Introdução ao Azure e Infraestrutura Básica de TI como Serviço

Bootcamp: Profissional Azure Cloud Computing

Marcelo Leite

2021

Introdução ao Azure e Infraestrutura Básica de TI como Serviço

Bootcamp: Profissional Azure Cloud Computing

Marcelo Leite

Sumário

Capítulo 1. Introdução ao Azure

O Azure é uma plataforma de computação em nuvem da Microsoft. Essa plataforma conta com serviços de software que podem ser utilizados sob demanda, habilitando infraestrutura e softwares avançados para empresas de todos os portes.

Os serviços do Azure vão desde servidores virtuais simples, até aplicações de big data e inteligência artificial, com vários modelos de implementação para ajudar empresas a criarem soluções para desafios de negócios.

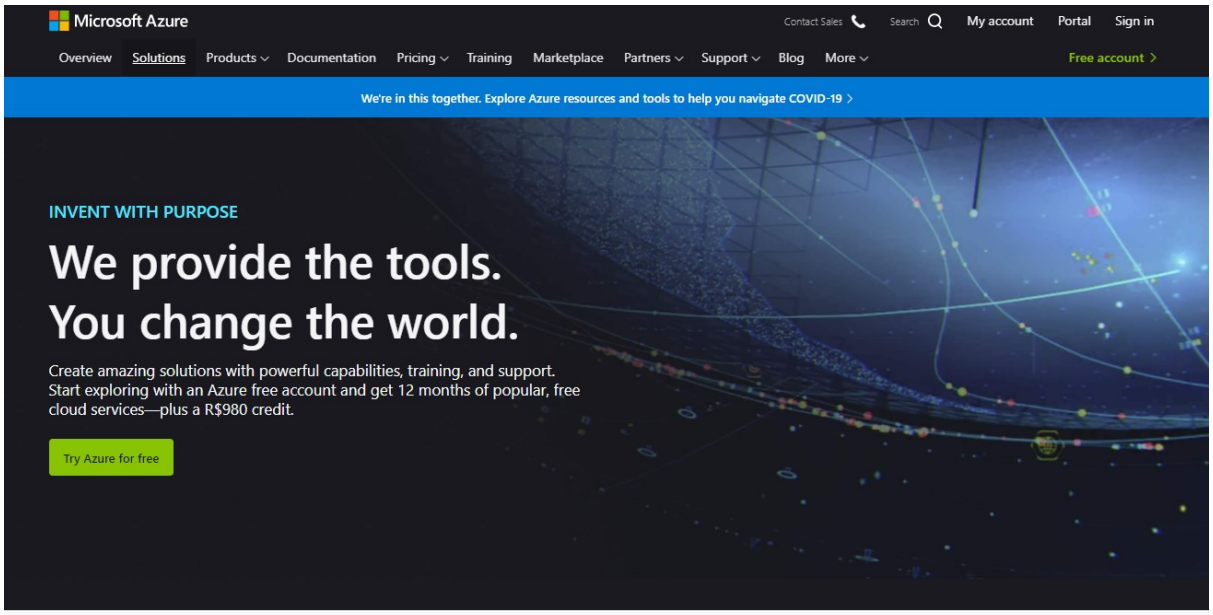
O que é computação em Nuvem?

A computação em nuvem, ou “Cloud Computing” é a disponibilização de serviços de software e hardware como serviço, por empresas de tecnologia. Esses serviços podem ser utilizados sob demanda, pois possuem como padrão a cobrança por meio de créditos pré-pagos ou pós-pagos de nuvem.

Computação em nuvem vem proporcionado acesso à tecnologia de ponta para empresas de todos os portes e segmentos, além da escalabilidade global dos serviços, que faz com que a internacionalização das empresas seja facilitada.

No site do Azure, a Microsoft disponibiliza documentação completa sobre seus serviços próprios e de parceiros, calculadora de estimativa de custos, criação de conta gratuita, entre outros recursos.

Figura 1 – Captura de tela que mostra o website portal do Azure.

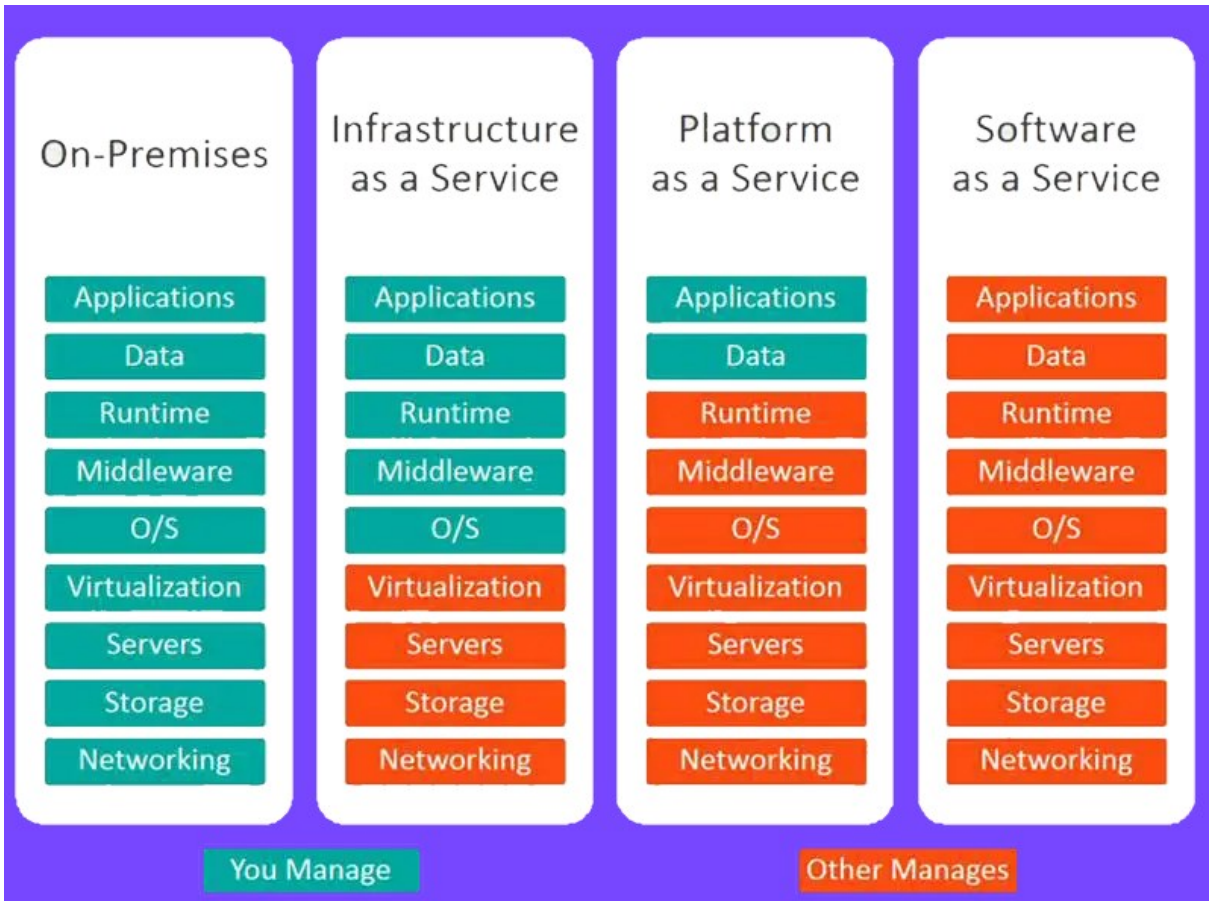


Quais são os modelos de serviços em nuvem?

Para entender o Azure é importante entender o modelo de negócios da computação em nuvem e seus formatos. Os serviços são categorizados em PaaS, IaaS e SaaS. Os softwares e hardwares que são presentes em datacenters tradicionais ficaram com a nomenclatura “On Premisses”, ou No Local.

Cada categoria de serviço de nuvem abrange um diferente nível de responsabilidade de manutenção daquele serviço. Os provedores de Cloud, ao invés de detalhar todas as suas operações, divulgam um SLA (Service Level Agreement) de disponibilidade do serviço e o usuário pode utilizar esse SLA para montagem da sua estratégia de uso.

Figura 2 – Diferenças entre modelos de serviços em nuvem.



As categorias são:

- **IaaS (Infrastructure as a Service):**

A IaaS é a categoria de serviços mais próxima de um datacenter local, pois simula a virtualização de servidores amplamente presente nos datacenters das empresas. O IaaS disponibiliza servidores em máquinas virtuais, ou VMs (Virtual Machines) para seus usuários e toda a manutenção e operação do hardware do datacenter é de responsabilidade do provedor de Cloud.

O principal benefício nesse formato é que o usuário pode “alugar” sob demanda servidores de diferentes modelos e tamanhos, junto com softwares de sistemas operacionais e bancos de dados.

- **PaaS (Platform as a Service):**

O formato PaaS oferece um nível maior de alto gerenciamento, ou seja, menor carga de trabalho em manutenção do serviço que será utilizado. É o formato mais utilizado para implementação de soluções nativas da nuvem, pois entrega escalabilidade, inovação e manutenção facilitadas.

- **SaaS (Software as a Service):**

O SaaS é um formato de software hospedado e totalmente gerenciado pelo provedor de Cloud. Os benefícios deste formato estão relacionados ao foco na utilização do serviço ou software, e não em operações de desenvolvimento e manutenção.

Os serviços presentes na plataforma Azure são baseados nos formatos IaaS e PaaS, destinados à montagem de soluções de TI.

Exemplos de softwares SaaS são o Office 365 e o Dynamics 365 da Microsoft.

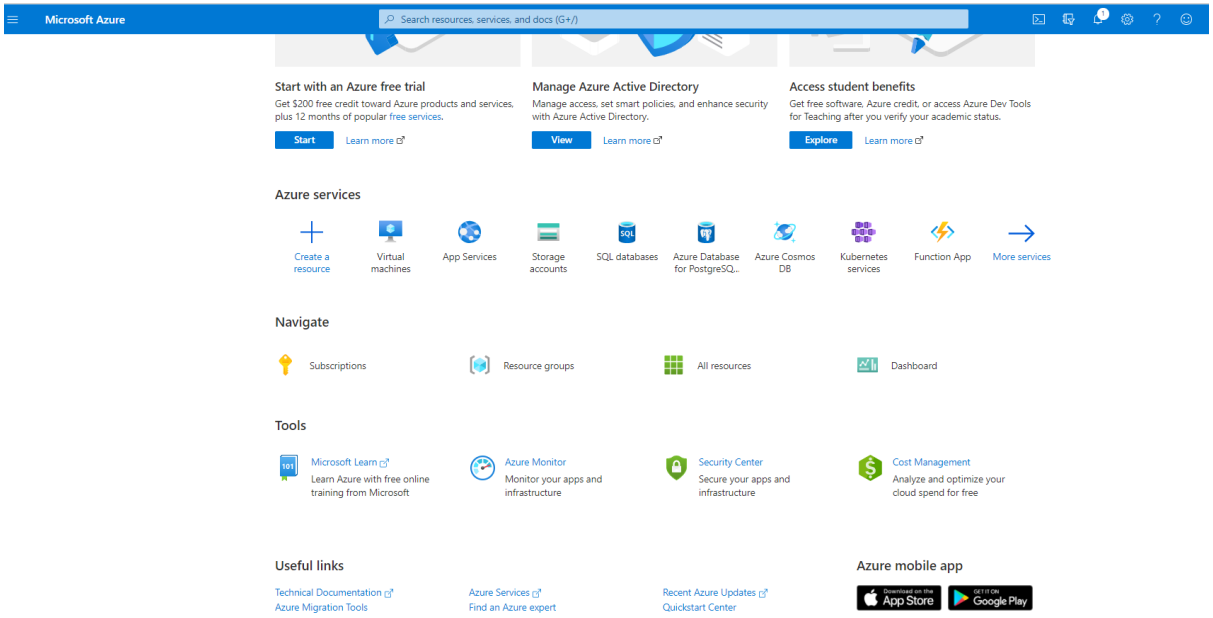
Portal Azure

O portal do Azure é o console central para acesso aos serviços e administração dos mesmos, tanto para softwares da Microsoft quanto de parceiros (Azure Marketplace). O Azure também conta com uma interface de linhas de comando que pode ser utilizada para automatização de processos e configurações avançadas.

No portal você conta com a interface gráfica do usuário, facilitando o acesso aos serviços e as configurações deles, de usuário e roles, subscrições e monitoramento de toda a infraestrutura.

O Portal Azure foi projetado para estar sempre disponível, para acesso de qualquer lugar do mundo através de um link de internet. Ele tem constante atualização, tanto em termos de usabilidade quanto na disponibilização de novos recursos e documentações que auxiliam na utilização da plataforma.

Figura 3 – Captura de tela que mostra o portal do Azure.

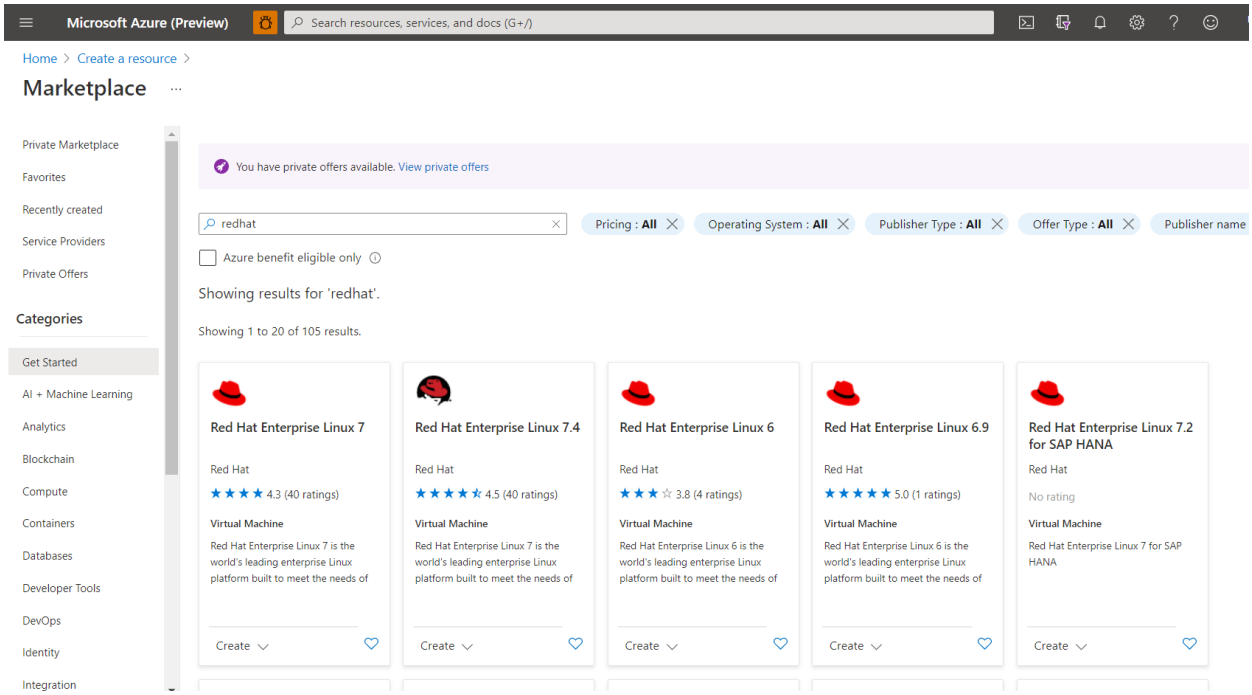


Marketplace do Azure

O Azure Marketplace é um módulo integrado à pesquisa de recursos do Portal Azure, que apoia os usuários a encontrarem soluções de parceiros da Microsoft para implementar softwares já homologados, testados e otimizados para o Azure.

Muitas vezes esses softwares podem ser testados com uma licença do tipo “trial”, comprados através do portal Azure ou você pode incluir uma licença adquirida fora do contrato Azure e apenas utilizar o Marketplace para acelerar a instalação do software.

Figura 4 – Captura de tela que mostra o Azure Marketplace filtrando uma pesquisa.



Os softwares disponibilizados estão organizados pelas categorias à esquerda do portal e permeiam softwares para infraestrutura de TI, segurança de TI, bancos de dados, desenvolvimento e soluções voltadas aos negócios.

Para disponibilizar uma solução no Azure Marketplace, o parceiro precisa criar uma “imagem” que acelera a sua implementação independentemente se ela utilizará VMs, contêineres ou outras infraestruturas para ser instalada e homologar essa imagem com os times de engenharia da Microsoft.

Capítulo 2. Overview dos Serviços do Azure

Visão geral dos serviços no Azure

O Azure oferece uma variedade muito grande de serviços de TI em uma arquitetura global distribuída em regiões de datacenters.

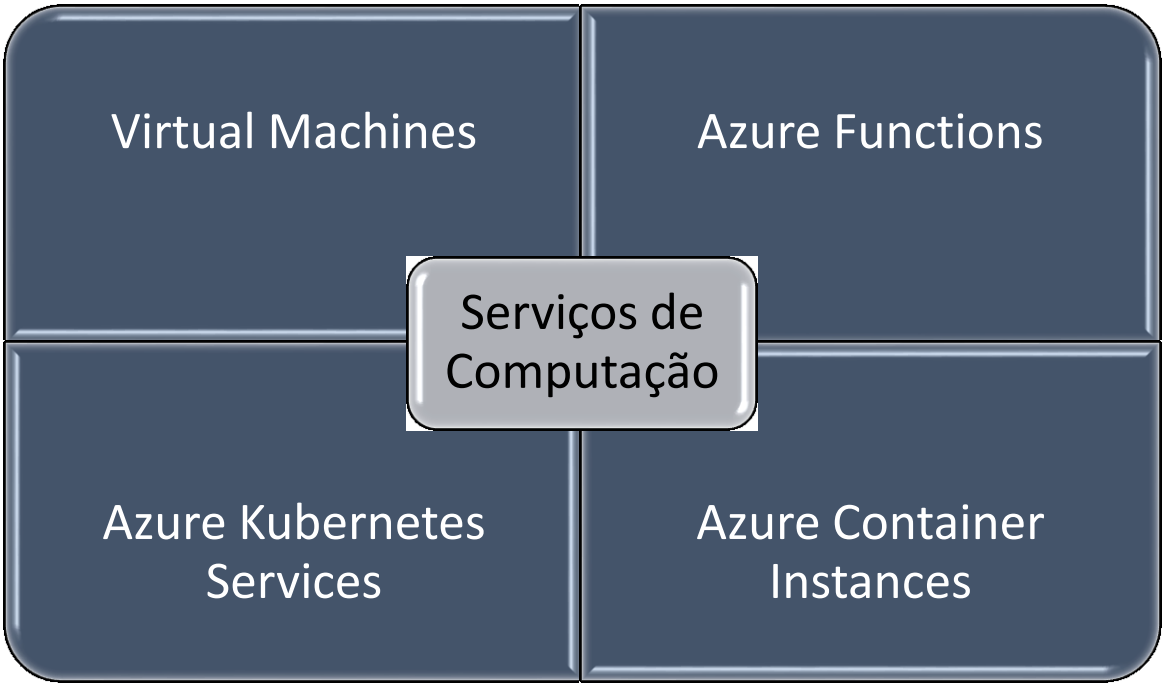
Os serviços são disponibilizados em categorias. Listamos abaixo as principais categorias utilizadas:

- Computação.
- Redes.
- Armazenamento.
- Móvel.
- Bancos de dados.
- Web.
- Internet das coisas (IoT).
- Big Data.
- IA.
- DevOps.

Serviços de Computação

Os serviços de computação entregam capacidades de computadores em formato de serviços gerenciados. Eles vão desde o IaaS com disponibilização de Virtual Machines (VMs), passando por infraestrutura de contêineres até serviços de execução de blocos de códigos.

Alguns exemplos de serviços de computação mais utilizados são:

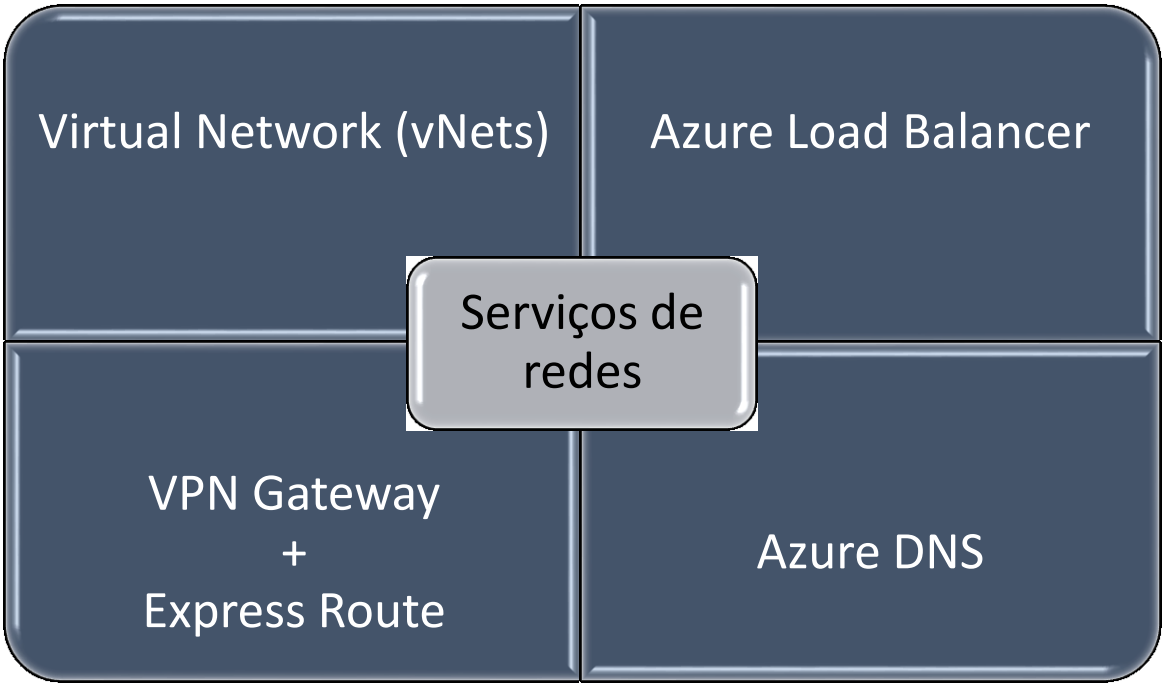


Redes

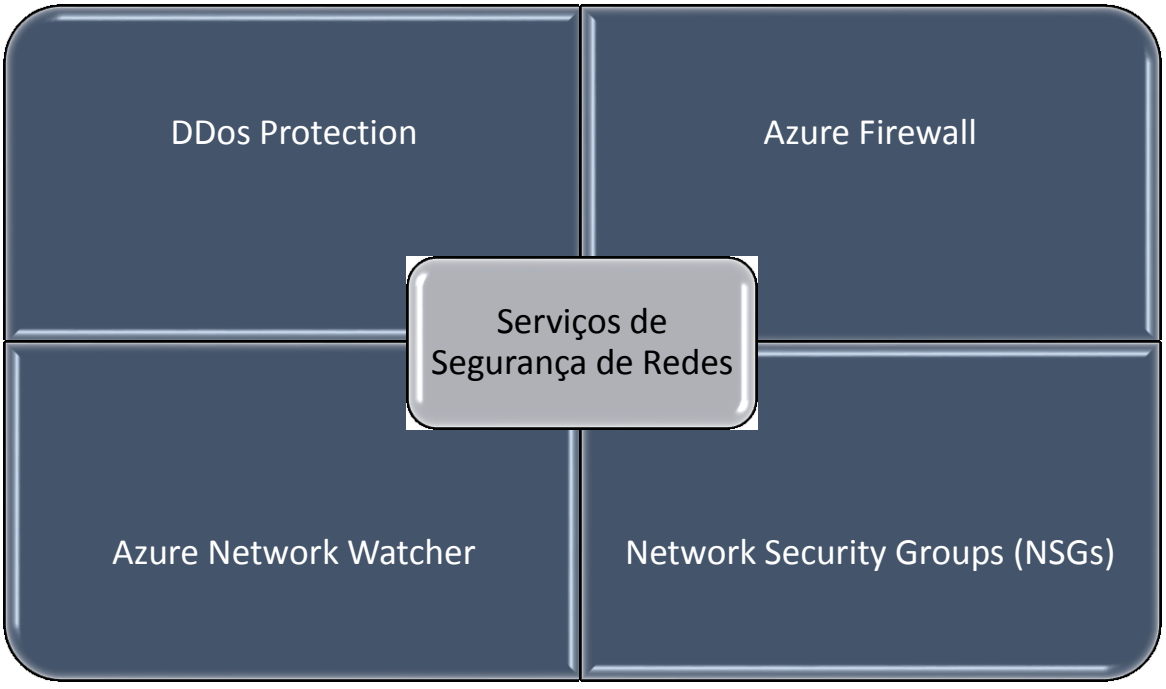
Como toda infraestrutura de servidores, é necessário interligar os serviços por meio de redes virtuais, que conectam esses serviços e criam organizações lógicas para a sua infraestrutura. As redes também têm papel importante em segurança, uma vez que é possível criar redes que bloqueiam acessos externos ao Azure, da mesma maneira como criação de ambientes preparados para acessar a internet de forma controlada.

Os padrões de topologia de redes que podem ser montados no Azure são muito similares às topologias tradicionais empregadas em datacenters e empresas pelo mundo, mas como benefício da rede global do Azure, o usuário pode ainda interconectar duas ou mais regiões em diferentes continentes, com apenas alguns cliques e configurações.

Alguns serviços de rede do Azure são:



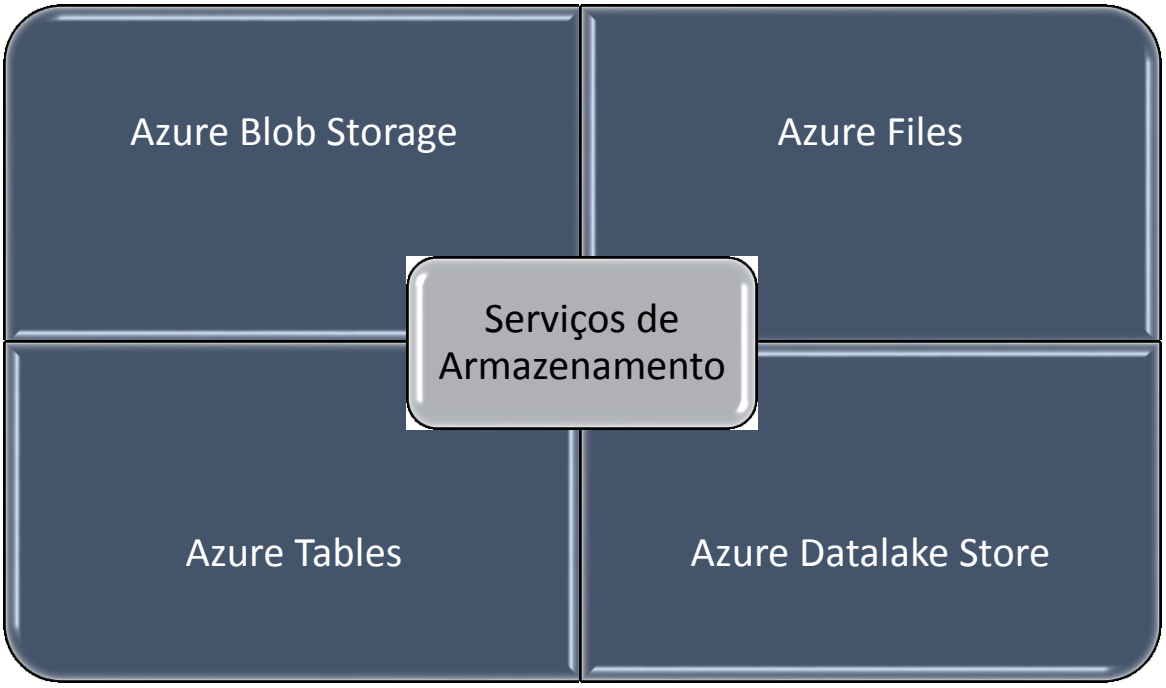
Além destes serviços básicos, o Azure conta também com serviços específicos de segurança e controle de redes, como:



Armazenamento

Um dos principais diferenciais do modelo de nuvem pública, as camadas de armazenamento oferecem acesso a diferentes tipos de “storage” de maneira simples, flexível e mais barata do que em datacenters locais.

Alguns exemplos de formatos de armazenamento do Azure são:



Os serviços têm algumas características comuns:

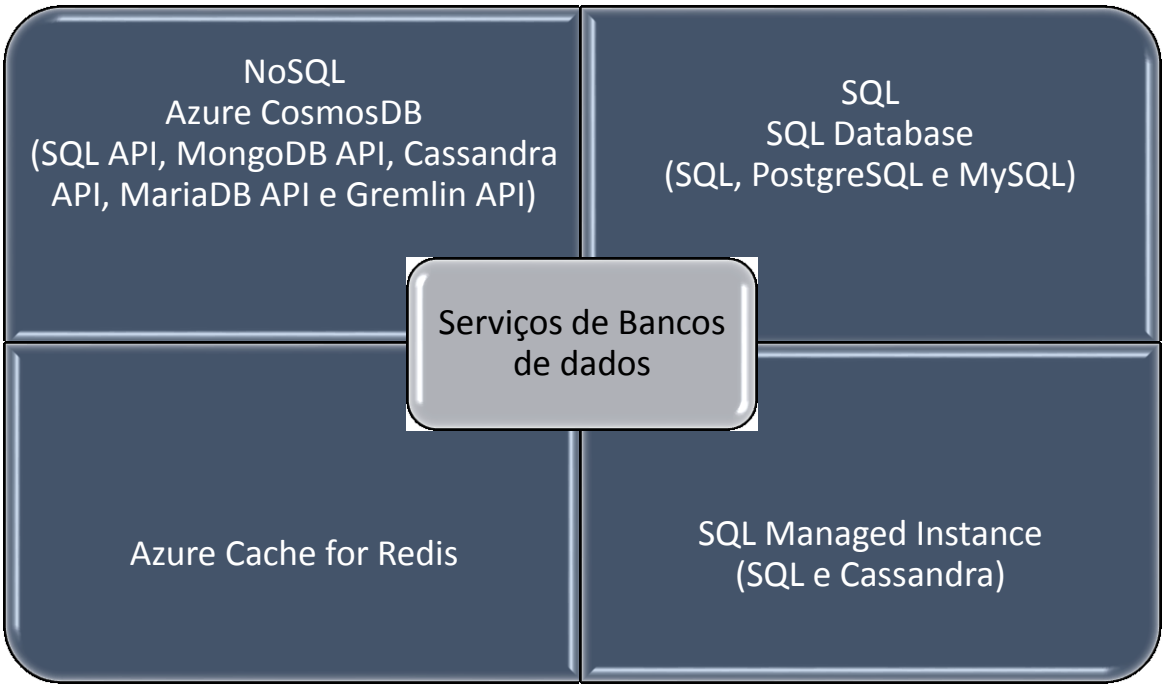
- **Duráveis** e altamente disponíveis com redundância e replicação.
- **Seguros** por meio de criptografia automática e controle de acesso baseado em função.
- **Escalonáveis** com um armazenamento praticamente ilimitado.
- **Gerenciados**, cuidando da manutenção e de quaisquer eventuais problemas críticos para você.
- **Acessíveis** de qualquer lugar do mundo por HTTP ou HTTPS.

Bancos de dados

A maioria dos sistemas tem necessidades de um ou mais bancos de dados e para atender esse requisito o Azure oferece vários formatos diferentes de bancos de dados, desde versões do Microsoft SQL Server, até versões gerenciadas dos bancos de dados Open Source mais utilizados no mundo.

Utilizar um banco de dados PaaS pode simplificar muito a carga de trabalho de um DBA, automatizando processos e simplificando operações.

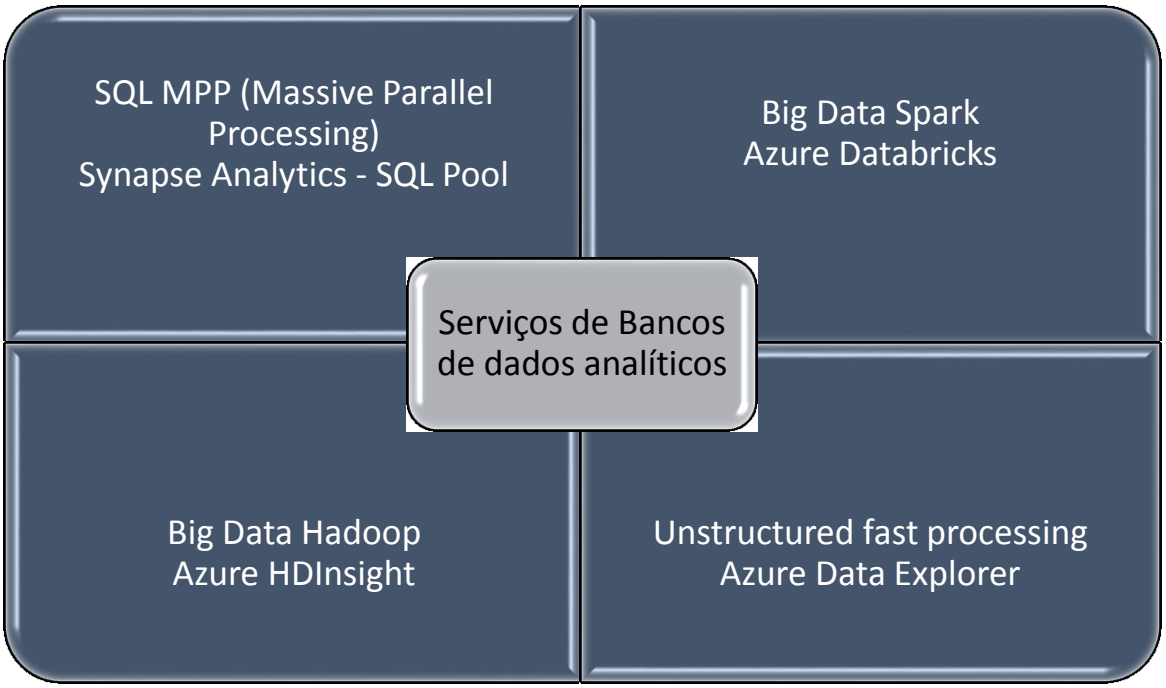
Alguns tipos de bancos de dados encontrados no Azure são:



O Azure também oferece formatos de bancos de dados específicos para aplicações analíticas, baseados nos conceitos de Big Data, com capacidades escaláveis para atender qualquer necessidade de processamento de altos volumes de dados.

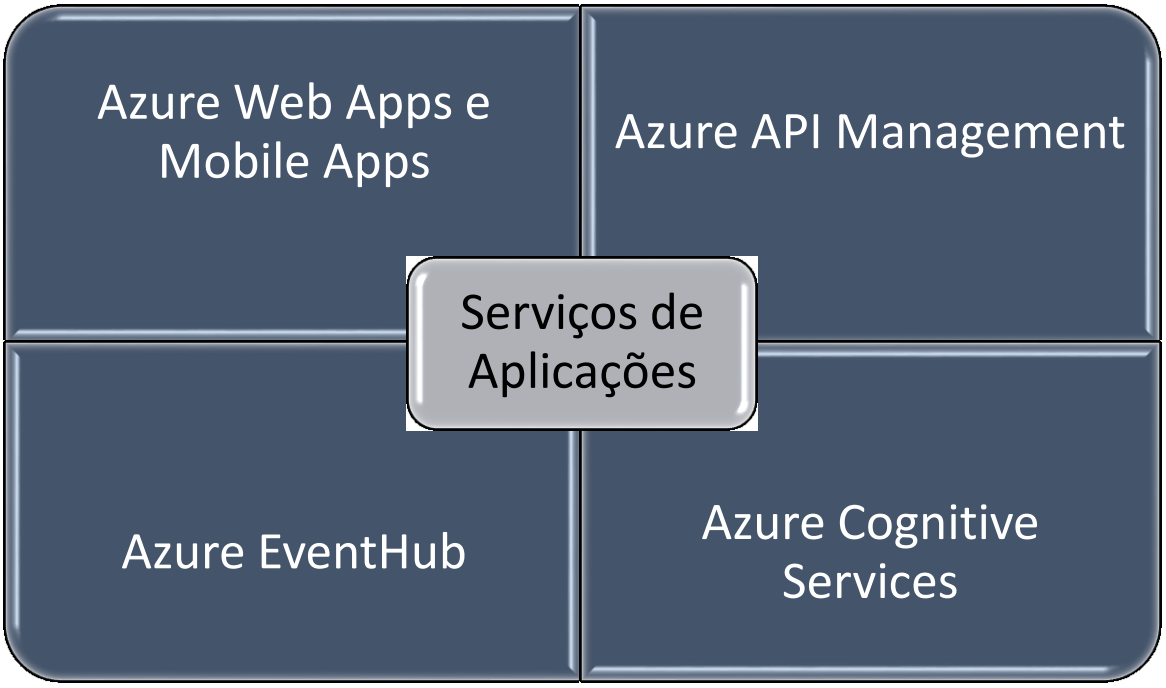
Para estes bancos de dados os formatos e tamanhos podem ser variados. Quando falamos em Big Data, estamos nos referindo a ***grandes*** volumes de dados.

Tecnologias de cluster de Open Source foram desenvolvidas para lidar com esses grandes conjuntos de dados, baseados no projeto Hadoop. O Azure oferece diferentes formatos para atender todas as necessidades. Alguns exemplos são:



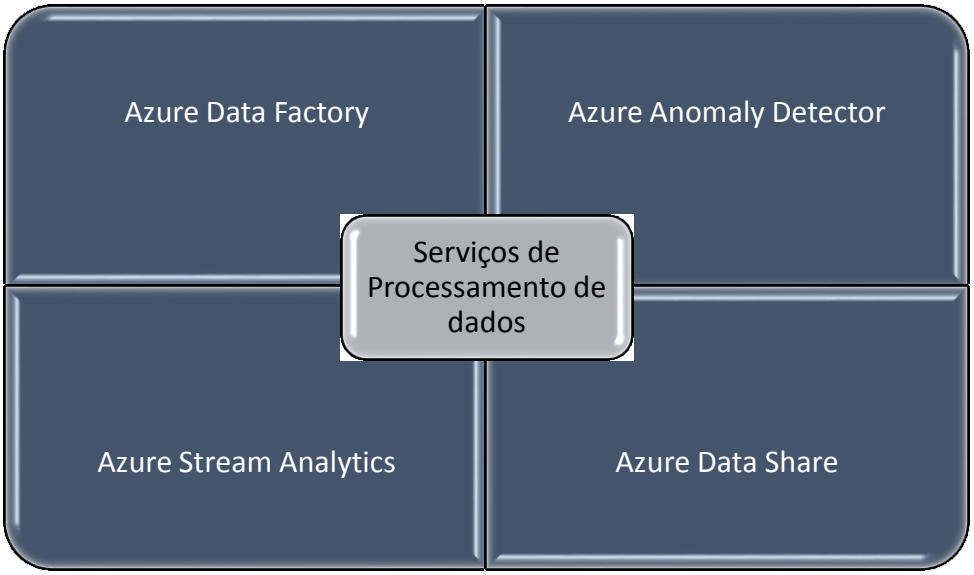
Aplicações

Para hospedar aplicativos modernos no Azure, os usuários contam com uma variedade de serviços para hospedar a aplicação e montá-la utilizando aceleradores prontos da nuvem. Exemplos dos serviços do Azure que apoiam no desenvolvimento de aplicações modernas, são:



Processamento de dados

Alguns serviços do Azure ajudam os usuários na orquestração de dados entre as aplicações e bancos de dados, processam essas informações criando regras de negócios e entregando aos bancos de dados analíticos informação para disponibilização. Alguns serviços utilizados para essas funções, são:

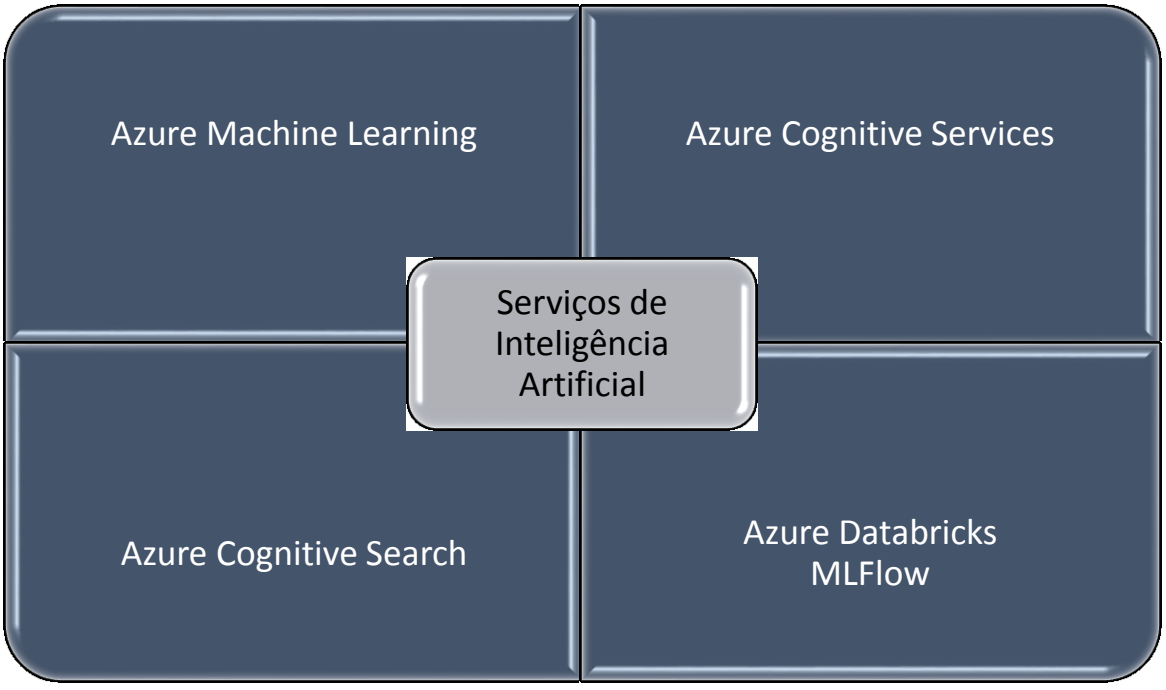


Utilizar a computação em nuvem permite à empresas de todos os tamanhos o acesso a serviços de computação avançada para processamento de modelos de inteligência artificial em diferentes níveis.

Um dos ramos da inteligência artificial mais utilizado no mundo é o aprendizado de máquina (Machine Learning), que utiliza a capacidade de computadores para analisar padrões em dados que definem probabilidades com base em estatística.

Outro ramo importante são os serviços cognitivos, que buscam reproduzir capacidades cognitivas humanas (visão, fala, compreensão, leitura, entre outros), para criar aplicações que auxiliam pessoas a executar atividades corriqueiras com o apoio de Inteligência Artificial.

Aqui estão alguns dos tipos de serviço de IA e Machine Learning mais comuns do Azure:



DevOps

Uma prática importante no desenvolvimento de aplicações moderna, o conceito de DevOps consiste em organizar os times técnicos que estejam atuando em um projeto, governar os processos na montagem deste projeto e automatizar ao máximo processos técnicos para garantir o máximo de produtividade dos times envolvidos.

Os conceitos de CI/CD (Continuous Integration e Continuous Delivery) do DevOps, devem ser empregados em projetos de aplicações modernas e em projetos analíticos de dados. Para apoiar nestas implementações o Azure conta com o serviço Azure DevOps com vários módulos diferentes para auxiliar nas configurações, como:

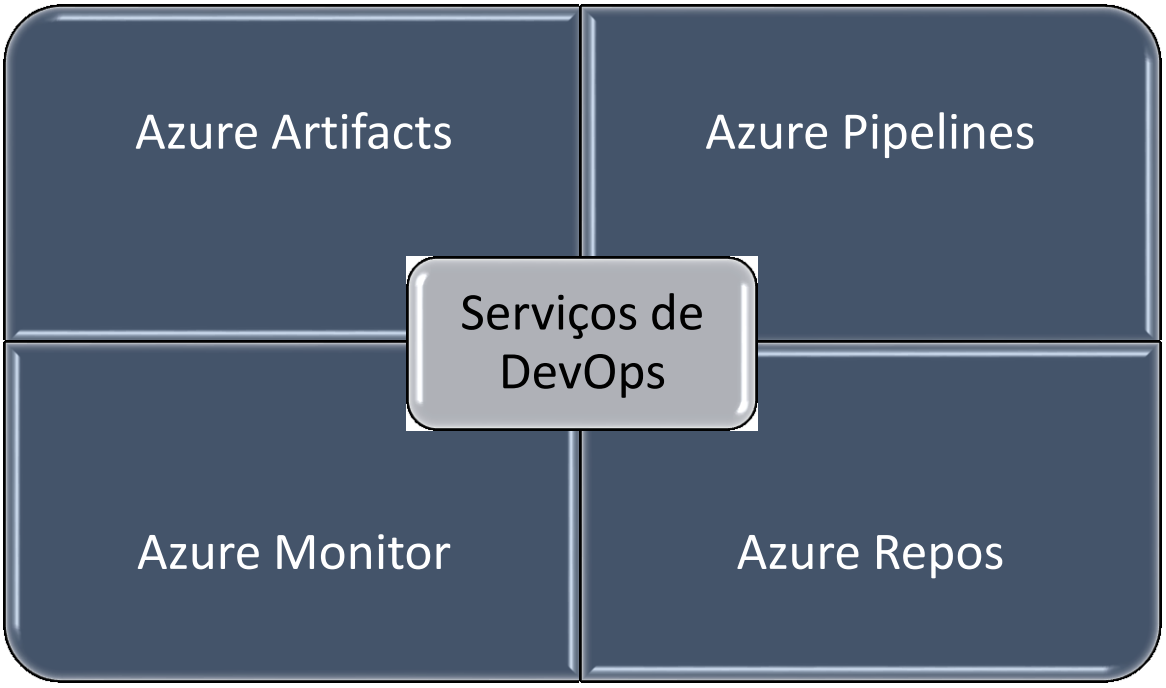
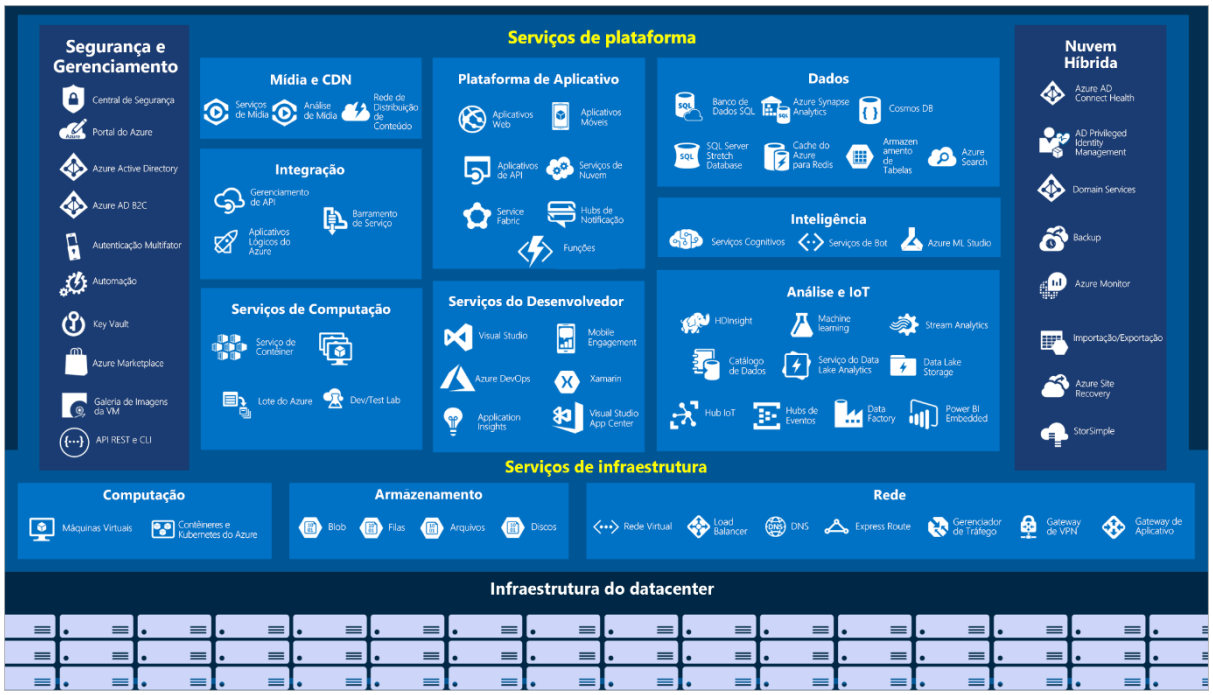


Figura 5 – Visão geral de serviços disponíveis no Azure.



Fonte: Microsoft

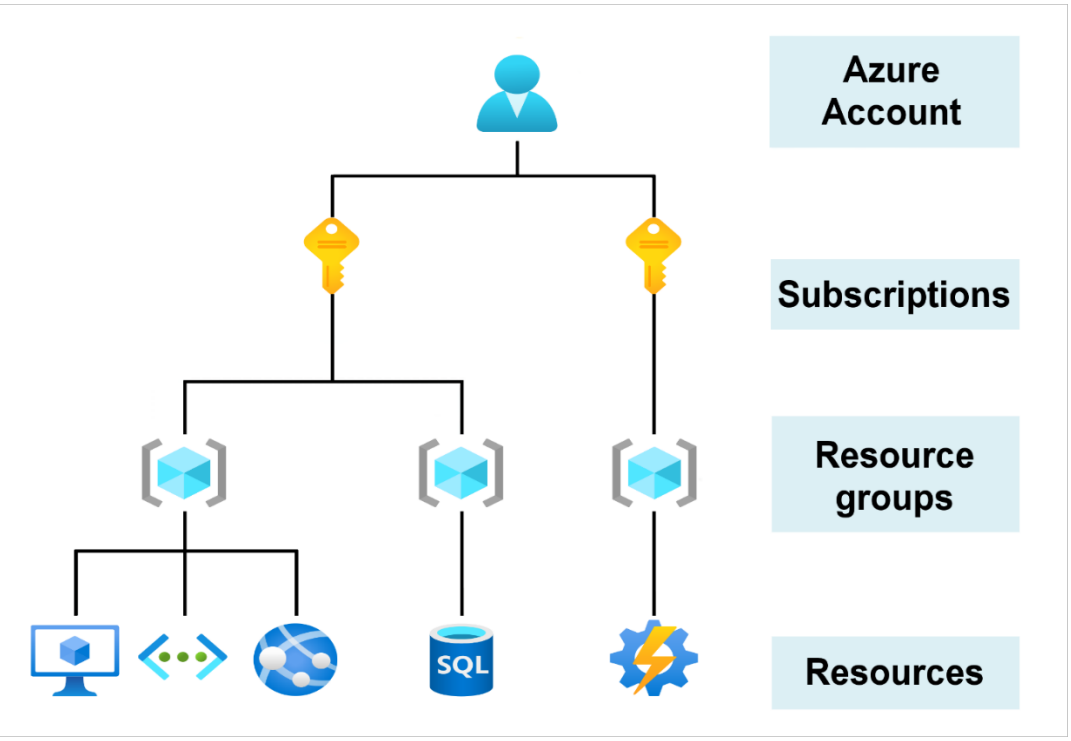
Capítulo 3. Introdução a contas do Azure

Para manter uma organização do seu ambiente Azure, é importante conhecer a hierarquia dos objetos no portal Azure. O administrador pode organizar seus objetos para manter uma governança sobre os serviços e garantir uma apuração correta sobre os investimentos relacionados por projeto ou departamento da empresa.

Quando um usuário (pessoal ou corporativo) abre um contrato com a Microsoft para utilização de Azure, ele abre um Azure Account. Esse é o primeiro nível de organização do Azure. Abaixo das Azure Accounts, temos a subdivisão subscrição (Subscriptions) e então os grupos de recursos (Resource groups). Um exemplo de utilização desta hierarquia é: a empresa pode usar apenas uma conta do Azure para os negócios, com assinaturas separadas para os departamentos de desenvolvimento, marketing e vendas.

Abaixo uma ilustração que ajuda na compreensão desta hierarquia:

Figura 6 – Ilustração mostrando os diferentes níveis de escopo da conta.



Fonte: Microsoft

Cloud Adoption Framework (CAF)

Para auxiliar os administradores e empresas que adotam o Azure na organização dos objetos dentro do portal Azure, além de padrões para implementação dos projetos foi criada a metodologia Cloud Adoption Framework (CAF).

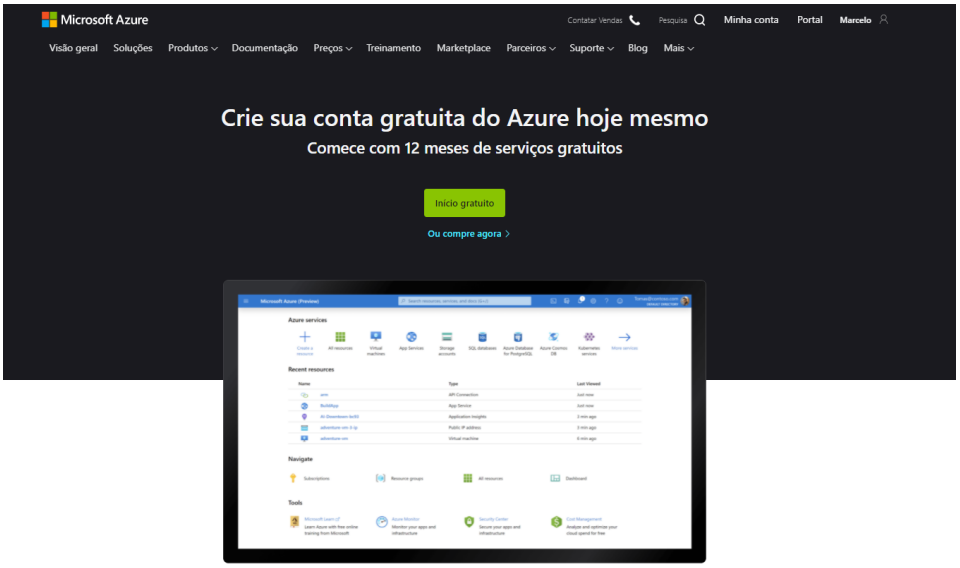
Esse documento é uma ótima fonte de consulta quando estamos no planejamento de um novo projeto. É acessada através da URL: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/.

Criando uma conta do Azure

Você pode ativar uma conta de Azure diretamente no site oficial da Microsoft, o Azure ou por meio de uma revenda da Microsoft através de um contrato corporativo.

O Azure disponibiliza um crédito gratuito inicial para profissionais testarem seus serviços. A criação da conta de avaliação é feita por meio do site e é válida por 12 meses com vários serviços 100% gratuitos:

Figura 7 – Captura de tela do website Azure – Conta gratuita.



Capítulo 4. Infraestrutura Global do Azure

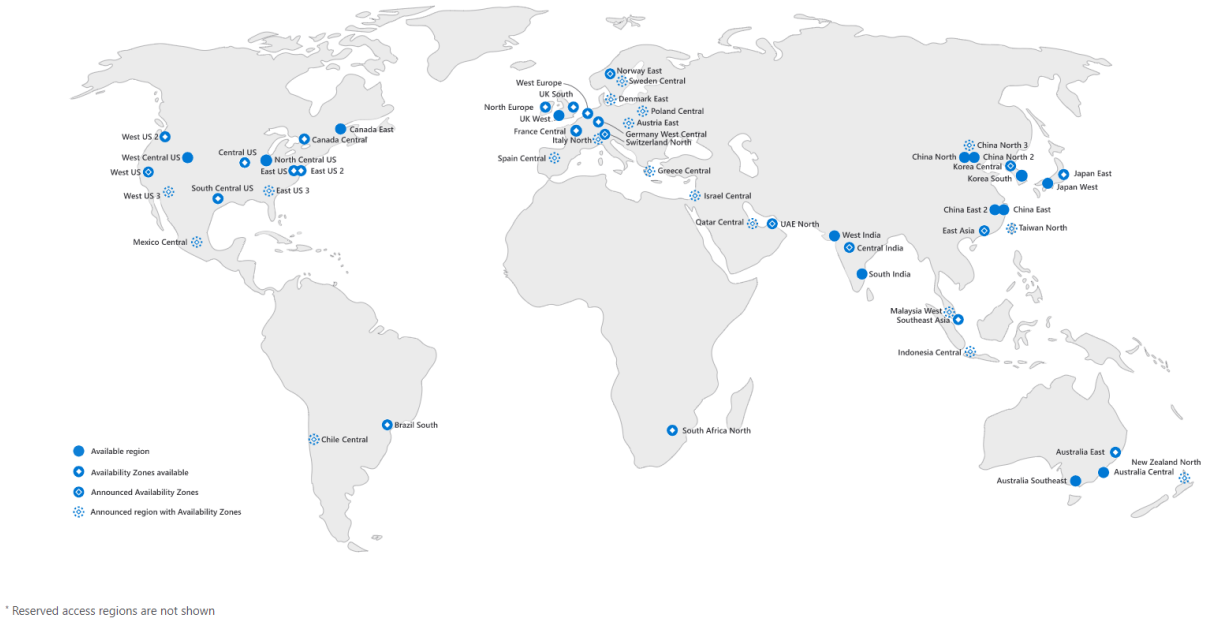
O Azure conta com a maior quantidade de regiões no mundo todo. Elas estão presentes em todos os continentes e contam com uma rede de ligação de alta velocidade entre elas. Uma região é a representação de um conjunto de datacenters interligados em uma localização geográfica específica, por exemplo a região Brazil South representa datacenters que estejam na porção sul no Brasil. A localização dos datacenters não é divulgada publicamente, garantindo uma segurança adicional para os usuários desta infraestrutura.

As regiões globais proporcionam maior escalabilidade e redundância. Elas também preservam a residência de dados de seus serviços, que por algumas vezes é necessária para atender regulamentações.

Regiões do Azure

Quando você implanta um recurso no Azure você precisa escolher a região em que deseja que ele seja implantado. Cada serviço do Azure tem disponibilidade e roadmap de implantações diferentes entre as regiões. Sempre consulte o site oficial do Azure para avaliar se aquele serviço que você irá utilizar estará disponível na região Azure escolhida.

Figura 8 – Ilustração das regiões disponíveis no Azure.



* Reserved access regions are not shown

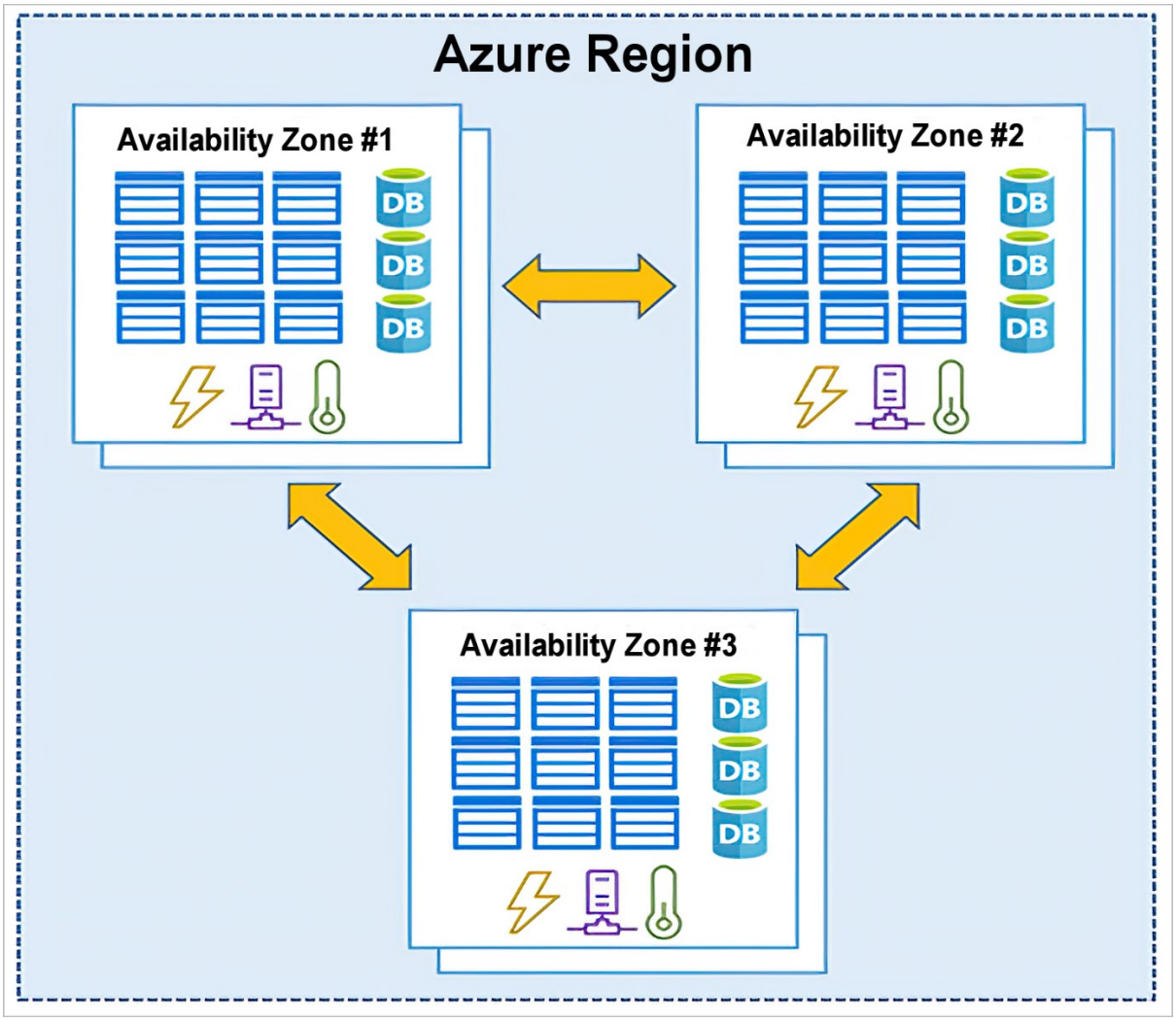
Fonte: Microsoft

Zonas de Disponibilidade do Azure (Availability Zone)

Quando estiver planejando seu projeto para rodar em Azure é importante listar os serviços que serão utilizados, para que seja analisado qual a região que será utilizada e identificar também qual a estratégia de prevenção a desastres com essa região. O planejamento começa com os requisitos do projeto, como por exemplo: a disponibilidade multirregional que garante um SLA de disponibilidade maior é necessária? Então é importante ficar atento se a região escolhida tem AZs.

AZs (Availability Zones), ou zonas de disponibilidade, são datacenters separados fisicamente dentro de uma região do Azure. Cada AZ é composta de um ou mais datacenters equipados com energia, resfriamento e rede independentes. Uma AZ é feita para ser redundância de um outro datacenter na mesma zona. Se uma zona ficar inativa, as outras continuarão funcionando. AZs são conectadas por meio de redes de fibra óptica privadas de alta velocidade.

Figura 9 – Diagrama mostrando três datacenters conectados em uma região do Azure para representar uma zona de disponibilidade.



Fonte: Microsoft.

Nem todas as regiões têm suporte para AZs. Para obter uma lista atualizada, confira Regiões com suporte para AZs no website oficial da Microsoft do Azure.

Usar AZs em seus aplicativos

Você pode usar as AZs para manter um nível maior de prevenção às indisponibilidades em seus aplicativos. Atuando na arquitetura do ambiente, é

possível optar por serviços de computação, armazenamento, rede e bancos de dados em uma zona que se replica em outras zonas. Essas zonas diferentes farão com que o seu SLA de disponibilidade geral seja maior.

Os serviços do Azure que dão suporte a AZs enquadram-se em duas categorias:

- Serviços em zonas: você fixa o recurso a uma zona específica (ex.: VMs, discos gerenciados e endereços IP).
- Serviços com redundância de zona: a plataforma replica automaticamente entre zonas (ex.: armazenamento com redundância de zona e Banco de Dados).

É sempre bom analisar a documentação oficial e atualizada no website do Azure, para determinar quais elementos da sua arquitetura você precisa associar a uma zona de disponibilidade.

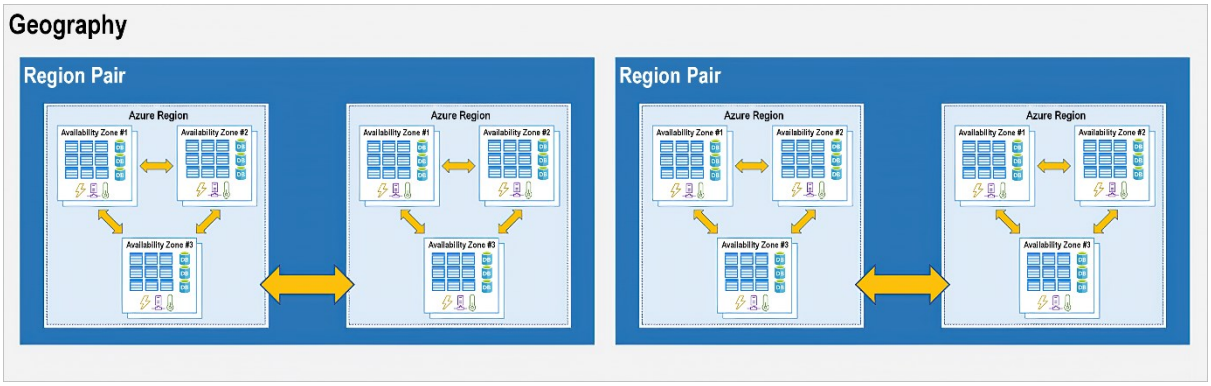
Azure Region Pairs

As AZs são criadas usando um ou mais data centers. Há um mínimo de três zonas em uma região de Azure, mas para aplicações mais críticas é necessário prever possíveis desastres maiores, que possam inutilizar uma região por completo. É para isso que foram criadas as regiões pares, ou Azure Region Pairs. Cada região do Azure é emparelhada com outra região na mesma área geográfica (como EUA, Europa ou Ásia) a pelo menos 480 km de distância. Essa interligação permite aos usuários replicação e conexão de recursos, como replicação de bancos de dados em uma geografia, o que ajuda a reduzir a probabilidade de interrupções devido a eventos como desastres naturais, quedas de energia bruscas ou interrupções de rede física afetarem as duas regiões ao mesmo tempo.

Essa é uma ótima estratégia de failover para suas aplicações mais críticas, mas não está disponível para todas as regiões, por isso é sempre importante avaliar

a documentação oficial do Azure no planejamento do seu projeto. Exemplos de regiões pares são East US e West US, muito utilizadas por empresas no Brasil devido à baixa latência de acesso aos serviços nestas regiões.

Figura 10 – Diagrama mostrando a relação entre regiões pares, geografia, região e datacenter. Cada região contém três AZs.



Fonte: Microsoft.

Alguns serviços oferecem armazenamento com redundância geográfica automática, alguns utilizando as regiões pares e outros qualquer região do globo.

Capítulo 5. Serviços de Computação Básica

Como citado no capítulo 4, os serviços de computação básicos entregam capacidades de computadores em formato de serviços gerenciados. O usuário do Azure pode contar com uma infraestrutura de servidor, um desktop virtual e opções de gerenciadores de contêineres para montagem do seu projeto de forma rápida e simples.

Serviços de computação do Azure

O serviço de computação é a categoria dos serviços de execução de softwares. Para a sua aplicação, você pode precisar de um servidor com Windows, Linux (várias distribuições), um ambiente em Docker ou Kubernetes ou simplesmente um executor de blocos de códigos sem servidor (serverless).

O Azure fornece estes serviços com suporte a diversos formatos desenvolvidos pela Microsoft, por terceiros como Oracle, IBM e SAP, e pela comunidade Open Source.

Alguns dos serviços mais utilizados são:

- Virtual Machines do Azure (VMs).
- Container Instances do Azure (ACI).
- Serviço de Kubernetes do Azure (AKS).
- Serviço de aplicativo do Azure (WebApp).
- Azure Functions.

Virtual Machines

O Azure Virtual Machine, ou simplesmente VMs, são servidores de diferentes tipos de configuração de processadores, memória RAM, armazenamento etc., para uso baseado em demanda. As VMs podem ser ativadas já com sistemas operacionais

e com imagens de softwares prontos. Através do Marketplace por exemplo, é possível instalar um servidor de SQL Server 2019 Enterprise preenchendo alguns parâmetros para a configuração e pagando apenas pelas horas utilizadas, tanto pela VM (poder de computação) quanto pela licença do SQL Server. Para acessar a VM você pode utilizar softwares dos sistemas operacionais, como o Windows Terminal Services ou um serviço do Azure chamado Bastion, que usa o navegador para emular o acesso no servidor.

As VMs são a representação das ofertas IaaS do Azure, uma vez que a infraestrutura é disponibilizada com suporte garantido às camadas de hardware, mas toda a manutenção e gestão da camada de software é de responsabilidade do usuário.

Figura 11 – Tabela de familia de Virtual Machines no Azure.

Type	Tamanhos comuns	Descrição
Propósito geral	B, Dsv3, Dv3, DSv2, Dv2, Av2, DC	CPU/memória equilibrados. Ideal para desenvolvimento/teste e para aplicativos de pequeno a médio porte e soluções de dados.
Computação otimizada	Fsv2	Relação de CPU/memória alta. Boa para aplicativos de tráfego médio, dispositivos de rede e processos em lote.
Memória otimizada	Esv3, Ev3, M, DSv2, Dv2	Relação de memória/núcleo alta. Ótima para banco de dados relacionais, caches médios a grandes e análises na memória.
Armazenamento otimizado	Lsv2, Ls	Alta taxa de transferência de disco e de E/S. Ideal para Big Data, SQL e bancos de dados NoSQL.
GPU	NV, NVv2, NC, NCv2, NCv3, ND	VMs especializadas, destinadas para renderização gráfica e edição de vídeo pesadas.
Alto desempenho	H	Nossas VMs de CPU mais potentes com adaptadores de rede de alto rendimento (RDMA) opcionais.

Fonte: Microsoft.

Virtual Machine Scale Sets

É possível montar uma estrutura de balanceamento de carga baseada em VMs interligadas, chamadas Virtual Machine Scale Sets. Essa estrutura pode ser utilizada para dar sustentação elástica às aplicações que utilizem o IaaS, como padrão de processamento no Azure.

Container Instances e Kubernetes Services do Azure

Aplicações modernas estão utilizando conceitos de Deployment em contêineres devido à flexibilidade para serem criados e excluídos rapidamente e escalabilidade horizontal imediata para atender demandas de usuários. Nesse contexto o Azure disponibiliza dois serviços PaaS para implantar os aplicativos baseados em contêineres: o Azure Container Instances (ACI) e o Azure Kubernetes Services (AKS).

Serviço de Aplicativo do Azure

Caso a aplicação que seja hospedada no Azure esteja em padrões tradicionais de hospedagem em Web Servers como o Windows IIS (Internet Information Services) ou o Apache, podemos contar com o Serviço de Aplicativo do Azure. O Serviço de Aplicativo é um serviço PaaS (plataforma como serviço). Além de poder implantar aplicativos já existentes, é possível ativar ambientes com soluções Open Source como Moodle e Wordpress de maneira simples e rápida.

Os serviços de aplicativo do Azure podem ser utilizados para websites, Apps móveis e aplicações de barramentos customizados de API, pois auxiliam em escalabilidade e disponibilidade melhores que uma infraestrutura IaaS. Requisitos rigorosos de desempenho, escalabilidade e segurança podem ser atendidos com estes serviços.

Azure Functions

O Azure Functions é um serviço PaaS de execução de bloco de código sem servidor (serverless). Elas podem ser usadas para executar uma chamada de API ou criar uma interface de resposta a um evento (geralmente por meio de uma solicitação REST). O mais interessante é que podemos ter uma escalabilidade muito grande nessa execução, sendo feita em poucos segundos sem nenhum tipo de gerenciamento de servidores.

Azure Windows Virtual Desktop

Muitas empresas possuem diferentes tipos de necessidades de configuração de Desktop para seus funcionários, o que acaba dificultando a compra de computadores. O Azure Windows Virtual Desktop, ou WVD como é chamado, é um serviço que gera uma área de trabalho e é executado diretamente na nuvem do Azure. Para acessar esse WVD utilizamos um aplicativo de área de trabalho virtual que pode ser acionado por Windows, Mac, IOS, Android e Linux, e pode ser acessado através de aplicações de acesso remoto a computadores.

É uma ótima solução em termos de custo x benefício para manter o parque de computadores da empresa padronizado, porém adequado às necessidades de desktop específicas utilizando as capacidades da nuvem, por exemplo um desenvolvedor que precisa de um desktop com 8 vCores e 64GB de RAM, enquanto o notebook dele tem apenas 4 vCores e 16GB de RAM.

Capítulo 6. Serviços de Redes do Azure

As redes de computadores revolucionaram a forma como a tecnologia evoluiu, criando a internet (rede global de computadores) e a colaboração entre os computadores de uma rede local.

Na arquitetura do projeto Azure é importante planejar o esquema de redes que garantirá a segurança e a escalabilidade necessárias para a sua aplicação.

O que é a Azure Virtual Network?

As Azure Virtual Network (vNets) conectam os serviços do Azure, como as VMs, os aplicativos Web e os bancos de dados, para que estes comuniquem-se uns com os outros, com a Internet e com computadores desktop, por exemplo. Planejar bem uma topologia de redes mitiga riscos de acessos indevidos à infraestrutura e desorganização de seus projetos Azure.

As vNets do Azure oferecem as funcionalidades de rede essenciais:

- Acesso à Internet.
- Comunicação entre recursos do Azure.
- Comunicação com On Premisses.
- Isolamento e segmentação.
- Rotear tráfego de rede.
- Filtrar tráfego de rede.
- Conectar redes virtuais.

Isolamento e segmentação

Dentro do projeto Azure podemos definir várias redes virtuais isoladas para atender necessidades específicas de cada aplicação, como por exemplo acesso à internet ou não, conexões com datacenters locais (On Premisses) etc. Para configurar uma vNet é necessário definir o range de IPs que serão utilizados para esta rede, e é importante pensar nos serviços que serão implantados para definir a quantidade de IPs diferentes que serão utilizados. Você pode dividir esse range de endereços IP em subNets e alocar parte do espaço de endereço definido para cada subNet nomeada.

Acesso à Internet

Servidores IaaS no Azure podem se conectar à Internet por padrão, sendo assim importante pensar na topologia de redes no início do projeto para definir quais serão os pontos de contato com o "mundo exterior" e bloquear os acessos desnecessários.

É um mito que o seu ambiente Azure tem que estar sempre com um endpoint exposto para a internet, isto é, a vNet pode ser projetada de tal forma que todos os serviços se comuniquem apenas internamente por Private endpoints e o acesso a esses serviços seja feito apenas de dentro do Azure.

Comunicação entre os recursos do Azure

A topologia de redes define a forma como cada serviço interno do Azure irá se comunicar. Para que essas comunicações ocorram existem diferentes padrões por serviços, sendo os mais comuns:

- **vNets:** as redes virtuais podem ser utilizadas para ligar serviços IaaS e PaaS do Azure como bancos de dados, WebApps e VMs, além de serviços externos por meio de VPNs de conexão com outros datacenters.

- **Endpoints de serviço**: recursos PaaS do Azure possuem Endpoints de acesso. Alguns exemplos são bancos de dados PaaS e Storage Accounts. Os endpoints podem ser configurados como as extremidades de acesso à vNet, organizando ainda mais a comunicação entre os serviços e isolando acessos indevidos aos mesmos.

Comunicação com datacenter On Premisses

Muitas vezes é necessário conectar uma vNet do Azure à rede de um datacenter interno da empresa, o chamado On Premisses. Para isso o Azure conta com um serviço de VPN e a possibilidade de ligação física direta entre datacenters chamada Express Route, onde é possível estabelecer uma comunicação rápida e segura entre essas duas extremidades. Os diferentes tipos de ligação entre o Azure e um datacenter On Premisses são:

- **VPN point to site:** similar à tradicional conexão VPN (rede virtual privada) amplamente utilizada On Premisses, a VPN point-to-Site faz com que um computador que esteja fora da rede corporativa acesse recursos de dentro da vNet.

- **VPN site to site:** a VPN site to site cria um túnel entre a rede On Premisses e a rede Azure para uma vNet específica. Isso faz com que seja possível interligar redes On Premisses com as redes do Azure de maneira transparente para os usuários.

- **As duas opções de VPNs funcionam pela internet e criptografam suas conexões.**

- **Azure ExpressRoute:** quando a interconexão entre os ambientes On Premisses e o Azure tem requisitos de transações intensas de baixa latência ou bloqueios totais de uso de internet até para a conexão, o Azure ExpressRoute pode atender esse requisito, pois se trata de uma ligação privada e dedicada física entre os datacenters da empresa e do Azure. O

ExpressRoute é provido por empresas especializadas em datacenters (a ligação física) e no Azure é feita a configuração do serviço.

Rotear tráfego de rede

É possível customizar o formato de roteamento de tráfego entre as vNets e subNets do Azure, além dos acessos externos e à internet. Para tal, o Azure conta com as seguintes possibilidades:

- **Tabelas de rotas:** o usuário pode definir como o tráfego de comunicação dos pacotes de redes deve ser direcionado entre os serviços Azure.
- **Border Gateway Protocol:** o BGP (Border Gateway Protocol) funciona com gateways de VPN do Azure ou ExpressRoute para propagar as rotas BGP On Premisses para redes virtuais do Azure.

Grupos de Segurança de Redes NSGs

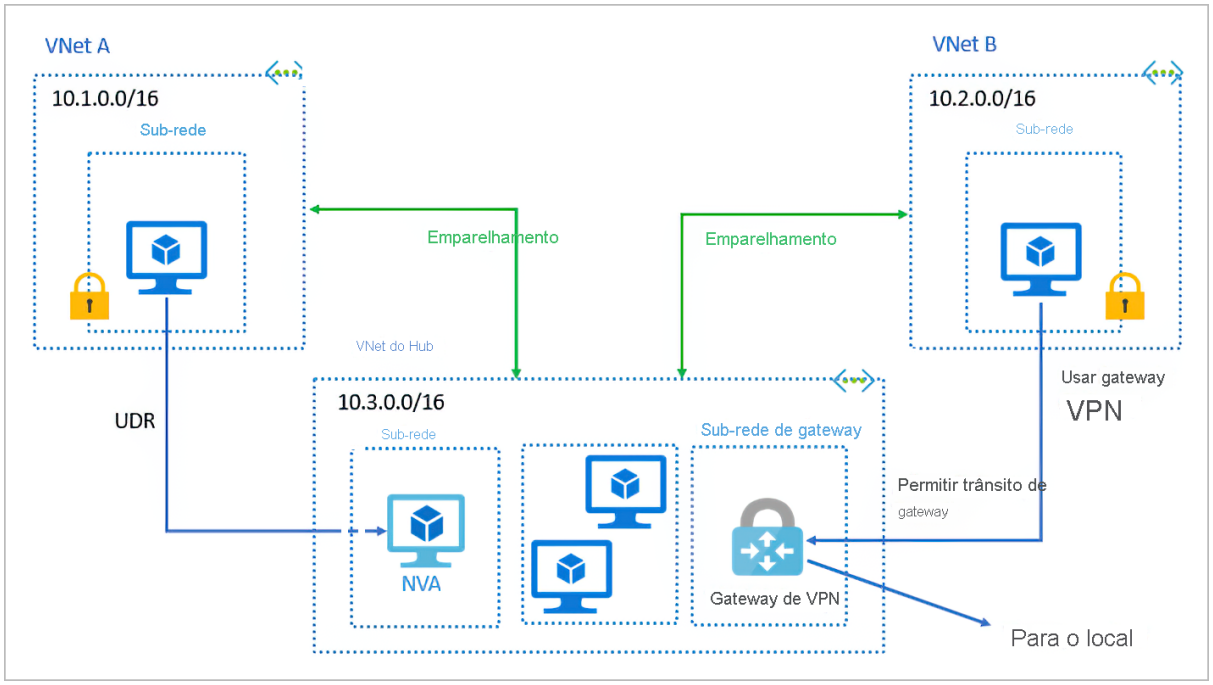
Um grupo de segurança de rede (NSG) é um recurso do Azure que permite criar regras de entrada e saída de pacotes entre os serviços da vNet, bloqueando tráfego por exemplo por IP de origem, portas de redes ou protocolos.

Conectar redes virtuais (vNet peering)

Quando o Azure é utilizado amplamente por uma empresa é natural ter que realizar conexões entre vNets, que atendem por exemplo projetos ou departamentos diferentes. Para tal, existe o conceito de vNet Peering.

Para realizar o Peering você utiliza o UDR, que é o roteamento definido pelo usuário. O UDR permite que os administradores de rede controlem as tabelas de roteamento citadas acima entre as subNets de uma vNet, bem como entre vNets, possibilitando um maior controle sobre o fluxo de tráfego de rede.

Figura 12 – Ilustração de uma topologia de redes conectando On Premisses com o Azure e vNet Peering habilitada.



Fonte: Microsoft.

Referências

Microsoft Azure oficial documentation. Microsoft, 2021. Disponível em: <https://docs.microsoft.com/en-us/azure/>. Acesso em: 26 abr. 2021.