A ARQUITETURA E OS SERVIÇOS DO AZURE

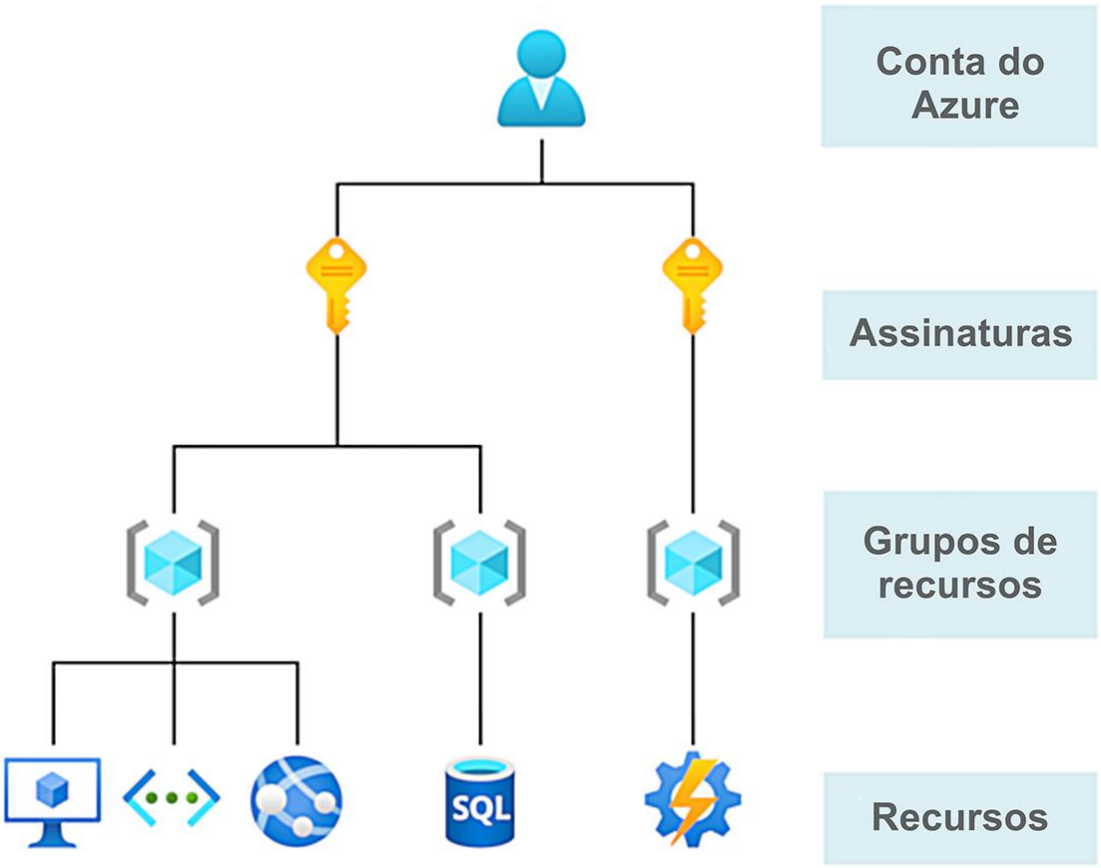
O que é Microsoft Azure?

O Azure é a nuvem da Microsoft, um conjunto de serviços de nuvem, em constante crescimento, que ajuda você a superar os desafios empresariais atuais e se preparar para os desafios futuros. Oferece a oportunidade de criar, gerenciar e implantar aplicativos em uma enorme rede global usando suas ferramentas e estruturas favoritas.

Contas do Azure

Para criar e utilizar recursos do Azure você precisa criar uma assinatura, que é o limite lógico e de custos do seu diretório. Recursos são alocados a assinaturas e um diretório pode ter uma ou mais assinaturas. Ao criar uma conta no Azure, automaticamente você cria o diretório e sua primeira assinatura.

Você pode criar mais assinaturas no seu diretório, por exemplo: você criou a conta da sua empresa e definiu que cada setor terá uma assinatura específica. Após a criação dessa estrutura, você poderá criar seus recursos dentro de cada assinatura específica.



Esquema de criação e funcionamento da conta Azure.

O que é uma conta gratuita do Azure?

A conta gratuita do Azure é uma assinatura com acesso gratuito a produtos populares do Azure por 12 meses, com um crédito de 100 dólares para serem utilizados em até 30 dias, além disso você terá à disposição mais de 25 produtos que são sempre gratuitos.

Infraestrutura física

Os datacenters são a base da infraestrutura física do Azure, possuem grande poder computacional e são distribuídos ao redor do mundo. São instalações com recursos redundantes e poderosos, vários links de operadoras de internet, infraestrutura de rede dedicada, servidores e switches organizados em racks e com refrigeração, nobreaks e fornecimento de energia individuais.

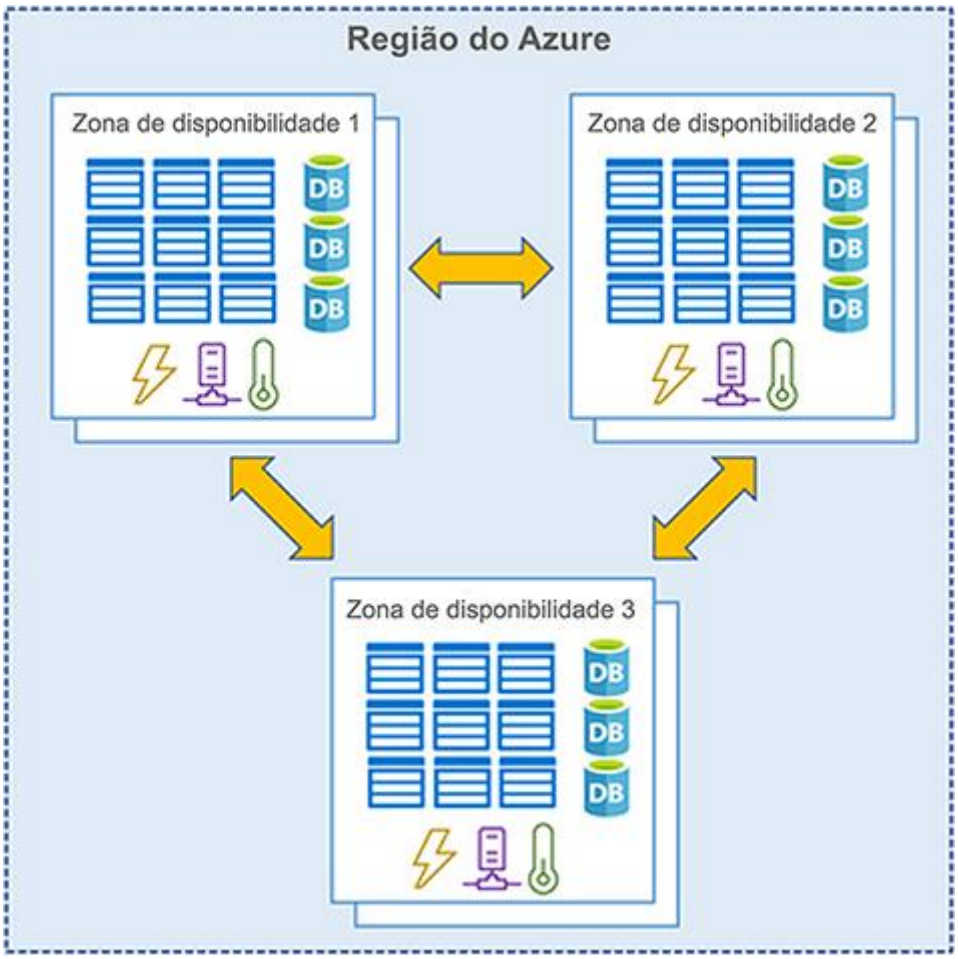
Datacenter.

Regiões

As regiões do Azure são áreas geográficas do planeta que possuem ao menos um datacenter, e, possivelmente, vários outros próximos, o que proporciona redes de baixa latência conectadas por redes de fibra ótica. Cada região garante a residência dos dados. Portanto, se uma máquina virtual for criada na região Sul do Brasil, por exemplo, a Microsoft garante que os dados estão localizados no Brasil. O Azure garante que as cargas de trabalho sejam balanceadas corretamente dentro das regiões disponibilizadas.

Zonas de disponibilidade

São datacenters dentro da mesma região que são separados fisicamente, mas conectados a uma rede de alta velocidade. Cada zona possui um ou mais datacenters, geralmente até três com energia, refrigeração e rede independentes. Uma zona é um limite de isolamento de forma que, caso uma zona fique indisponível, as outras continuam funcionando.



Zonas de disponibilidade do Azure.

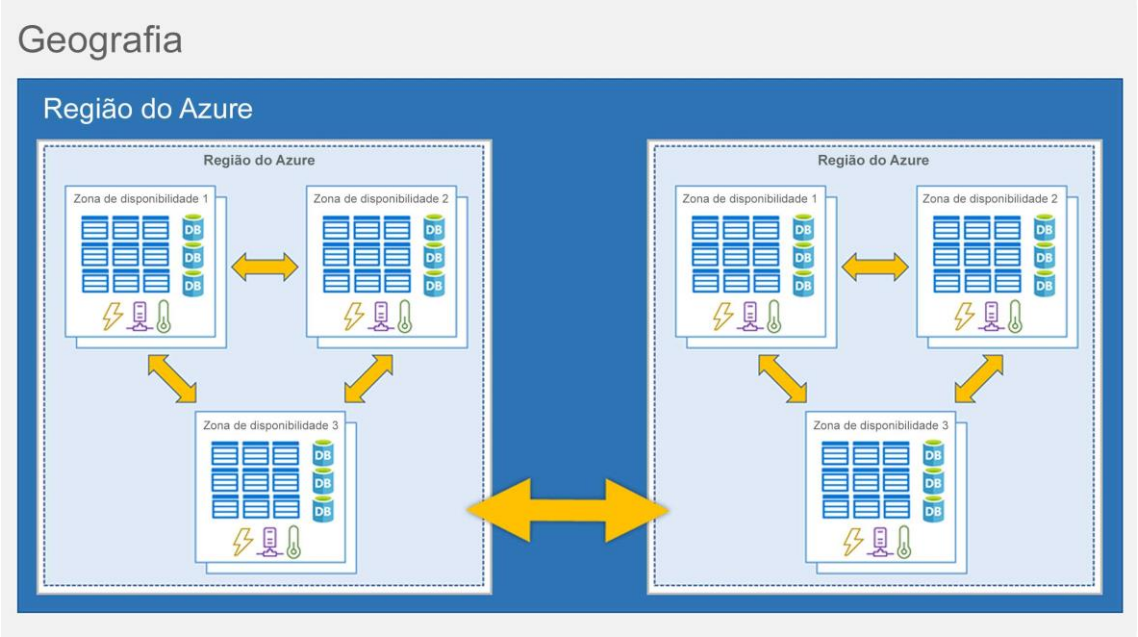
Pares de regiões

O emparelhamento de regiões proporciona a redução da possibilidade de interrupções devido a desastres naturais (enchentes, terremotos etc.), quedas de energia, conflitos civis (guerras) e interrupções de rede física na região específica. A maioria das regiões possui o seu par na mesma geografia, ou a pelo menos 300 milhas, ou 480 km. Alguns serviços do Azure já possuem, habilitados por padrão, essa configuração de regiões pares, possibilitando que, em caso de algum dos desastres citado, ocorra a migração do serviço para a região par.

Exemplo

Se um serviço no Leste dos EUA falhar, o serviço pode subir automaticamente na região par que é o Oeste dos EUA.

Veja a divisão das regiões por pares:



Azure e suas regiões.

Recursos e grupos de recursos do Azure

Um recurso é um container ou caixa, no qual todos os recursos são literalmente alocados como em uma gaveta de guarda-roupa. Qualquer recurso que for criado necessita de um grupo de recursos, como máquinas virtuais, bancos de dados, redes virtuais etc. Todos esses são recursos que, obrigatoriamente, precisam estar em um grupo de recursos.

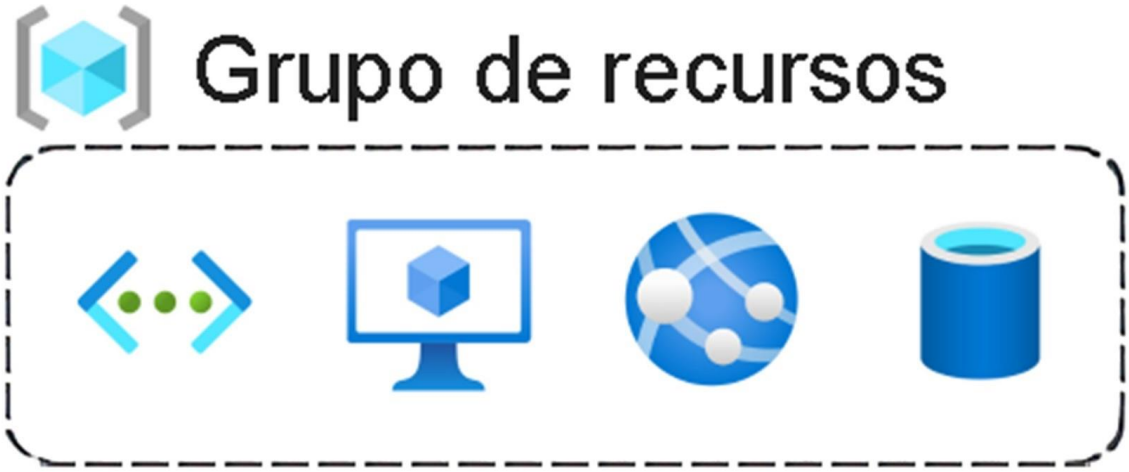


Ilustração dos grupos de recursos.

Uma das características dos grupos de recursos é que um recurso pode pertencer unicamente a um grupo de recursos, ou seja, o mesmo recurso não pode estar em mais de um grupo de recurso. Entretanto, você pode mover recursos entre grupo de recursos. Além disso, não podemos aninhar grupo de recursos, colocar um dentro do outro.

Os grupos de recursos foram criados para a organização dos recursos e normalmente são organizados por setor, região ou empresas. Ao aplicar uma política ou ação a um grupo de recursos, essa ação será aplicada a todos os recursos contidos nesse grupo.

Assinaturas do Azure

Têm um papel fundamental no gerenciamento, cobrança e escala. Servem para a organização lógica dos recursos, permitindo organizar, de forma lógica, seus grupos de recursos e facilitar a cobrança, pois são responsáveis pela bilhetagem e cobrança daquilo que está sendo utilizado.

Esquematização do funcionamento da conta e assinaturas no Azure.

A assinatura do Azure é necessária para utilização dos recursos de maneira que, sem uma assinatura, não podemos criar e gerenciar recursos. Outra característica da assinatura é a possibilidade de fornecer acesso autenticado e autorizado aos serviços do Azure. Ao criar a assinatura, você pode associá-la à sua conta do Azure, que é uma identidade (diretório) no Azure AD (Azure Active Directory).

Podemos usar dois tipos de limites de assinatura:

Limite de cobrança

São requisitos de cobrança conforme o tipo e quantidade de assinaturas realizadas pelo uso de uma conta do Azure.

Limite de controle de acesso

São políticas de gerenciamento de acesso no nível da assinatura da conta Azure, de maneira que podemos criar assinaturas separadas para refletir diferentes estruturas organizacionais.

Serviços de computação e rede do Azure

Máquinas virtuais do Azure

As máquinas virtuais (VMs, de virtual machines) do Azure nos permitem criar e usar VMs na nuvem. As VMs fornecem IaaS (infraestrutura como serviço) na forma de um servidor virtualizado e podem ser usadas de várias maneiras.

Como em um computador físico, você pode personalizar todos os programas de software em execução na VM. As VMs são uma opção ideal quando você precisa de:

- Controle total sobre o SO (sistema operacional).
- Capacidade para executar um software personalizado.
- Usar configurações personalizadas de hospedagem.

Conjuntos de escala de máquinas virtual

Os conjuntos de dimensionamento de máquinas virtuais permitem criar e gerenciar um grupo de VMs idênticas e com balanceamento de carga. Se você

simplesmente criou várias VMs com a mesma finalidade, precisará garantir que todas elas foram configuradas de modo idêntico e configurar parâmetros de roteamento de rede para garantir sua eficiência. Você também precisa monitorar a utilização para determinar se precisa aumentar ou diminuir o número de VMs.

Com conjuntos de dimensionamento de máquinas virtuais, o Azure automatiza a maior parte desse trabalho. Esses conjuntos de dimensionamento permitem que você gerencie, configure e atualize centralmente, em minutos, um grande número de VMs.

Recursos da máquina virtual

Ao provisionar uma VM, você também terá a oportunidade de escolher os recursos associados a ela, incluindo:

1. Tamanho

   Finalidade, número de núcleos de processador e quantidade de RAM.

2. Discos de armazenamento

   Unidades de disco rígido, unidades de estado sólido etc.

3. Rede

   Rede virtual, endereço IP público e configuração de porta.

Área de trabalho virtual do Azure (Azure Virtual Desktop)

É outro tipo de máquina virtual, um serviço de virtualização de área de trabalho e aplicativos que é executado na nuvem. Ele permite você usar uma versão do Windows hospedada na nuvem em qualquer localização.

A área de trabalho virtual do Azure opera em dispositivos e sistemas operacionais e funciona com aplicativos que você pode usar para acessar áreas de trabalho remotas ou a maioria dos navegadores modernos.

A área de trabalho virtual do Azure permite que você use a multissessão do Windows 10 ou Windows 11 Enterprise, único sistema operacional baseado em cliente Windows que habilita vários usuários simultâneos em uma VM. Também fornece uma experiência mais consistente com suporte a aplicativos, mais ampla, em comparação com sistemas operacionais baseados no Windows Server.

Contêineres do Azure

Contêineres são um ambiente de virtualização. Assim como a execução de várias máquinas virtuais em um só host físico, você pode executar vários contêineres em apenas um host físico ou virtual. Diferentemente das máquinas virtuais, você não gerencia o sistema operacional para um contêiner.

Máquinas virtuais

Parecem ser uma instância de um sistema operacional que você pode gerenciar e às quais pode se conectar.

Contêineres

São leves e projetados para serem criados, dimensionados e interrompidos dinamicamente.

É possível criar e implantar máquinas virtuais à medida que a demanda do aplicativo aumenta, mas os contêineres são um método mais leve e ágil e foram projetados para permitir que você responda às alterações sob demanda. Com contêineres, você pode reiniciar rapidamente se houver uma falha ou de uma interrupção de hardware. Um dos mecanismos de contêiner mais populares é o Docker, que tem suporte do Azure.

Logo das instâncias de contêiner do Azure.

As **instâncias de contêiner** do Azure oferecem a maneira mais rápida e simples de executar um contêiner, sem a necessidade de gerenciar máquinas virtuais nem adotar serviços adicionais. Instâncias de contêiner do Azure são uma oferta de PaaS (plataforma como serviço), que nos permitem carregar contêineres para que, então, o serviço execute esses contêineres.

Azure Functions

É uma opção de computação sem servidor controlada por eventos e que não requer a manutenção de máquinas virtuais ou contêineres. Se você criar um aplicativo usando VMs ou contêineres, esses recursos precisarão estar "em execução" para que seu aplicativo funcione. Com o Azure Functions, um evento desperta a função, reduzindo a necessidade de manter os recursos provisionados quando não há eventos.

Usar o Azure Functions é ideal quando você está preocupado apenas com o código que executa o serviço, e não com a plataforma ou a infraestrutura subjacente.

As funções costumam ser usadas quando você precisa executar um trabalho em resposta a um evento (geralmente por meio de uma solicitação REST), um

temporizador ou uma mensagem de outro serviço do Azure e quando esse trabalho pode ser concluído dentro de segundos.

Serviço de aplicativo do Azure

Esse serviço permite que você crie e hospede aplicativos web, trabalhos em segundo plano, back-ends de dispositivos móveis e APIs RESTful na linguagem de programação de sua escolha, sem gerenciar a infraestrutura. Ele oferece dimensionamento automático e alta disponibilidade. É compatível com o Windows e o Linux e permite implantações automatizadas do GitHub, Azure DevOps ou qualquer repositório Git para dar suporte a um modelo de implantação contínua.

Com o serviço de aplicativo, você pode hospedar os estilos mais comuns como:

Aplicativos web

Aplicativos de API

WebJobs

Aplicativos móveis

O serviço de aplicativo cuida da maioria das decisões de infraestrutura com as quais você lida ao hospedar aplicativos acessíveis pela web, de maneira que a implantação e o gerenciamento são integrados à plataforma, os pontos de extremidade podem ser protegidos, os sites podem ser dimensionados rapidamente para lidar com cargas de alto tráfego e o balanceamento de carga interno e o gerenciador de tráfego fornecem alta disponibilidade.

Redes virtuais

As redes virtuais e as sub-redes virtuais do Azure permitem que recursos do Azure, como VMs, aplicativos web e bancos de dados, comuniquem-se uns com os outros, com usuários na internet e com computadores cliente locais.

Você pode pensar em uma rede do Azure como uma extensão de sua rede local, com recursos que vinculam outros recursos do Azure.

As redes virtuais do Azure oferecem as seguintes funcionalidades essenciais de rede:

- Isolamento e segmentação.
- Comunicação pela internet.
- Comunicação entre recursos do Azure.
- Comunicação com os recursos locais.
- Rotear tráfego de rede.
- Filtrar tráfego de rede.
- Conectar redes virtuais.

A rede virtual do Azure dá suporte a pontos de extremidade públicos e privados para habilitar a comunicação entre recursos externos ou internos com outros recursos internos. Vamos entender melhor a diferença entre esses tipos de pontos de extremidade:

Pontos de extremidade públicos

Têm um endereço IP público e podem ser acessados de qualquer lugar do mundo.

Pontos de extremidade privados

Existem em uma rede virtual e têm um endereço IP privado dentro do espaço de endereço dessa rede virtual.

Redes virtuais privadas (VPNs)

Uma VPN (rede virtual privada) usa um túnel criptografado dentro de outra rede. As VPNs costumam ser implantadas para conectar, em uma rede não confiável (normalmente a internet pública), duas ou mais redes privadas

confiáveis entre si. Para evitar interceptação ou outros ataques, o tráfego é criptografado ao viajar pela rede não confiável. As VPNs podem permitir que as redes compartilhem informações confidenciais de modo seguro e protegido.

Gateways VPN

É um tipo de gateway de rede virtual. As **instâncias do gateway de VPN** do Azure são implantadas em uma sub-rede dedicada da rede virtual e permitem que seja possível:

1. Conectar datacenters locais a redes virtuais, por meio de uma conexão site a site.
2. Conectar dispositivos individuais a redes virtuais, por meio de uma conexão ponto a site.
3. Conectar redes virtuais a outras redes virtuais, por meio de uma conexão rede a rede.

Azure ExpressRoute

Permite que você estenda suas redes locais para a nuvem da Microsoft em uma conexão privada, com a ajuda de um provedor de conectividade. Essa conexão é chamada de **circuito do ExpressRoute**.

Com o ExpressRoute, você pode estabelecer conexões com os serviços em nuvem da Microsoft, como o Microsoft Azure e o Microsoft 365. Ela permite que você conecte escritórios, datacenters ou outras instalações à Microsoft Cloud, e maneira que cada local teria o próprio circuito do ExpressRoute.

O site do serviço (Microsoft.com) apresenta vários benefícios em usarmos o ExpressRoute como o serviço de conexão entre o Azure e as redes locais, por exemplo:

1. Conectividade com os serviços de nuvem da Microsoft em todas as regiões da região geopolítica.
2. Conectividade global com os serviços da Microsoft em todas as regiões com o Alcance Global do ExpressRoute.
3. Roteamento dinâmico entre sua rede e a Microsoft por meio do BGP (Border Gateway Protocol).

4. Redundância interna em cada local de emparelhamento para proporcionar maior confiabilidade.

DNS do Azure

É um serviço de hospedagem para domínios DNS que fornece a resolução de nomes usando a infraestrutura do Microsoft Azure. Ao hospedar seus domínios no Azure, você pode gerenciar seus registros DNS usando as mesmas credenciais, APIs, ferramentas e cobrança que seus outros serviços do Azure.

O DNS do Azure aproveita o escopo e a escala do Microsoft Azure para proporcionar inúmeros benefícios, incluindo:

- Confiabilidade e desempenho.
- Segurança.
- Facilidade de uso.
- Personalizar redes virtuais.
- Registros de alias.

Os serviços de armazenamento do Azure

Criação de uma conta de armazenamento

Uma conta de armazenamento fornece um namespace exclusivo para os dados do armazenamento do Azure que podem ser acessados de qualquer lugar do mundo por HTTP ou HTTPS. [RSDO1] Os dados nesta conta são seguros, altamente disponíveis, duráveis e maciçamente escalonáveis.

Veja os tipos de conta de armazenamento e suas características:

Tipo	Serviços com suporte	Opções de redundância	Uso
Uso geral v2 standard	Armazenamento de blobs (incluindo Data Lake Storage), armazanamento de filas, armazenamento de tabelas e arquivos do Azure.	LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS	Tipo de conta de armazenamento básico para blobs, compartilhamento de arquivos, filas e tabelas. Recomendado para a maioria dos cenários que usam o armazenamento do Azure.
Blobs de blocos premium	Armazenamento de blobs (incluindo Data Lake Storage)	LRS, ZRS	Tipo de conta de armazenamento premium para blobs de blocos e blobs de acréscimo. Recomendado para cenários com altas taxas

Tipo	Serviços com suporte	Opções de redundância	Uso
			de transação ou que usam objetos menores ou exigem uma latência de armazenamento sempre baixa.
Compartilhamentos de arquivos premium	Arquivos do Azure	LRS, ZRS	Tipo de conta de armazenamento premium somente para compartilhamentos de arquivos. Use esse tipo de conta caso deseje ter uma conta de armazenamento que dê suporte a compartilhame

Tipo	Serviços com suporte	Opções de redundância	Uso
			ntos de arquivos SMB e NFS.
Blobs de página premium	Blobs de páginas somente	LRS	Tipo de conta de armazenamento premium somente para blobs de páginas.

Tabela: Características das contas de armazenamento do Azure.
Francisco Ferreira

Redundância de armazenamento do Azure

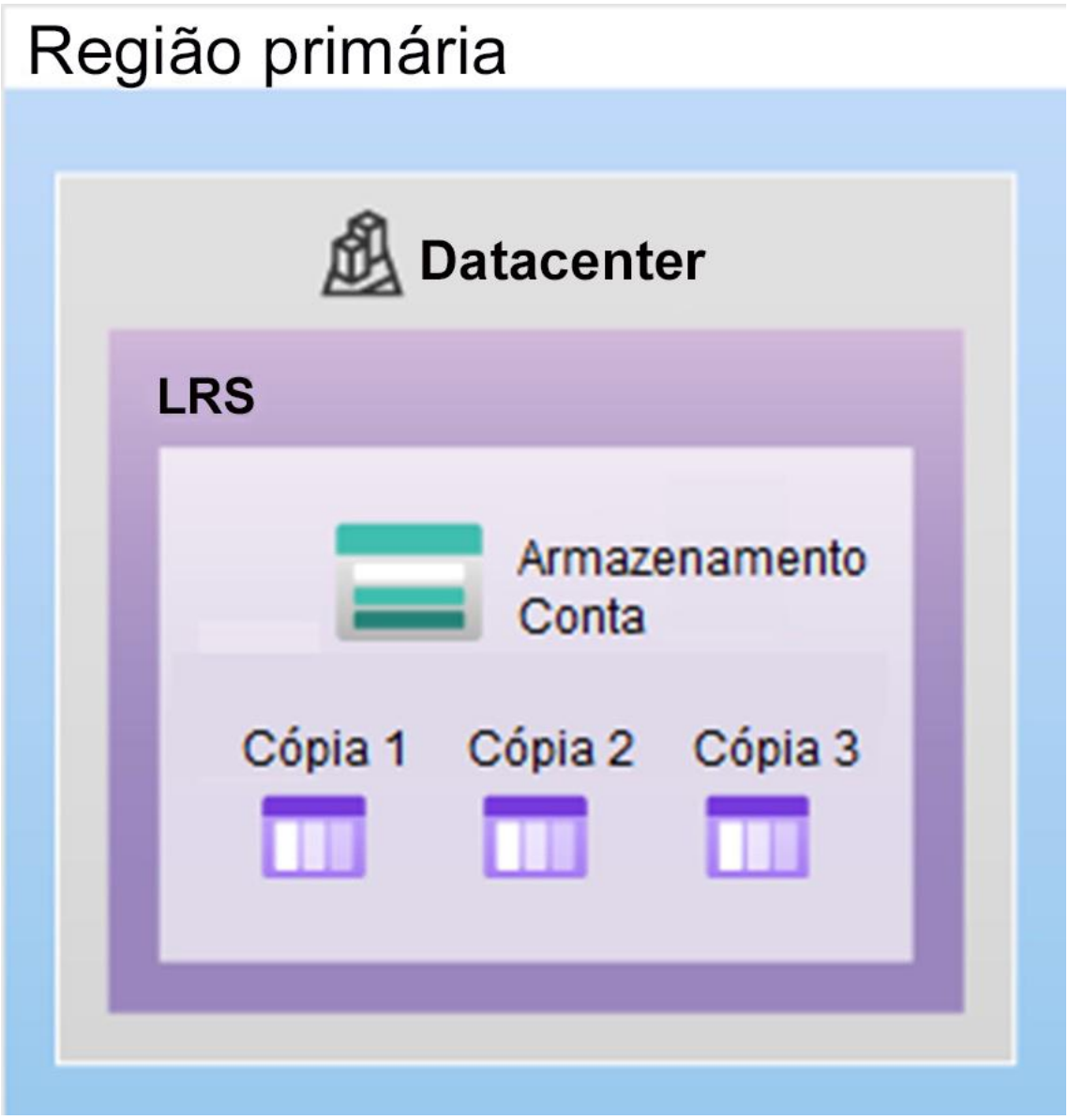
No Azure existem fatores que ajudam a determinar qual opção de redundância você deve escolher, veja:

1. Como os dados são replicados na região primária.
2. Se os dados são replicados em uma segunda região que está geograficamente distante da região primária, para protegê-los contra desastres regionais.
3. Se o aplicativo requer acesso de leitura aos dados replicados na região secundária, caso a região primária não esteja disponível.

Redundância na região primária

Armazenamento com redundância local

A replicação LRS é trabalhada de forma local, os seus dados são replicados três vezes no mesmo datacenter e na mesma região primária. Esse tipo de replicação fornece no mínimo 11 noves de durabilidade (99,999999999%) dos objetos armazenados durante um ano.

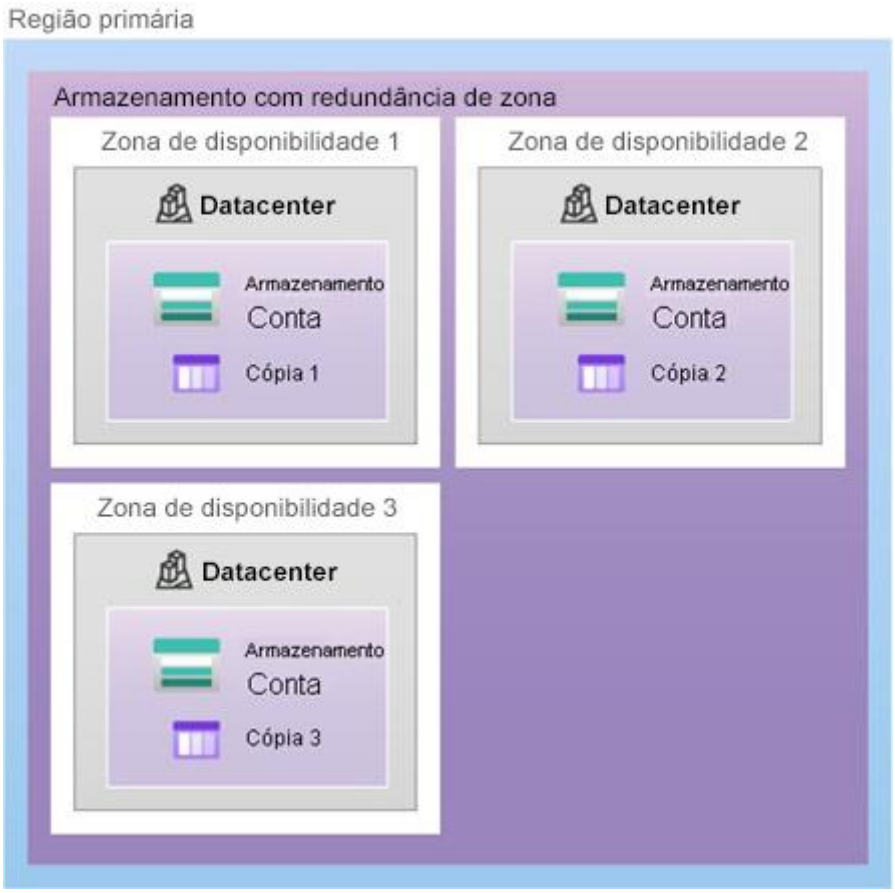


Região primária e redundância local.

Armazenamento com redundância de zona

A replicação com redundância de zona é disponibilizada nas regiões habilitadas (regiões que possuem 3 zonas), ela é chamada de ZRS (armazenamento com redundância de zona). Esse tipo de replicação grava, de forma síncrona, em três zonas de disponibilidade do Azure na mesma região

primária. Da mesma forma ela fornece durabilidade dos objetos gravados de, no mínimo, 12 noves (99,9999999999%) durante um ano.

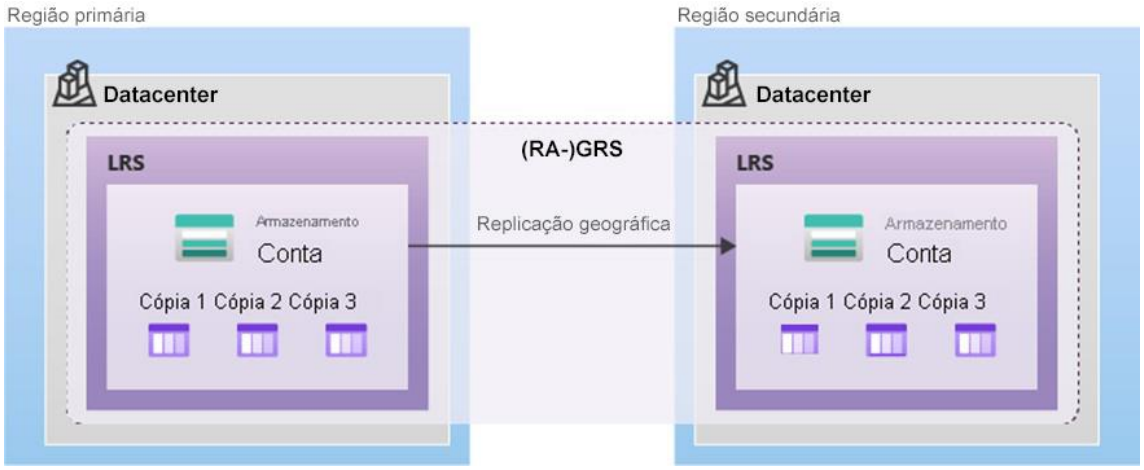


Região primária e redundância de zona.

Redundância em uma região secundária

Armazenamento com redundância geográfica

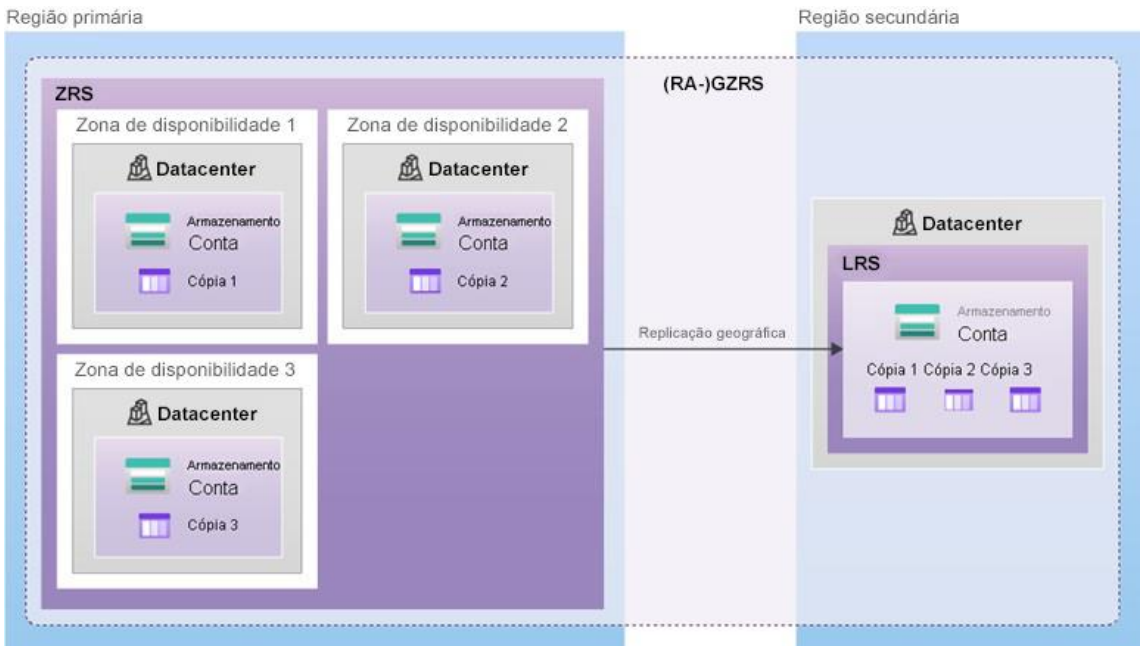
No armazenamento com redundância geográfica é realizada a replicação por meio da cópia de seus dados. Esse tipo de replicação é do tipo GRS e ocorre de forma síncrona, três vezes dentro do mesmo datacenter e na mesma região usando LRS. Logo após, é realizada, de maneira assíncrona, a cópia dos dados em um único datacenter na região secundária (o par da região) usando LR, sendo essa uma das replicações de maior custo. O GRS oferece durabilidade para dados armazenados de, no mínimo, 16 noves (99,99999999999999%) durante um ano.



Região secundária e redundância geográfica.

Armazenamento com redundância de zona geográfica

O armazenamento com redundância de zona geográfica é caracterizado pela redundância entre zonas de disponibilidade, em conjunto com a proteção contra interrupções regionais (desastres naturais ou falta de comunicação) fornecidas pelo modelo de replicação geográfica. A replicação do tipo GZRS possui as características da alta disponibilidade e serve como exemplo desse tipo de armazenamento. Logo, os dados em uma conta de armazenamento GZRS são copiados entre três zonas de disponibilidade no mesmo datacenter, na mesma região primária (semelhante ao ZRS), e são replicados em uma região geográfica secundária usando LRS para proteção contra desastres regionais.



Região secundária e redundância de zona geográfica.

Serviços de armazenamento do Azure

As contas de armazenamento do Azure possuem os seguintes serviços:

Blobs do Azure

É um espaço de armazenamento para dados considerados não estruturados, como arquivos de texto, vídeos, imagens, documentos e dados binários, dados que crescem de uma forma escalonável. Esse tipo de armazenamento também dá suporte a análise de Big Data por meio do Data Lake Storage Gen2.I

Arquivos do Azure

É o compartilhamento de arquivos (usando o protocolo SMB) bem familiar (que conhecemos nos sistemas Windows), que pode ser utilizado em implementações locais e em nuvem.

Filas do Azure

É um tipo de armazenamento de mensagens para um sistema de mensagens entre componentes do aplicativo, também usado para logs.

Azure Disks

É um tipo de armazenamento usado para dos discos de máquina virtual, que é usado em nível de bloco.

Armazenamento de blob

Os blobs do Azure servem para armazenar objetos na nuvem. Muito utilizados para grandes volumes de dados, como textos, imagens, streaming e/ou dados binários. Eles também são conhecidos como armazenamento de dados não estruturados, e são chamados assim porque podem armazenar qualquer tipo de dados sem impedimentos. Os blobs do Azure também têm a capacidade de

gerenciar milhares de transferências simultâneas, grandes volumes de dados de vídeo, arquivos de log, além da possibilidade de serem acessados de qualquer lugar que possua internet. Os blobs normalmente são entregues a aplicações, como apps de celular e/ou softwares de backup.

O armazenamento de blobs é usado para armazenamento de:

- Imagens, documentos, vídeos para acesso por meio de um navegador.
- Arquivos para acesso distribuído.
- Transmissões por streaming de áudio e vídeo (como Youtube, Netflix).
- Dados para backup e restauração, recuperação de desastres e arquivamento, normalmente usados com softwares escritos para enxergar as contas de armazenamento.
- Dados para análise por um serviço local ou hospedado no Azure.

No armazenamento do Azure existem diferentes camadas, chamadas de **tiers**. Para acesso e para seu armazenamento de blobs, cada camada possui características específicas, relacionadas a performance e custo. As camadas de acesso disponíveis são:

1. ## Camada de acesso quente(hot)

   Camada usada para armazenar dados que são acessados com frequência (por exemplo, imagens e vídeos de seu site).

2. ## Camada de acesso frio(cool)

   Camada usada para armazenar dados que são acessados com menos frequência e guardados pelo menos 30 dias (por exemplo, faturas de seus clientes, laudos médicos).

3. ## Camada de acesso aos arquivos(archive)

Camada usada para armazenar dados acessados de forma rara e guardados por pelo menos por 180 dias, com latências flexíveis (por exemplo, arquivamento de backups).

Arquivos do Azure (Azure Files)

Os arquivos do Azure são um tipo de armazenamento em nuvem que possui compatibilidade com os protocolos SMB ou NFS, usando a familiar tecnologia de compartilhamento de arquivos. Esse compartilhamento de arquivos pode ser mapeado tanto por máquinas virtuais no Azure como por máquinas locais. Devido a utilização do protocolo SMB, o compartilhamento de arquivos pode ser acessado por máquinas que utilizam sistemas operacionais Windows, Linux e macOS. Além disso, pode ser usado como cache nos servidores Windows Server com a sincronização de arquivos (Azure File Sync) para acesso rápido a partir de onde os dados estão sendo usados. Um detalhe importante é que a porta 445 deve estar aberta para utilização no provedor de internet.

Veja algumas vantagens dos arquivos do Azure:

Acesso compartilhado

Os compartilhamentos de arquivo do Azure utilizam protocolos SMB e NFS, que são familiares no mercado.

Totalmente gerenciados

Os compartilhamentos de arquivo do Azure podem ser criados diretamente na nuvem e não precisam ser gerenciados por um sistema operacional ou hardware, pois o mapeamento é feito de forma simples.

Script e ferramentas

Os scripts PowerShell e o Az-Cli podem ser usados para criar, montar e gerenciar compartilhamentos de arquivo rapidamente.

Resiliência

Serviço altamente disponível, que permite substituir compartilhamentos locais pelos arquivos do Azure. Portanto, você não precisa se preocupar com interrupções inesperadas, como energia elétrica ou redes locais, pois como os arquivos estão na nuvem, o gerenciamento é feito pelo Azure.

Gerenciamento familiar

Como já é utilizado e familiar aos usuários, podem acessar dados no compartilhamento e APIs do sistema de arquivos.

Armazenamento de filas (Azure Queues)

É um tipo de armazenamento usado para armazenar mensagens em grande escala. Após o armazenamento, é possível acessá-las de qualquer local por meio de autenticação HTTP ou HTTPS. Em uma fila é possível armazenar mensagens em uma quantidade muito grande (possivelmente milhões). As filas são usadas para criar uma lista de pendências de trabalho para processamento assíncrono.

Identidade e segurança do Azure

Serviços de diretório do Azure

O Azure AD (Azure Active Directory) é um serviço de diretório que permite que você entre e acesse aplicativos de nuvem da Microsoft e aplicativos de nuvem que você desenvolve. O Azure AD também pode ajudar a manter sua implantação do Active Directory local.

O Azure AD permite gerenciamento de identidade e acessos.

Em ambientes locais, o Active Directory em execução no Windows Server, fornece um serviço de gerenciamento de identidade e acesso gerenciado pela sua organização. O Azure AD é o serviço de gerenciamento de acesso e

identidade baseado em nuvem da Microsoft. Com o Azure AD, você controla as contas de identidade, mas a Microsoft garante que o serviço esteja disponível globalmente.

Quando você protege identidades locais com o Active Directory, a Microsoft não monitora tentativas de conexão. Quando você conecta o Active Directory ao Azure AD, a Microsoft pode ajudar a protegê-lo, detectando tentativas de conexão suspeitas, sem custo adicional. Por exemplo, o Azure AD pode detectar tentativas de conexão de locais inesperados ou dispositivos desconhecidos.

O Azure AD fornece serviços como:

Autenticação

Inclui verificar a identidade para acessar aplicativos e recursos. Também inclui fornecer funcionalidades, como redefinição de senha por autoatendimento, autenticação multifatorial, uma lista personalizada de senhas banidas e serviços de bloqueio inteligente.

Logon único

Permite lembrar apenas de um nome de usuário e uma senha para acessar vários aplicativos. Uma única identidade é vinculada a um usuário, o que simplifica o modelo de segurança.

Gerenciamento de aplicativo

Permite gerenciar seus aplicativos de nuvem e locais usando o Azure AD. Recursos como proxy de aplicativo, aplicativos SaaS, o portal Meus Aplicativos e o login único proporcionam uma experiência do usuário aprimorada.

Gerenciamento de dispositivo

Permite suporte ao registro de dispositivos. O registro permite que os dispositivos sejam gerenciados por meio de ferramentas como o Microsoft

Intune. Também permite que políticas de acesso condicional baseadas no dispositivo restrinjam tentativas de acesso somente às contas provenientes de dispositivos conhecidos, independentemente da conta de usuário solicitante.

Controle de acesso baseado em função (RBAC)

O gerenciamento de acesso para recursos de nuvem é uma função crítica para qualquer organização que esteja usando a nuvem. O RBAC do Azure (controle de acesso baseado em funções do Azure) ajuda a gerenciar quem tem acesso aos recursos do Azure, o que pode fazer com esses recursos e a quais áreas tem acesso.

O RBAC do Azure é um sistema de autorização baseado no Azure Resource Manager, que fornece gerenciamento de acesso refinado para recursos do Azure.

Exemplo

Imagine possuir dois grupos de recursos, um com os recursos do setor de marketing e outro com os recursos do setor financeiro. Através do RBAC você pode determinar que apenas os usuários do setor financeiro acessem os recursos do seu setor, da mesma forma com o setor de marketing. Cada usuário acessará apenas os recursos do seu próprio setor. A isso chamamos de segmentação do gerenciamento de recursos.

Defesa em profundidade

É um conjunto de camadas, com os dados a serem protegidos no centro e as demais camadas operando para proteger a camada central. Envolvem todo o processo de acesso do datacenter, passando pela segurança física, identidade, perímetro, rede, computação, aplicativo e até chegar ao dado propriamente dito.

Esquematização da defesa em profundidade.