

DOCUMENTAÇÃO DE ARQUITETURA

Microsoft Azure - Infraestrutura de Alta Disponibilidade

Região: Brazil South

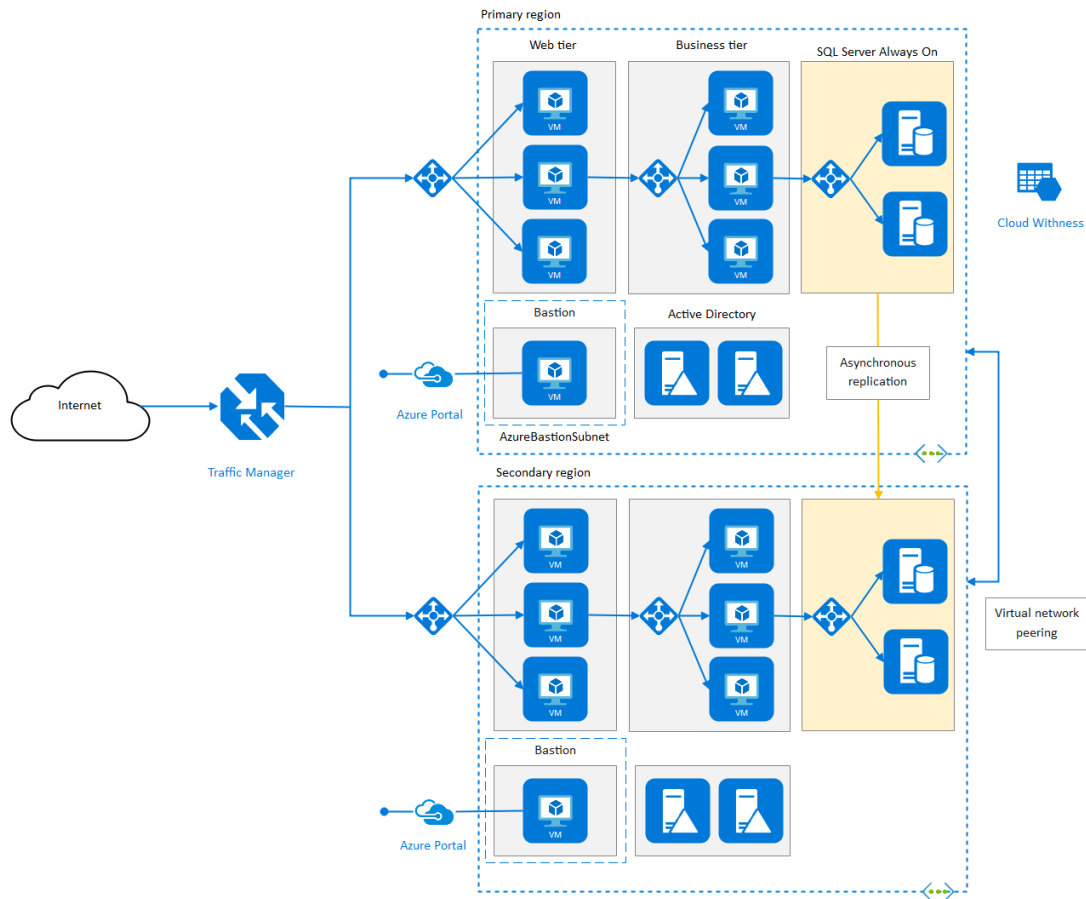
Versão 1.0
Janeiro 2026

Sumário

1. 1. Visão Geral da Arquitetura
2. 2. Topologia de Rede
3. 3. Componentes da Infraestrutura
4. 4. Procedimento de Implantação
5. 5. Configuração de Alta Disponibilidade
6. 6. Segurança e Conformidade
7. 7. Monitoramento e Manutenção
8. 8. Anexos

1. Visão Geral da Arquitetura

Esta documentação descreve a arquitetura de infraestrutura em nuvem Microsoft Azure projetada para alta disponibilidade e resiliência. A solução implementa uma arquitetura multi-tier distribuída em duas regiões geográficas com replicação assíncrona e failover automático.



1.1. Objetivos da Arquitetura

- Garantir disponibilidade de 99.99% para aplicações críticas
- Implementar redundância geográfica com failover automático
- Proporcionar isolamento de segurança através de sub-redes segmentadas
- Otimizar performance através de balanceamento de carga
- Facilitar manutenção e atualizações sem interrupção de serviço

1.2. Principais Características

- Arquitetura Multi-Region: Primary Region (Brazil South) e Secondary Region (Brazil South - zona secundária)
- Segregação de Camadas: Web Tier, Business Tier e Data Tier isoladas
- Alta Disponibilidade: SQL Server Always On com replicação assíncrona
- Acesso Seguro: Bastion Hosts para gerenciamento administrativo
- Conectividade Híbrida: VPN site-to-site e peering entre VNets

2. Topologia de Rede

2.1. Região Primária (Brazil South)

A região primária hospeda todos os componentes ativos da aplicação com redundância em múltiplas zonas de disponibilidade.

2.1.1. Virtual Network

- Nome: VNet-Primary-BrSouth
- Espaço de Endereçamento: 10.1.0.0/16
- Região: Brazil South

2.1.2. Sub-redes

Sub-rede	CIDR	Finalidade	IPs Disponíveis
WebTierSubnet	10.1.1.0/24	Servidores Web Frontend	251
BusinessTierSubnet	10.1.2.0/24	Camada de Negócios	251
DataTierSubnet	10.1.3.0/24	SQL Server Always On	251
AzureBastionSubnet	10.1.250.0/26	Azure Bastion Service	59
GatewaySubnet	10.1.255.0/27	VPN Gateway	27

2.2. Região Secundária (Brazil South - Secondary)

A região secundária mantém réplicas dos componentes críticos para failover e disaster recovery.

2.2.1. Virtual Network

- Nome: VNet-Secondary-BrSouth
- Espaço de Endereçamento: 10.2.0.0/16
- Região: Brazil South (Zona Alternativa)
- Virtual Network Peering: Conectada à VNet Primária

3. Componentes da Infraestrutura

3.1. Traffic Manager

O Azure Traffic Manager atua como balanceador de carga global DNS-based, direcionando o tráfego de usuários para a região primária e automaticamente redirecionando para a região secundária em caso de falha.

3.1.1. Configurações

- Nome: tm-prod-app-brsouth
- Método de Roteamento: Priority
- Protocolo de Monitoramento: HTTPS
- Porta de Monitoramento: 443
- Caminho de Verificação: /health
- TTL: 60 segundos

3.2. Web Tier

A camada Web hospeda os servidores frontend que atendem as requisições dos usuários. Implementa balanceamento de carga e auto-scaling para garantir disponibilidade e performance.

3.2.1. Máquinas Virtuais

- SKU: Standard_D4s_v5 (4 vCPUs, 16 GB RAM)
- Sistema Operacional: Ubuntu Server 22.04 LTS
- Quantidade por Região: 3 VMs
- Disponibilidade: Distribuídas em Availability Zones
- Disco OS: Premium SSD 128 GB
- Disco Dados: Premium SSD 256 GB

3.2.2. Load Balancer

- Tipo: Application Load Balancer (Layer 7)
- SKU: Standard
- Algoritmo: Round Robin
- Health Probe: HTTP:80/health
- Session Affinity: Cookie-based

3.3. Business Tier

A camada de negócios processa a lógica da aplicação e se comunica com a camada de dados. Isolada em sub-rede privada para maior segurança.

3.3.1. Máquinas Virtuais

- SKU: Standard_D8s_v5 (8 vCPUs, 32 GB RAM)
- Sistema Operacional: Ubuntu Server 22.04 LTS
- Quantidade por Região: 3 VMs
- Disponibilidade: Distribuídas em Availability Zones
- Disco OS: Premium SSD 128 GB
- Disco Dados: Premium SSD 512 GB

3.4. Data Tier - SQL Server Always On

A camada de dados utiliza SQL Server Always On Availability Groups para garantir alta disponibilidade e recuperação de desastres com replicação síncrona na região primária e assíncrona entre regiões.

3.4.1. Máquinas Virtuais SQL Server

- SKU: Standard_D16s_v5 (16 vCPUs, 64 GB RAM)
- Sistema Operacional: Windows Server 2022 Datacenter
- SQL Server: Enterprise 2022
- Quantidade Região Primária: 2 VMs (Always On)
- Quantidade Região Secundária: 2 VMs (Always On Replicas)
- Disco OS: Premium SSD 256 GB
- Disco Dados: Premium SSD 1 TB
- Disco Logs: Premium SSD 512 GB

3.4.2. Always On Configuration

- Availability Group: AG-Production
- Modo de Disponibilidade Primário: Synchronous Commit
- Modo de Disponibilidade Secundário: Asynchronous Commit
- Failover Mode: Automatic
- Listener: ag-prod-listener.database.local
- Porta: 1433

3.5. Azure Bastion

Azure Bastion fornece conectividade RDP e SSH segura para as máquinas virtuais sem expor portas públicas, eliminando a necessidade de jump boxes.

- SKU: Standard
- Instâncias: 2 por região
- Protocolos: RDP, SSH
- Integração: Azure AD para autenticação

3.6. Azure Portal / Cloud Witness

Cloud Witness é um recurso do Windows Server Failover Clustering que utiliza Azure Blob Storage como ponto de arbitragem para o quorum do cluster.

- Tipo: Azure Storage Account
- Replicação: Geo-Redundant Storage (GRS)
- Finalidade: Quorum testemunha para SQL Cluster

4. Procedimento de Implantação

4.1. Pré-requisitos

- Assinatura Azure ativa com permissões de Contributor ou Owner
- Azure CLI instalado e configurado
- Azure PowerShell instalado
- Acesso ao Azure Portal
- Licenças SQL Server Enterprise
- Certificados SSL/TLS válidos

4.2. Etapa 1: Criação do Resource Group

Execute os comandos Azure CLI para criar os resource groups nas duas regiões:

```
az group create --name RG-Production-Primary --location  
brazilsouth
```

```
az group create --name RG-Production-Secondary --  
location brazilsouth
```

4.3. Etapa 2: Criação das Virtual Networks

4.3.1. VNet Primária

```
# Criar VNet Primária  
az network vnet create \  
--resource-group RG-Production-Primary \  
--name VNet-Primary-BrSouth \  
--address-prefix 10.1.0.0/16 \  
--location brazilsouth
```

4.3.2. Sub-redes Primárias

```
# Web Tier Subnet  
az network vnet subnet create \  
--resource-group RG-Production-Primary \  
--vnet-name VNet-Primary-BrSouth \  
--name WebTierSubnet \  
--address-prefix 10.1.1.0/24  
  
# Business Tier Subnet  
az network vnet subnet create \  
--resource-group RG-Production-Primary \  

```

```
--vnet-name VNet-Primary-BrSouth \  
--name BusinessTierSubnet \  
--address-prefix 10.1.2.0/24  
  
# Data Tier Subnet  
az network vnet subnet create \  
--resource-group RG-Production-Primary \  
--vnet-name VNet-Primary-BrSouth \  
--name DataTierSubnet \  
--address-prefix 10.1.3.0/24  
  
# Azure Bastion Subnet  
az network vnet subnet create \  
--resource-group RG-Production-Primary \  
--vnet-name VNet-Primary-BrSouth \  
--name AzureBastionSubnet \  
--address-prefix 10.1.250.0/26  
  
# Gateway Subnet  
az network vnet subnet create \  
--resource-group RG-Production-Primary \  
--vnet-name VNet-Primary-BrSouth \  
--name GatewaySubnet \  
--address-prefix 10.1.255.0/27
```

4.3.3. VNet Secundária

```
# Criar VNet Secundária  
az network vnet create \  
--resource-group RG-Production-Secondary \  
--name VNet-Secondary-BrSouth \  
--address-prefix 10.2.0.0/16 \  
--location brazilsouth  
  
# Criar Sub-redes (mesmo padrão da primária com prefixo  
10.2.x.x)
```

4.4. Etapa 3: VNet Peering

Estabelecer peering bidirecional entre as VNets primária e secundária para permitir comunicação privada:

```
# Peering Primária -> Secundária
az network vnet peering create \
  --resource-group RG-Production-Primary \
  --name Primary-to-Secondary \
  --vnet-name VNet-Primary-BrSouth \
  --remote-vnet /subscriptions/{subscription-id}/resourceGroups/RG-
Production-Secondary/providers/Microsoft.Network/virtualNetworks/VNet-
Secondary-BrSouth \
  --allow-vnet-access \
  --allow-forwarded-traffic

# Peering Secundária -> Primária
az network vnet peering create \
  --resource-group RG-Production-Secondary \
  --name Secondary-to-Primary \
  --vnet-name VNet-Secondary-BrSouth \
  --remote-vnet /subscriptions/{subscription-id}/resourceGroups/RG-
Production-Primary/providers/Microsoft.Network/virtualNetworks/VNet-
Primary-BrSouth \
  --allow-vnet-access \
  --allow-forwarded-traffic
```

4.5. Etapa 4: Network Security Groups (NSGs)

Criar e configurar NSGs para controlar o tráfego entre as camadas:

4.5.1. NSG Web Tier

```
# Criar NSG
az network nsg create \
  --resource-group RG-Production-Primary \
  --name NSG-WebTier

# Permitir HTTP da Internet
az network nsg rule create \
  --resource-group RG-Production-Primary \
  --nsg-name NSG-WebTier \
  --name Allow-HTTP \
  --priority 100 \
  --source-address-prefixes Internet \
  --destination-port-ranges 80 \
  --access Allow \
  --protocol Tcp

# Permitir HTTPS da Internet
az network nsg rule create \
  --resource-group RG-Production-Primary \
  --nsg-name NSG-WebTier \
```

```
--name Allow-HTTPS \  
--priority 110 \  
--source-address-prefixes Internet \  
--destination-port-ranges 443 \  
--access Allow \  
--protocol Tcp
```

```
# Associar NSG à subnet  
az network vnet subnet update \  
--resource-group RG-Production-Primary \  
--vnet-name VNet-Primary-BrSouth \  
--name WebTierSubnet \  
--network-security-group NSG-WebTier
```

4.5.2. NSG Business Tier

```
# Criar NSG
az network nsg create \
  --resource-group RG-Production-Primary \
  --name NSG-BusinessTier

# Permitir tráfego da Web Tier
az network nsg rule create \
  --resource-group RG-Production-Primary \
  --nsg-name NSG-BusinessTier \
  --name Allow-From-WebTier \
  --priority 100 \
  --source-address-prefixes 10.1.1.0/24 \
  --destination-port-ranges 8080 \
  --access Allow \
  --protocol Tcp

# Associar NSG à subnet
az network vnet subnet update \
  --resource-group RG-Production-Primary \
  --vnet-name VNet-Primary-BrSouth \
  --name BusinessTierSubnet \
  --network-security-group NSG-BusinessTier
```

4.5.3. NSG Data Tier

```
# Criar NSG
az network nsg create \
  --resource-group RG-Production-Primary \
  --name NSG-DataTier

# Permitir SQL da Business Tier
az network nsg rule create \
  --resource-group RG-Production-Primary \
  --nsg-name NSG-DataTier \
  --name Allow-SQL-From-BusinessTier \
  --priority 100 \
  --source-address-prefixes 10.1.2.0/24 \
  --destination-port-ranges 1433 \
  --access Allow \
  --protocol Tcp

# Permitir Always On entre réplicas
az network nsg rule create \
  --resource-group RG-Production-Primary \
  --nsg-name NSG-DataTier \
  --name Allow-AlwaysOn-Primary \
  --priority 110 \
  --source-address-prefixes 10.1.3.0/24 \
  --destination-port-ranges 5022 \
  --access Allow \
  --protocol Tcp

# Permitir Always On da região secundária
az network nsg rule create \
```

```
--resource-group RG-Production-Primary \  
--nsg-name NSG-DataTier \  
--name Allow-AlwaysOn-Secondary \  
--priority 120 \  
--source-address-prefixes 10.2.3.0/24 \  
--destination-port-ranges 5022 \  
--access Allow \  
--protocol Tcp
```

```
# Associar NSG à subnet  
az network vnet subnet update \  
--resource-group RG-Production-Primary \  
--vnet-name VNet-Primary-BrSouth \  
--name DataTierSubnet \  
--network-security-group NSG-DataTier
```

4.6. Etapa 5: Criação das Máquinas Virtuais - Web Tier

Criar as VMs Web distribuídas em Availability Zones:

```
# Criar Availability Set (alternativa às Zones)
az vm availability-set create \
  --resource-group RG-Production-Primary \
  --name AS-WebTier \
  --platform-fault-domain-count 3 \
  --platform-update-domain-count 5
```

```
# VM Web 1 - Zone 1
az vm create \
  --resource-group RG-Production-Primary \
  --name vm-web-01 \
  --location brazilsouth \
  --zone 1 \
  --size Standard_D4s_v5 \
  --image Ubuntu2204 \
  --vnet-name VNet-Primary-BrSouth \
  --subnet WebTierSubnet \
  --admin-username azureuser \
  --generate-ssh-keys \
  --os-disk-size-gb 128 \
  --storage-sku Premium_LRS \
  --data-disk-sizes-gb 256 \
  --public-ip-address ""
```

```
# Repetir para vm-web-02 (zone 2) e vm-web-03 (zone 3)
```

5. Configuração de Alta Disponibilidade

5.1. Windows Server Failover Clustering (WSFC)

5.1.1. Pré-requisitos

- Active Directory Domain Services configurado
- Todas as VMs SQL ingressadas no domínio
- Conta de serviço dedicada para SQL Server
- Storage Account para Cloud Witness

5.1.2. Instalação do Feature Failover Clustering

Executar em todas as VMs SQL Server via PowerShell:

```
# Instalar Feature Failover Clustering  
Install-WindowsFeature -Name Failover-Clustering -  
IncludeManagementTools
```

```
# Reiniciar servidor  
Restart-Computer -Force
```

5.1.3. Criação do Cluster

```
# Validar configuração do cluster  
Test-Cluster -Node vm-sql-primary-01, vm-sql-primary-02, vm-sql-secondary-  
01, vm-sql-secondary-02
```

```
# Criar cluster  
New-Cluster -Name SQLCluster -Node vm-sql-primary-01, vm-sql-primary-02,  
vm-sql-secondary-01, vm-sql-secondary-02 -StaticAddress 10.1.3.10 -  
NoStorage
```

```
# Configurar Cloud Witness  
$StorageAccountName = "sacloudwitness"  
$StorageAccountKey = "<storage-account-key>"
```

```
Set-ClusterQuorum -CloudWitness -AccountName $StorageAccountName -  
AccessKey $StorageAccountKey
```

5.2. SQL Server Always On Availability Groups

5.2.1. Habilitar Always On

```
# Executar em cada instância SQL via SQL Server Configuration Manager  
# Ou via PowerShell:
```


Import-Module SqlServer

```
$nodes = @(  
    "vm-sql-primary-01",  
    "vm-sql-primary-02",  
    "vm-sql-secondary-01",  
    "vm-sql-secondary-02"  
)
```

```
foreach ($node in $nodes) {  
    Enable-SqlAlwaysOn -ServerInstance $node -Force  
}
```

5.2.2. Criar Availability Group

```
-- Criar Endpoint em cada servidor
CREATE ENDPOINT AlwaysOn_Endpoint
STATE = STARTED
AS TCP (LISTENER_PORT = 5022)
FOR DATABASE_MIRRORING (
    ROLE = ALL,
    AUTHENTICATION = WINDOWS_NEGOTIATE,
    ENCRYPTION = REQUIRED_ALGORITHM_AES
);
GO

-- Criar Availability Group
CREATE AVAILABILITY GROUP [AG-Production]
FOR DATABASE [ProductionDB]
REPLICA ON
    -- Primário 1 (Synchronous)
    N'vm-sql-primary-01' WITH (
        ENDPOINT_URL = N'TCP://vm-sql-primary-01.domain.local:5022',
        AVAILABILITY_MODE = SYNCHRONOUS_COMMIT,
        FAILOVER_MODE = AUTOMATIC,
        BACKUP_PRIORITY = 50,
        SECONDARY_ROLE(ALLOW_CONNECTIONS = NO)
    ),
    -- Primário 2 (Synchronous)
    N'vm-sql-primary-02' WITH (
        ENDPOINT_URL = N'TCP://vm-sql-primary-02.domain.local:5022',
        AVAILABILITY_MODE = SYNCHRONOUS_COMMIT,
        FAILOVER_MODE = AUTOMATIC,
        BACKUP_PRIORITY = 50,
        SECONDARY_ROLE(ALLOW_CONNECTIONS = READ_ONLY)
    ),
    -- Secundário 1 (Asynchronous)
    N'vm-sql-secondary-01' WITH (
        ENDPOINT_URL = N'TCP://vm-sql-secondary-01.domain.local:5022',
        AVAILABILITY_MODE = ASYNCHRONOUS_COMMIT,
        FAILOVER_MODE = MANUAL,
        BACKUP_PRIORITY = 25,
        SECONDARY_ROLE(ALLOW_CONNECTIONS = READ_ONLY)
    ),
    -- Secundário 2 (Asynchronous)
    N'vm-sql-secondary-02' WITH (
        ENDPOINT_URL = N'TCP://vm-sql-secondary-02.domain.local:5022',
        AVAILABILITY_MODE = ASYNCHRONOUS_COMMIT,
        FAILOVER_MODE = MANUAL,
        BACKUP_PRIORITY = 25,
        SECONDARY_ROLE(ALLOW_CONNECTIONS = READ_ONLY)
    );
GO
```

5.2.3. Criar Listener

```
-- Criar Listener para o Availability Group
ALTER AVAILABILITY GROUP [AG-Production]
ADD LISTENER N'ag-prod-listener' (
```

```
WITH IP (  
  (N'10.1.3.100', N'255.255.255.0'),  
  (N'10.2.3.100', N'255.255.255.0')  
),  
PORT = 1433  
);  
GO
```

6. Segurança e Conformidade

6.1. Azure Security Center

- Habilitar Azure Defender para todas as VMs
- Configurar alertas de segurança
- Implementar recomendações de hardening

6.2. Azure Key Vault

Criar Key Vault para armazenamento seguro de credenciais:

```
# Criar Key Vault
az keyvault create \
  --resource-group RG-Production-Primary \
  --name kv-prod-secrets \
  --location brazilsouth \
  --enabled-for-deployment true \
  --enabled-for-disk-encryption true

# Armazenar senha do SQL Admin
az keyvault secret set \
  --vault-name kv-prod-secrets \
  --name sql-admin-password \
  --value '{SenhaSegura123!}'
```

6.3. Backup e Recovery

6.3.1. Azure Backup para VMs

```
# Criar Recovery Services Vault
az backup vault create \
  --resource-group RG-Production-Primary \
  --name rsv-prod-backup \
  --location brazilsouth

# Habilitar backup para VMs
for vm in vm-web-01 vm-web-02 vm-web-03 vm-biz-01 vm-biz-02 vm-biz-03; do
  az backup protection enable-for-vm \
    --resource-group RG-Production-Primary \
    --vault-name rsv-prod-backup \
    --vm $vm \
    --policy-name DefaultPolicy
done
```

6.3.2. SQL Server Backup

- Backup Full: Diário às 02:00 AM
- Backup Diferencial: A cada 6 horas
- Backup de Log: A cada 15 minutos
- Retenção: 30 dias local, 90 dias Azure Blob Storage

7. Monitoramento e Manutenção

7.1. Azure Monitor

Configurar Log Analytics Workspace e métricas:

```
# Criar Log Analytics Workspace
az monitor log-analytics workspace create \
  --resource-group RG-Production-Primary \
  --workspace-name law-prod-monitoring \
  --location brazilsouth

# Conectar VMs ao Workspace
WORKSPACE_ID=$(az monitor log-analytics workspace show \
  --resource-group RG-Production-Primary \
  --workspace-name law-prod-monitoring \
  --query customerId -o tsv)

WORKSPACE_KEY=$(az monitor log-analytics workspace get-shared-keys \
  --resource-group RG-Production-Primary \
  --workspace-name law-prod-monitoring \
  --query primarySharedKey -o tsv)

# Instalar agente em todas as VMs
for vm in vm-web-01 vm-web-02 vm-web-03 vm-biz-01 vm-biz-02 vm-biz-03; do
  az vm extension set \
    --resource-group RG-Production-Primary \
    --vm-name $vm \
    --name OmsAgentForLinux \
    --publisher Microsoft.EnterpriseCloud.Monitoring \
    --settings "{\"workspaceId\":\"$WORKSPACE_ID\"}" \
    --protected-settings "{\"workspaceKey\":\"$WORKSPACE_KEY\"}"
done
```

7.2. Alertas Críticos

7.2.1. Métricas a Monitorar

Componente	Métrica	Threshold Crítico
VMs Web/Business	CPU Utilization	> 85% por 15 min
VMs Web/Business	Memory Available	< 500 MB
SQL Server	AG Synchronization Health	Not Healthy
SQL Server	Disk Latency	> 20ms
Load Balancer	Unhealthy Instances	> 2 instâncias
Traffic Manager	Endpoint Status	Degraded

7.3. Manutenção Preventiva

7.3.1. Janelas de Manutenção

- Domingos: 02:00 - 06:00 (horário de Brasília)

- Patches Windows: Primeiro domingo do mês
- Patches Linux: Segundo domingo do mês
- SQL Server Maintenance: Terceiro domingo do mês

7.3.2. Tarefas Recorrentes

- Diário: Verificação de backups e alertas
- Semanal: Análise de performance e capacity planning
- Mensal: Teste de failover e DR
- Trimestral: Revisão de custos e otimizações

8. Anexos

8.1. Glossário

- **AG:** Availability Group
- **AZ:** Availability Zone
- **CIDR:** Classless Inter-Domain Routing
- **GRS:** Geo-Redundant Storage
- **LRS:** Locally Redundant Storage
- **NSG:** Network Security Group
- **RDP:** Remote Desktop Protocol
- **RPO:** Recovery Point Objective
- **RTO:** Recovery Time Objective
- **SLA:** Service Level Agreement
- **SSH:** Secure Shell
- **VNet:** Virtual Network
- **WSFC:** Windows Server Failover Clustering

8.2. Referências

- Microsoft Azure Documentation: <https://docs.microsoft.com/azure>
- SQL Server Always On Availability Groups:
<https://docs.microsoft.com/sql/database-engine/availability-groups>
- Azure Traffic Manager: <https://docs.microsoft.com/azure/traffic-manager>
- Azure Bastion: <https://docs.microsoft.com/azure/bastion>
- Azure Monitor: <https://docs.microsoft.com/azure/azure-monitor>

8.3. Histórico de Revisões

Versão	Data	Autor	Descrição
1.0	Janeiro 2026	Arquiteto de Soluções	Versão inicial

8.4. Contatos e Suporte

Equipe de Infraestrutura Azure
Email: azure-infra@empresa.com.br
Telefone: +55 (11) 1234-5678

Suporte Microsoft Azure
Portal: <https://portal.azure.com>
Suporte Técnico: Através do Azure Portal > Help + Support