temporário | Ausente (Implícito pela série 'ls') | Reduz o custo de entrada, mas aumenta a dependência do IOPS dos discos persistentes. |  |
| Preço Spot (Atual 09/2025) | US$ 0,01774/hora | Valor de desconto significativo. |  |
| Preço Máximo (Cap) (09/2025) | US$ 0,096/hora | Estratégia de estabilidade: alto teto para evitar expulsão por preço. |  |

**V. Passo 4: Definições de Ingressos de Rede e Implicações de Segurança (Análise da Imagem 5)**

****

Objetivo é abordar as regras de portas de entrada, o ponto mais crítico da implantação em termos de segurança de rede.

**5.1. Configuração de Regras de Portas de Entrada**

Na seção Regras de portas de entrada, foi selecionada opção: ***Permitir portas selecionadas*** e especificou duas portas públicas: HTTP (80) e SSH (22).

**5.2. Análise Crítica do Aviso de Segurança do Azure**

A interface do portal exibe um aviso claro: "Isso permitirá que todos os endereços IP acessem sua máquina virtual. É recomendado somente para testes."

Esta configuração implementa imediatamente uma vulnerabilidade de segurança significativa. Ao abrir a **Porta 22 (SSH)** para o mundo (implícita pela configuração de portas selecionadas sem restrições avançadas), a VM fica exposta a varreduras contínuas e ataques automatizados de força bruta, que são comuns em ambientes de nuvem.6 Dado que o usuário selecionou a autenticação por senha (em vez de chave SSH), o risco é maximizado. A filosofia de segurança de rede do Azure (Network Access Control) exige a limitação da conectividade a dispositivos ou sub-redes específicas, um princípio que foi violado pela exposição da porta 22 ao tráfego de entrada da internet pública.7

A abertura da **Porta 80 (HTTP)**, embora necessária para servir tráfego web, não garante a comunicação criptografada, o que é uma deficiência de segurança moderna. A melhor prática é utilizar sempre HTTPS (Porta 443).

**5.3. Recomendações de Mitigação de Risco e Melhores Práticas de Segurança**

A configuração atual da rede deve ser corrigida imediatamente após o provisionamento, pois a exposição administrativa compromete o ambiente. A Microsoft oferece soluções robustas para evitar a abertura de portas administrativas:

1. **Azure Bastion:** Esta é a solução PaaS recomendada. Ela permite que os usuários se conectem à VM via SSH/RDP através do portal Azure usando SSL/TLS na porta 443, eliminando a necessidade de expor as portas 22 ou 3389 ao endereço IP público da VM.
2. **Acesso Just-in-Time (JIT):** Integrado ao Microsoft Defender for Cloud, o JIT é uma ferramenta de segurança que mantém as portas administrativas fechadas por padrão. Ele abre as portas ***somente mediante solicitação aprovada***, por um período limitado (tipicamente até três horas) e apenas para endereços IP de origem especificados. O JIT reduz drasticamente a superfície de ataque ao garantir que o acesso administrativo só seja permitido quando estritamente necessário.

Table 2: Análise de Risco das Portas de Entrada Públicas Selecionadas

| **Porta (Protocolo)** | **Serviço** | **Risco Associado à Abertura Pública (0.0.0.0/0)** | **Melhor Prática Recomendada** |
| --- | --- | --- | --- |
| 22 (TCP) | SSH | Acesso administrativo direto. Exposição a ataques de força bruta, conforme alertado. | Restringir o IP de origem no NSG ou utilizar **Azure Bastion/Acesso JIT**. |
| 80 (TCP) | HTTP | Servidor web não criptografado. Transmissão de dados sensíveis em texto simples. | Mover para HTTPS (443). Usar Application Gateway ou Front Door para WAF e segurança perimetral. |
| Fonte de Entrada | Qualquer IP (0.0.0.0/0) | Superfície de ataque máxima. Viola o princípio de segurança de menor privilégio. | Definir sub-redes de gerenciamento ou Application Security Groups (ASGs) para limitar o acesso. |

**VI. Conclusões e Checklist de Implementação Otimizada**

**6.1. Síntese Arquitetônica**

O provisionamento da Máquina Virtual reflete uma implementação estratégica de Infraestrutura como Serviço (IaaS) projetada para alcançar eficiência de custos sem sacrificar a resiliência regional contra desastres de larga escala.

1. **Otimização de Custo:** O uso de uma Instância Spot (Standard\_D2ls\_v3) e o tamanho de custo otimizado (sem armazenamento temporário) demonstram um foco em minimizar despesas operacionais.
2. **Gerenciamento de Risco de Custo:** A definição de um preço máximo alto (US$ 0,096) (dados de Setembro/2025) para a expulsão Spot é uma tática de gerenciamento de risco que prioriza a disponibilidade da VM em relação à obtenção do custo mais baixo absoluto, protegendo o ambiente contra interrupções frequentes devido a picos de preço de capacidade.
3. **Resiliência Regional:** A implantação em uma Zona de Disponibilidade garante que a instância esteja protegida contra a falha de um datacenter inteiro na região, um diferencial crítico para cargas de trabalho que, embora possam ser interrompidas momentaneamente, não podem tolerar desastres geográficos..

**6.2. Checklist Crítico de Segurança Pós-Provisionamento**

A configuração atual, embora arquitetonicamente sólida em termos de custo e resiliência, apresenta uma falha de segurança de rede de alto risco. As seguintes ações corretivas são obrigatórias imediatamente após o provisionamento da VM:

* **Bloqueio da Porta 22 (SSH):** O Network Security Group (NSG) associado à VM deve ser modificado para restringir o acesso à Porta 22. A origem (Source) da regra de entrada (Ingress) deve ser alterada de Any para um endereço IP de gerenciamento conhecido ou para o Service Tag AzureBastion.
* **Implementação de Acesso Remoto Seguro:** A melhor prática é provisionar o **Azure Bastion** na VNet associada para permitir conexões SSH seguras e privadas através do portal, eliminando a exposição pública da porta 22.
* **Adoção de JIT:** Se o Azure Bastion não for utilizado, a implementação do **Acesso Just-in-Time (JIT)** via Microsoft Defender for Cloud deve ser configurada para garantir que as portas administrativas permaneçam fechadas por padrão.
* **Segurança de Serviço Web:** Se a VM se destina a hospedar um serviço web, a Porta 80 deve ser desativada, e o tráfego deve ser migrado para o protocolo criptografado HTTPS (Porta 443).