**ANÁLISE DETALHADA DE REDE, SEGURANÇA PERIMETRAL E PERFORMANCE**

Este relatório foca na análise das configurações de rede da Máquina Virtual. As escolhas feitas nesta etapa definem a conectividade da VM, o perímetro de segurança e a otimização de desempenho.

**I. Configuração da Interface de Rede (VNet, Subnet e IP Público) (imagem 1)**

A primeira seção do guia "Rede" estabelece a infraestrutura de rede virtual (VNet) onde a VM será implantada.

**1.1. Estrutura da Rede Virtual e Subnet**

O usuário está criando uma nova rede virtual ((Novo) vnet-westus2) e uma nova sub-rede (snet-westus2-1).

* **VNet:** vnet-westus2 (rg-DIO\_AZ900). O nome da VNet está alinhado com o Grupo de Recursos e a região (West US 2), seguindo boas práticas de nomeação. Uma VNet é o limite de rede privado e isolado na nuvem Azure, permitindo que os recursos se comuniquem com segurança entre si, com a internet e com redes locais.
* **Sub-rede:** snet-westus2-1, com o bloco de endereço 172.16.0.0/24. As sub-redes são divisões da VNet, permitindo a organização e o controle de acesso de tráfego (via NSGs).

**1.2. Implantação e Redundância do Endereço IP Público**

O usuário opta por criar um novo IP público, vm-ubuntu-az900-ip (Imagem 2), com características específicas que se alinham à escolha inicial de Zona de Disponibilidade da VM.

* **SKU:** Standard. O SKU Standard é o padrão moderno do Azure, oferecendo recursos aprimorados em comparação com o SKU Basic (que está em processo de aposentadoria).
* **Resiliência Zonal:** A opção selecionada é **Com redundância de zona** (Zone-redundant). Esta configuração é mandatória ao implantar a VM em uma Zona de Disponibilidade. Um IP público com redundância de zona garante que o endereço IP sobreviva à falha de uma única Zona de Disponibilidade, pois o recurso é replicado em várias zonas dentro da região. Isso garante a alta disponibilidade em nível de rede.

O aviso exibido na Imagem 1, "A anexação de um IP público existente está desabilitada quando a zona selecionada pelo Azure é escolhida...", reforça que a arquitetura zonal da VM impõe requisitos específicos para a criação e anexação de recursos de IP público.

**II. Definições de Segurança de Rede (Network Security Group - NSG)**

A seção de Portas de entrada públicas e Grupo de segurança de rede define o perímetro de segurança para a VM.

**2.1. Configuração do NSG**

O usuário escolhe uma configuração de NSG simplificada (possivelmente Básico ou inline) ao selecionar **Permitir portas selecionadas** sob o Grupo de segurança de rede do adaptador. Um Network Security Group (NSG) atua como um firewall, filtrando o tráfego de rede de entrada (inbound) e saída (outbound) para a VM.

**2.2. O Risco Crítico das Portas de Entrada**

O usuário selecionou explicitamente a abertura das seguintes portas:

* **HTTP (80)**
* **SSH (22)**

O portal Azure emite um aviso de segurança severo: **"Isso permitirá que todos os endereços IP acessem sua máquina virtual. Isso é recomendado somente para testes."**

* **Exposição SSH (Porta 22):** Abrir a porta SSH (22) para a internet pública (implícito pela ausência de restrições de IP de origem) expõe a VM a ataques automatizados de força bruta. Este risco é amplificado pelo fato de o usuário ter optado pela autenticação baseada em **Senha** (conforme a análise inicial) em vez de Chaves SSH. A melhor prática de segurança, que foi comprometida, exige o bloqueio da porta 22 ao tráfego de entrada da Internet.
* **Exposição HTTP (Porta 80):** A abertura da Porta 80 para serviços web permite a comunicação, mas não oferece criptografia em trânsito. A recomendação moderna é migrar para HTTPS (Porta 443) para garantir a segurança da comunicação.

A combinação de um IP público com redundância de zona (alta disponibilidade) com portas de gerenciamento abertas ao mundo representa uma falha de segurança que precisa de correção imediata, preferencialmente por meio de serviços como **Azure Bastion** (que acessa a VM por SSH/443 privado) ou **Acesso Just-in-Time (JIT)** (que fecha a porta 22 por padrão, abrindo-a apenas mediante solicitação).

**III. Otimização de Performance e Gerenciamento do Ciclo de Vida**

A seção final da aba "Rede" (Imagem 3) aborda recursos avançados para desempenho e limpeza de recursos.

**3.1. Habilitação de Rede Acelerada**

A opção **Habilitar rede acelerada** está **marcada**.

* **Análise de Performance:** A Rede Acelerada (Accelerated Networking) é uma otimização de desempenho de rede que utiliza a virtualização de E/S de raiz única (SR-IOV). Isso permite que o tráfego de rede ignore o host, reduzindo significativamente a latência, o jitter e a utilização da CPU da VM. É uma escolha de performance recomendada para máquinas virtuais de uso geral, como a série D, quando implantadas com 2 ou mais vCPUs, o que se aplica à VM Standard\_D2ls\_v3.

**3.2. Gerenciamento do Ciclo de Vida do IP e NIC**

A opção **Excluir o IP Público e a NIC quando a VM for excluída** está **marcada**.

* **Análise de Custo e Gerenciamento:** Esta é uma excelente prática operacional, alinhada com a natureza descartável de uma Instância Spot. Ao marcar esta caixa, o Azure garante que a Interface de Rede (NIC) e o Endereço IP Público associados à VM serão removidos automaticamente quando a VM for desalocada ou excluída. Isso evita cobranças desnecessárias por recursos órfãos, complementando a política de exclusão do disco de SO (analisada no relatório anterior).

**3.3. Balanceamento de Carga**

O usuário selecionou **Nenhum** nas Opções de balanceamento de carga.

* **Análise de Arquitetura:** Esta configuração indica que a VM operará como uma instância única, sem distribuição de tráfego por um Load Balancer (Camada 4) ou um Application Gateway (Camada 7). Se o propósito do ambiente for testar uma única instância, essa configuração é aceitável; no entanto, para qualquer carga de trabalho de produção de alta disponibilidade, um balanceador de carga seria necessário para distribuir o tráfego entre várias VMs.