

AZ-900TOO

Roteiro de aprendizagem 02:
Arquitetura e serviços
do Azure



Estrutura de tópicos do roteiro de aprendizagem

Roteiro de aprendizagem 02: estrutura de tópicos

Você vai aprender os conceitos a seguir:

1 Componentes de arquitetura do Azure

- Regiões e zonas de disponibilidade
- Assinaturas e grupos de recursos

2 Computação e rede

- Tipos de computação
- Hospedagem de aplicativos
- Redes virtuais

3 Armazenamento

- Serviços de armazenamento
- Opções de redundância
- Gerenciamento e migração de arquivos

4 Identidade, acesso e segurança

- Serviços de diretório
- Métodos de autenticação
- Modelos de segurança



Contas do Azure

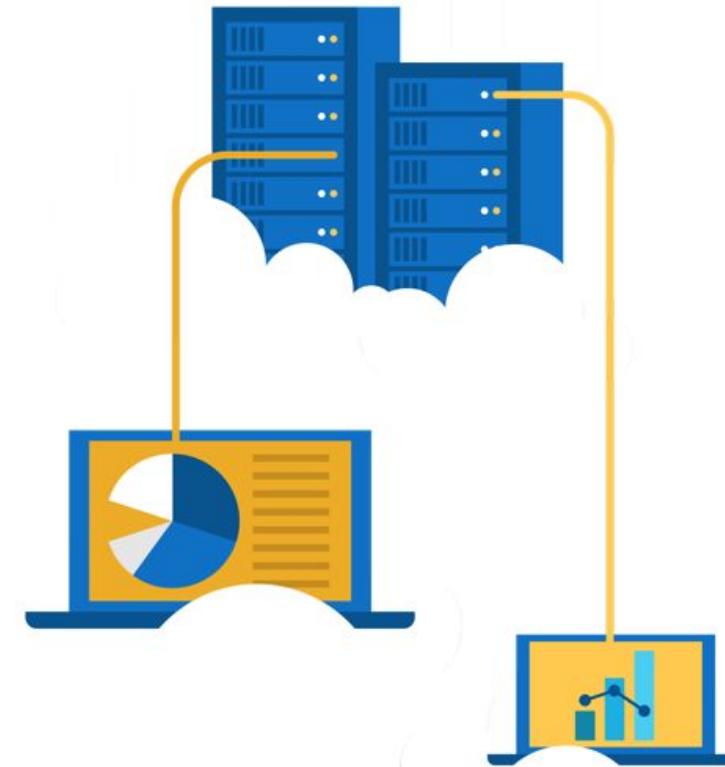
- Conta do Azure
- Conta gratuita do Azure
- Conta de estudante gratuita do Azure
- Área restrita do Microsoft Learn



Passo a passo: criar uma conta do Azure

Criar uma conta gratuita
do Azure

1. Criar uma conta gratuita
do Azure.



Exercício: explorar a área restrita do Learn

Explore a área restrita
do Learn

1. Ative a área restrita
2. Use o PowerShell
3. Mude para o Bash
4. Mude para o modo interativo
do Azure
5. Navegue no portal



Componentes de arquitetura do Azure

Principais componentes arquitetônicos do Azure: domínio de objetivo

- Descrever regiões, pares de regiões e regiões soberanas do Azure.
- Descrever as zonas de disponibilidade.
- Descrever os datacenters do Azure.
- Descrever os recursos e os grupos de recursos do Azure.
- Descrever as assinaturas.
- Descrever os grupos de gerenciamento.
- Descrever a hierarquia de grupos de recursos, assinaturas e grupos de gerenciamento.

Regiões

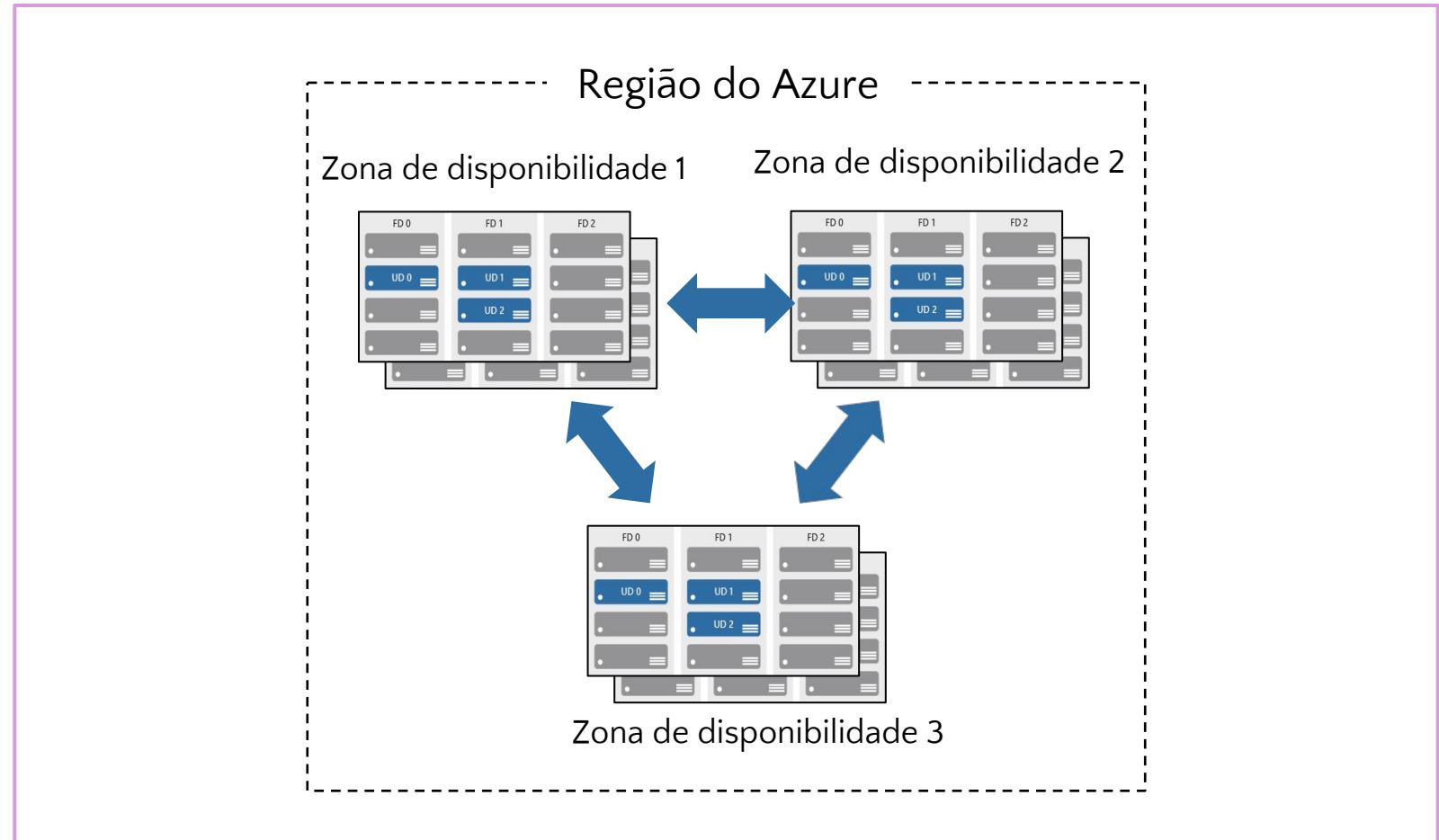
O Azure oferece mais regiões globais do que qualquer outro provedor de nuvem, com mais de 60 regiões representando mais de 140 países



- As regiões são compostas de um ou mais datacenters muito próximos.
- Eles fornecem flexibilidade e escala para reduzir a latência do cliente.
- As regiões preservam a residência dos dados com uma oferta abrangente de conformidade.

Zonas de disponibilidade

- Fornece proteção contra tempo de inatividade devido a falha do datacenter.
- Separe fisicamente os datacenters dentro da mesma região.
- Cada datacenter é equipado com alimentação, resfriamento e rede independentes.
- Conectadas por meio de redes privadas de fibra óptica.

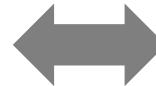


Pares de regiões

- No mínimo 300 milhas de separação entre pares de regiões.
- Replicação automática para alguns serviços.
- Recuperação de região priorizada em caso de interrupção.
- As atualizações são distribuídas sequencialmente para minimizar o tempo de inatividade.
- Link da Web:

<https://aka.ms/PairedRegions-ptb>

Região	Região
Centro-Norte dos EUA	Centro-Sul dos EUA
Leste dos EUA	Oeste dos EUA
Oeste dos EUA 2	Centro-Oeste dos EUA
Leste dos EUA 2	EUA Central
Canadá Central	Leste do Canadá
Norte da Europa	Oeste da Europa
Oeste do Reino Unido	Sul do Reino Unido
Alemanha Central	Nordeste da Alemanha
Sudeste da Ásia	Leste da Ásia
Leste da China	Norte da China
Leste do Japão	Oeste do Japão
Sudeste da Austrália	Leste da Austrália
Sul da Índia	Índia Central
Sul do Brasil (Principal)	Centro-Sul dos EUA

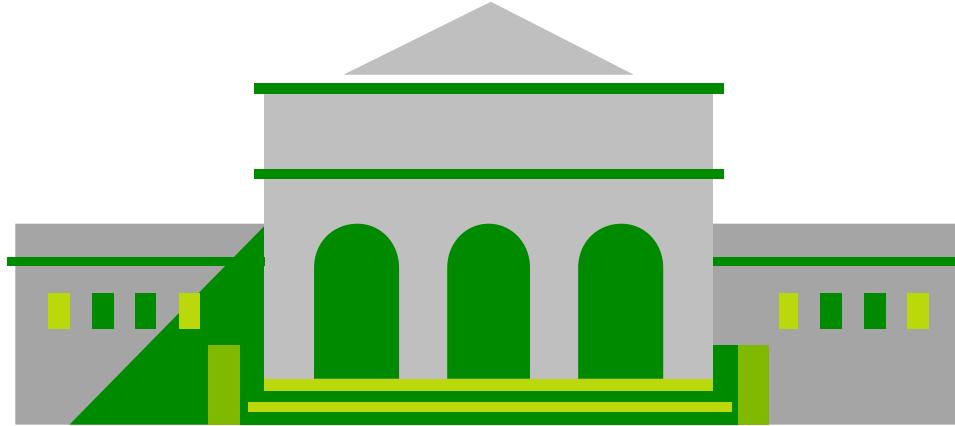


Regiões soberanas do Azure (serviços Governamentais dos EUA)

Atende às necessidades de segurança e conformidade das agências federais, governos estaduais e locais dos EUA e seus provedores de soluções.

Azure Governamental:

- Instância separada do Azure.
- Fisicamente isolada de implantações que não sejam do governo dos EUA.
- Acessível somente a pessoal verificado e autorizado.



Regiões soberanas do Azure (Azure China)

A Microsoft é o primeiro provedor estrangeiro de serviços de nuvem pública da China, em conformidade com as regulamentações governamentais.

10101
01010
00100

Recursos do Azure China:

- Instância fisicamente separada dos serviços de nuvem do Azure operados pela 21Vianet.
- Todos os dados permanecem dentro da China para garantir a conformidade.

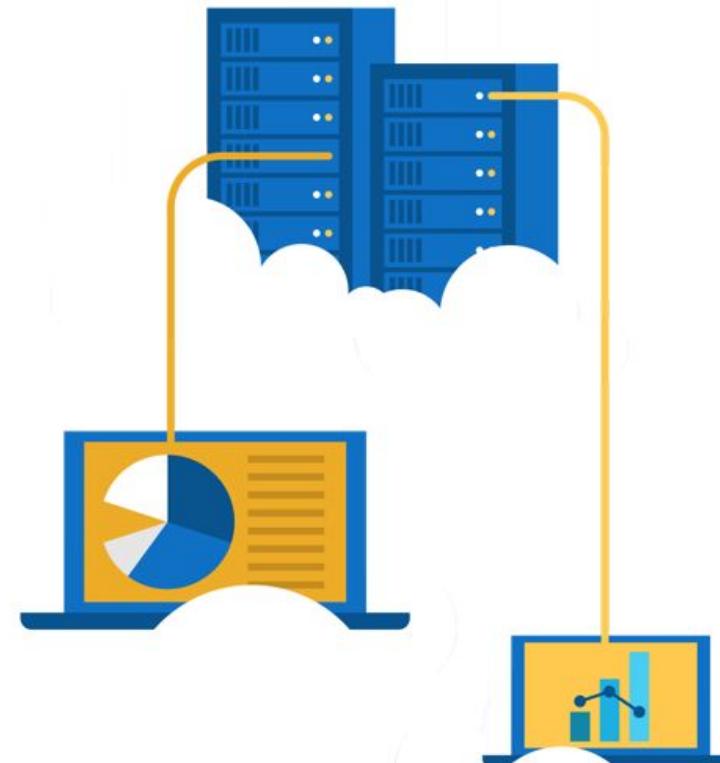
10101
01010
00100

10101
01010
00100

Passo a passo: explorar a infraestrutura global do Azure

Explore a infraestrutura global do Azure

1. Selecione **Explorar o Globo** (após a introdução).
2. Observe os diferentes ícones (geografia, regiões, PoP (pontos de presença) e assim por diante).
3. Encontre sua localização no globo e, em seguida, encontre o PoP e a região mais próximos.



Recursos do Azure

Os **recursos** do Azure são componentes como armazenamento, máquinas virtuais e redes que estão disponíveis para criar soluções de nuvem.



Máquinas virtuais



Contas de
armazenamento



Redes virtuais



Serviços de
aplicativos



Bancos de dados
SQL



Funções

Grupos de recursos

Um grupo de recursos

é um contêiner que você usa para gerenciar e agrregar recursos em uma única unidade.

- Os recursos podem existir em apenas um grupo de recursos.
- Os recursos podem existir em diferentes regiões.
- Os recursos podem ser movidos para diferentes grupos de recursos.
- Os aplicativos podem utilizar vários grupos de recursos.

Grupos de recursos
(Web mais BD, VM, armazenamento) em um grupo



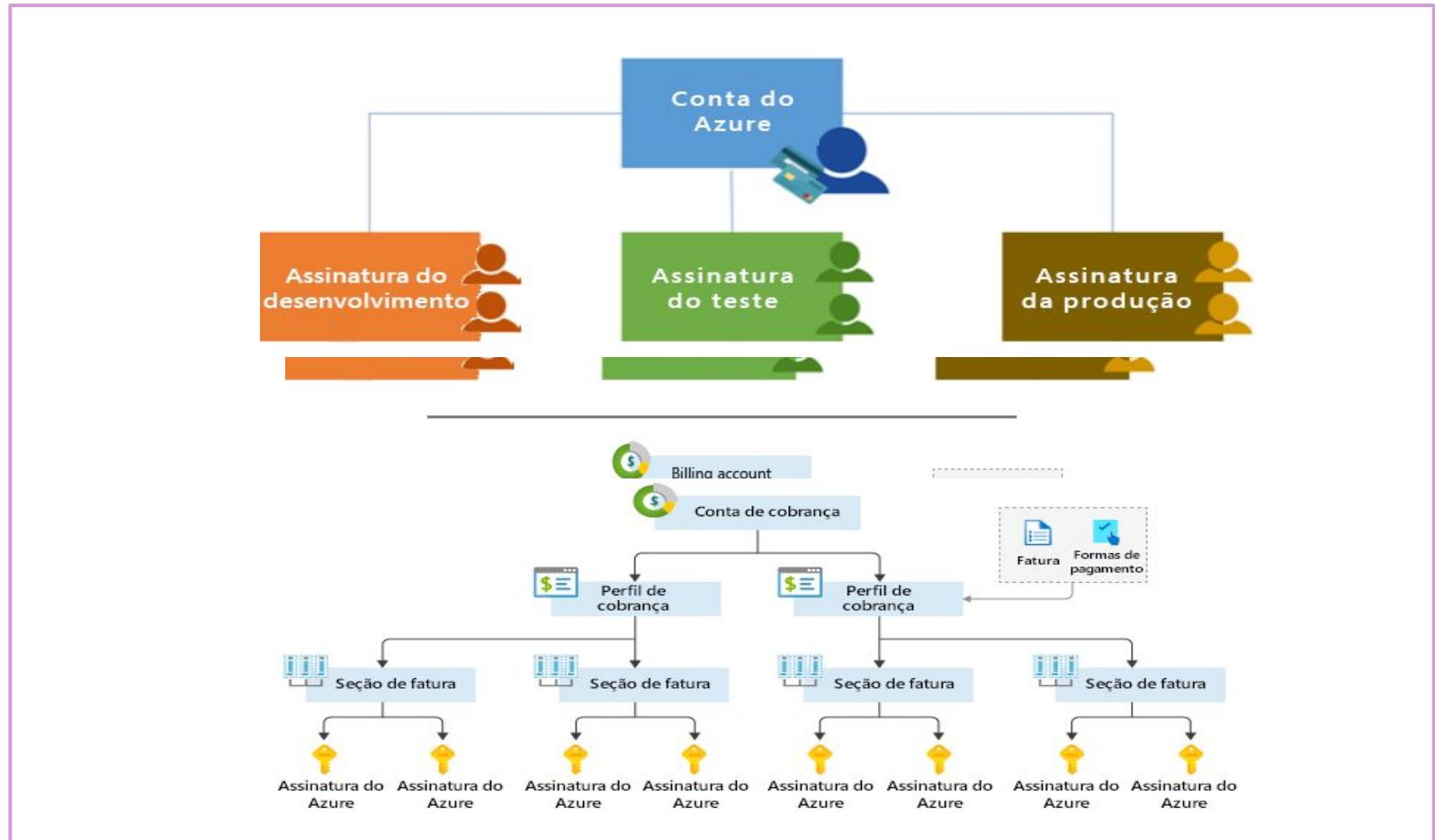
OU



Assinaturas do Azure

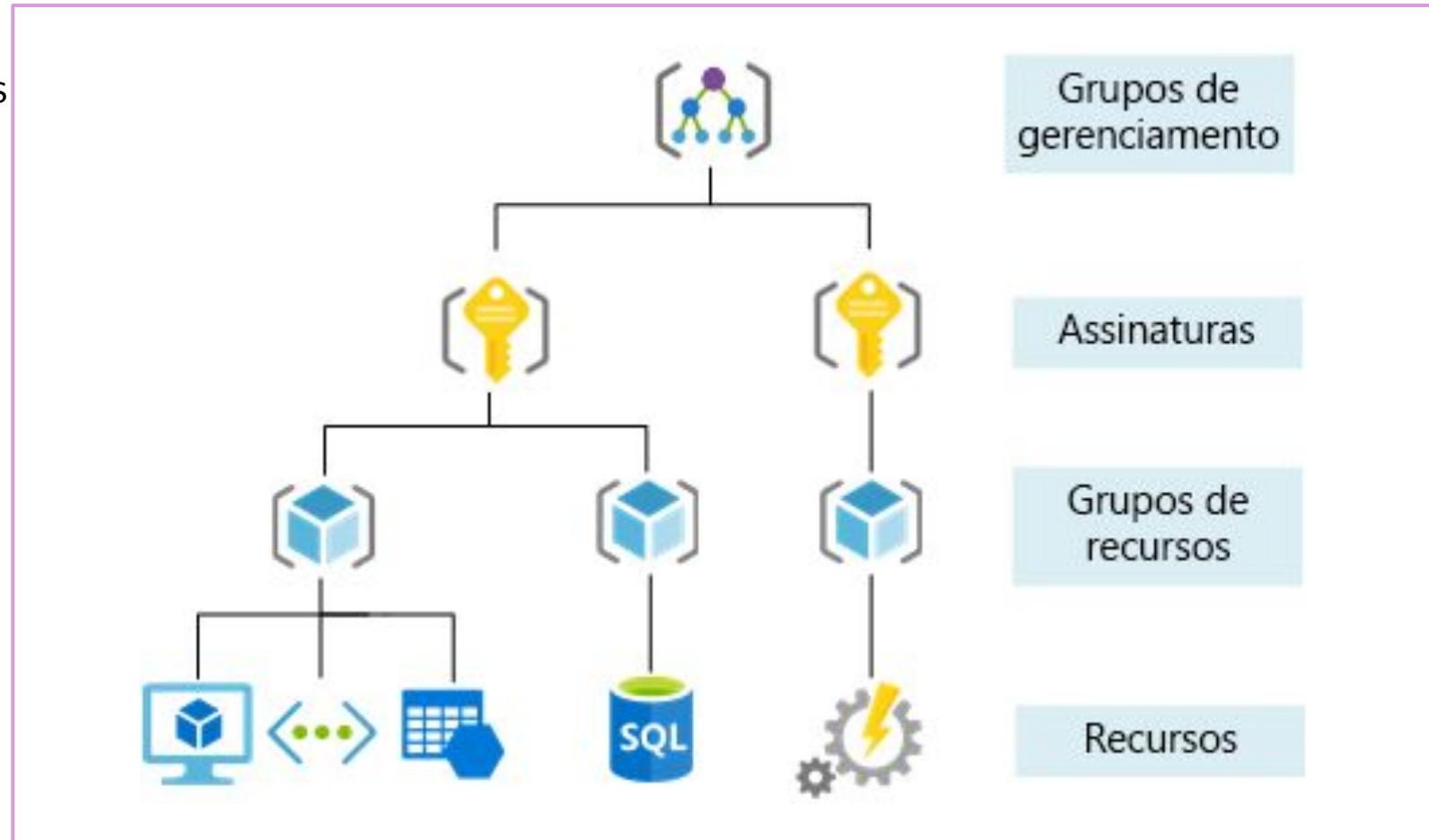
Uma assinatura do Azure fornece a você acesso autenticado e autorizado às contas do Azure.

- **Limite de cobrança:** gere relatórios de cobrança e faturas separados para cada assinatura.
- **Limite do controle de acesso:** gerenciar e controlar o acesso aos recursos que os usuários podem provisionar com assinaturas específicas.



Grupos de gerenciamento

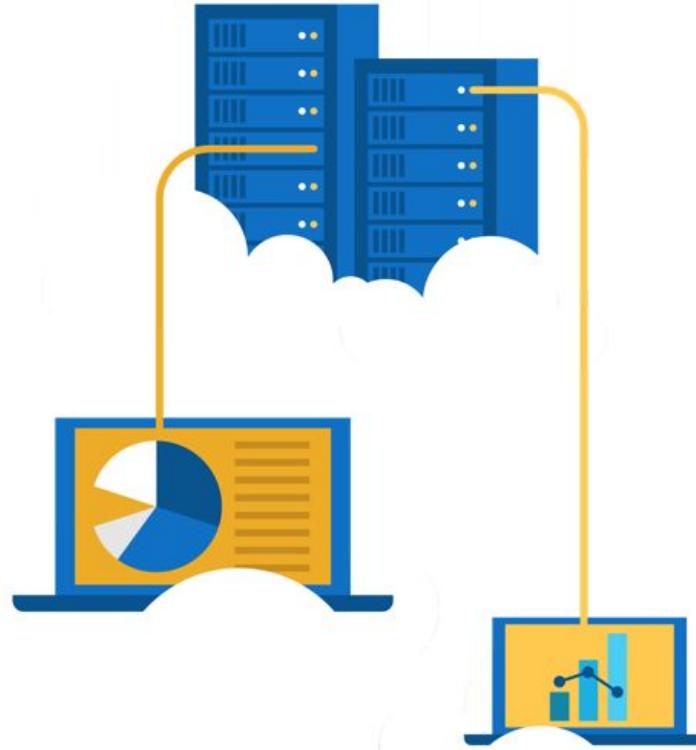
- Os grupos de gerenciamento podem incluir várias assinaturas do Azure.
- As assinaturas herdam as condições aplicadas ao grupo de gerenciamento.
- É possível oferecer suporte a 10.000 grupos de gerenciamento em um único diretório.
- Uma árvore de grupos de gerenciamento pode oferecer suporte a até seis níveis de profundidade.



Exercício: criar um recurso do Azure

Crie um recurso do Azure e monitore o grupo de recursos para ver se os recursos exigidos estão sendo criados no mesmo grupo.

1. Crie uma máquina virtual.
2. Monitore o grupo de recursos.



Computação e rede

Computação e rede: domínio de objetivo

Descrever os benefícios e o uso:

- Comparar tipos de computação, incluindo instâncias de contêiner, máquinas virtuais e funções.
- Descrever as opções de máquina virtual, incluindo VMs (máquinas virtuais), conjuntos de dimensionamento de máquinas virtuais, conjuntos de disponibilidade de máquinas virtuais e a Área de Trabalho Virtual do Azure.
- Descrever os recursos exigidos para as máquinas virtuais.
- Descrever as opções de hospedagem de aplicativos, incluindo Aplicativos Web do Azure, contêineres e máquinas virtuais.
- Descrever a rede virtual, incluindo a finalidade das Redes Virtuais do Azure, das sub-redes virtuais do Azure, do emparelhamento, do DNS do Azure, do Gateway de VPN e do ExpressRoute.
- Definir pontos de extremidade públicos e privados.

Serviços de computação do Azure

A **Computação** do Azure é um serviço sob demanda que fornece recursos de computação, como discos, processadores, memória, rede e sistemas operacionais.



Virtual
Virtuais



Aplicativo
Serviços



Contêiner
Instâncias



Serviços de
Kubernetes do Azure
(AKS)



Área de Trabalho
Virtual do Azure

Máquinas virtuais do Azure

As **máquinas virtuais** do Azure (VMs) são emulações de software de computadores físicos.

- Inclui processador virtual, memória, armazenamento e rede.
- Oferta de IaaS que oferece personalização e controle total.



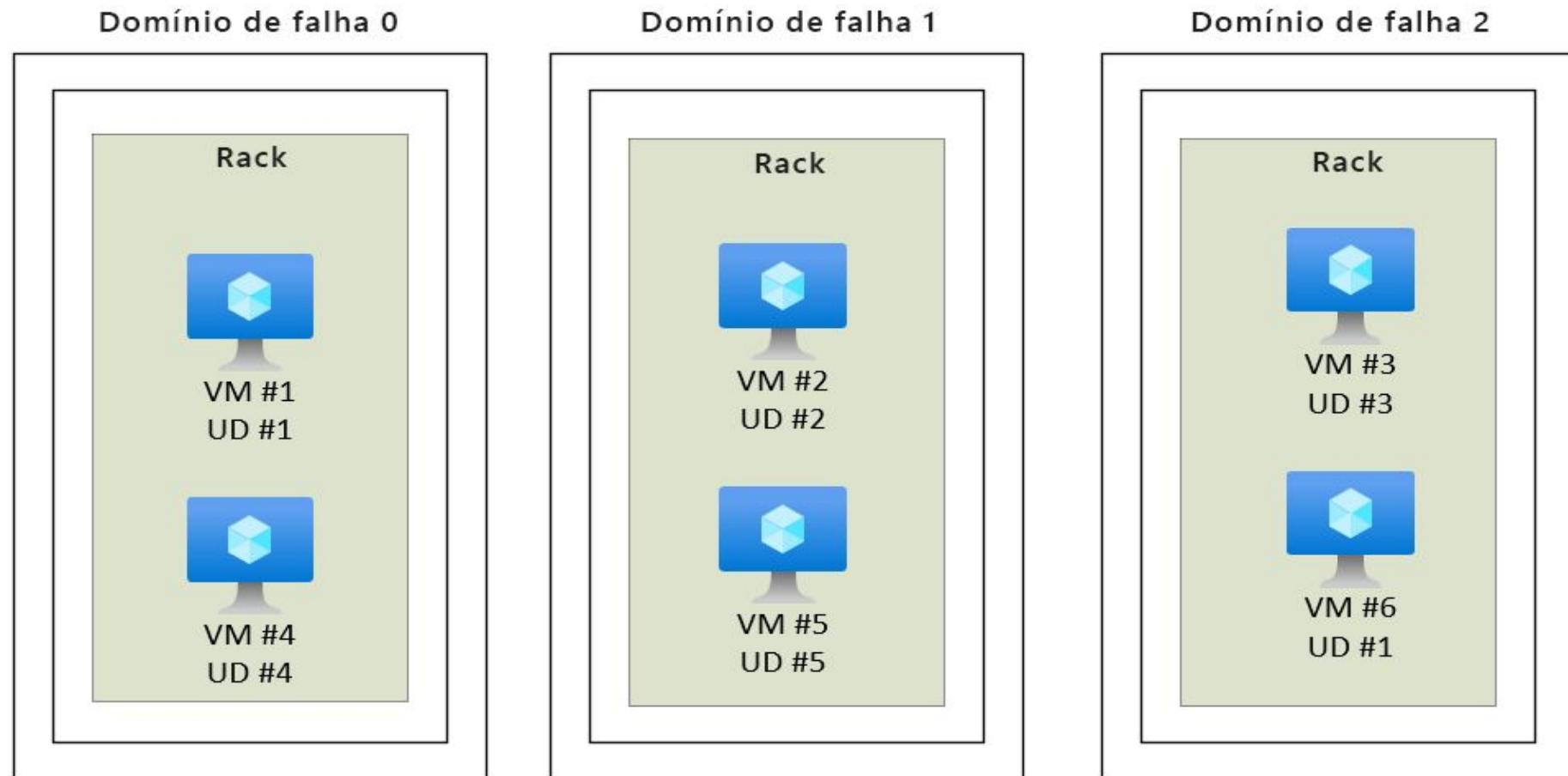
Conjuntos de dimensionamento de VMs

Os conjuntos de dimensionamento oferecem uma oportunidade de balanceamento de carga para dimensionar os recursos automaticamente.

- Escalar horizontalmente quando o recurso precisar aumentar.
- Reduzir horizontalmente quando o recurso precisar diminuir.



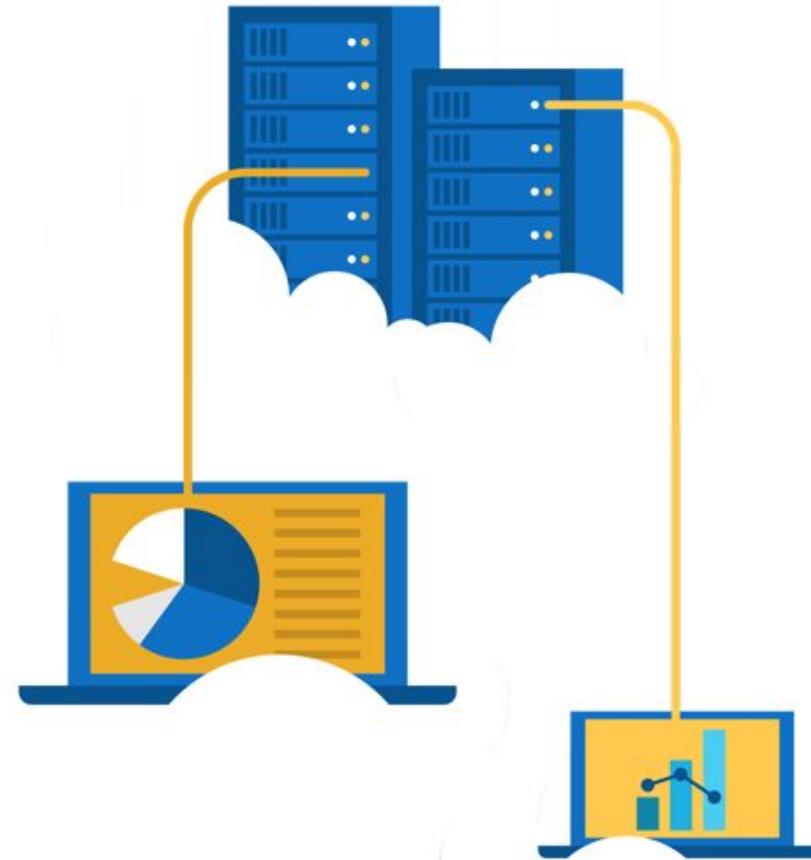
Conjuntos de disponibilidade de VM



Exercício: criar uma máquina virtual

Criar uma máquina virtual no portal do Azure, conectar-se à máquina virtual, instalar a função de servidor Web e teste.

1. Criar a máquina virtual.
2. Instale o pacote do servidor Web.



Área de Trabalho Virtual do Azure

A **Área de Trabalho Virtual do Azure** é uma virtualização de área de trabalho e aplicativo executada na nuvem.

- Crie um ambiente completo de virtualização da área de trabalho sem precisar executar outros servidores de gateway.
- Reduza o risco de que o recurso seja deixado para trás.
- Implantações reais de várias sessões.



Serviços de contêineres do Azure

Os **contêineres** do Azure fornecem um ambiente leve e virtualizado que não exige o gerenciamento do sistema operacional e pode responder a alterações sob demanda.



Instâncias de Contêiner do Azure: uma oferta de PaaS que executa um contêiner ou pod de contêineres no Azure.



Aplicativos de Contêiner do Azure: uma oferta de PaaS, como instâncias de contêineres, que pode balancear a carga e escalar.



Serviço de Kubernetes do Azure: um serviço de orquestração para contêineres com arquiteturas distribuídas e grandes volumes de contêineres.

Azure Functions



Azure Functions: uma oferta de PaaS que dá suporte a operações de computação sem servidor. O código baseado em eventos é executado quando chamado, sem exigir uma infraestrutura de servidor durante períodos inativos.

Comparar opções de computação do Azure

Máquinas virtuais

- Servidor baseado em nuvem que dá suporte a ambientes Windows ou Linux.
- Útil para migrações de lift-and-shift para a nuvem.
- Pacote do sistema operacional completo, incluindo o sistema operacional do host.

Área de Trabalho Virtual

- Fornece uma experiência de área de trabalho do Windows baseada em nuvem.
- Aplicativos dedicados para conexão e uso ou acessíveis de qualquer navegador moderno.
- O logon de vários clientes permite que vários usuários façam logon no mesmo computador na ao mesmo tempo.

Contêineres

- Ambiente leve e em miniatura adequado para a execução de microsserviços.
- Projetado para escalabilidade e resiliência por meio da orquestração.
- Os aplicativos e serviços são empacotados em um contêiner que fica na parte superior do sistema operacional do host. Vários contêineres podem ficar em um sistema operacional do host.

Serviços de Aplicativo do Azure

Os **Serviços de Aplicativos** do Azure consistem em uma plataforma totalmente gerenciada para criar, implantar e dimensionar aplicativos Web e APIs rapidamente.

- Trabalha com .NET, .NET Core, Node.js, Java, Python ou php.
- Oferta de PaaS com requisitos de nível corporativo de desempenho, segurança e conformidade.



Serviços de rede do Azure



A Rede Virtual do Azure (VNet) permite que os recursos do Azure se comuniquem uns com os outros, com a Internet e com as redes locais.

- Pontos de extremidade públicos, acessíveis de qualquer lugar na Internet.
- Pontos de extremidade privados, acessíveis somente de dentro da sua rede.
- As sub-redes virtuais segmentam sua rede para atender às suas necessidades.
- O emparelhamento de rede conecta suas redes privadas diretamente.

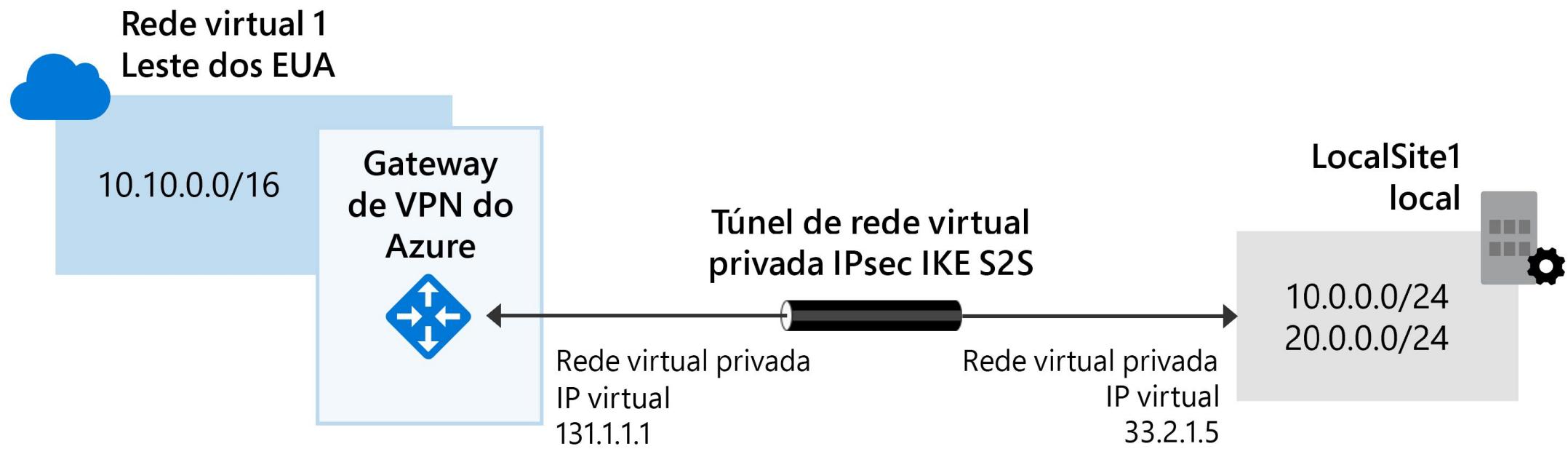
Passo a passo: configurar o acesso à rede

Configure o acesso público à máquina virtual criada anteriormente.

1. Verifique as portas abertas no momento.
2. Criar uma rede grupo de segurança
3. Configurar o acesso HTTP (porta 80)
4. Testar a conexão.

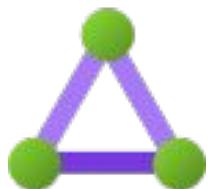
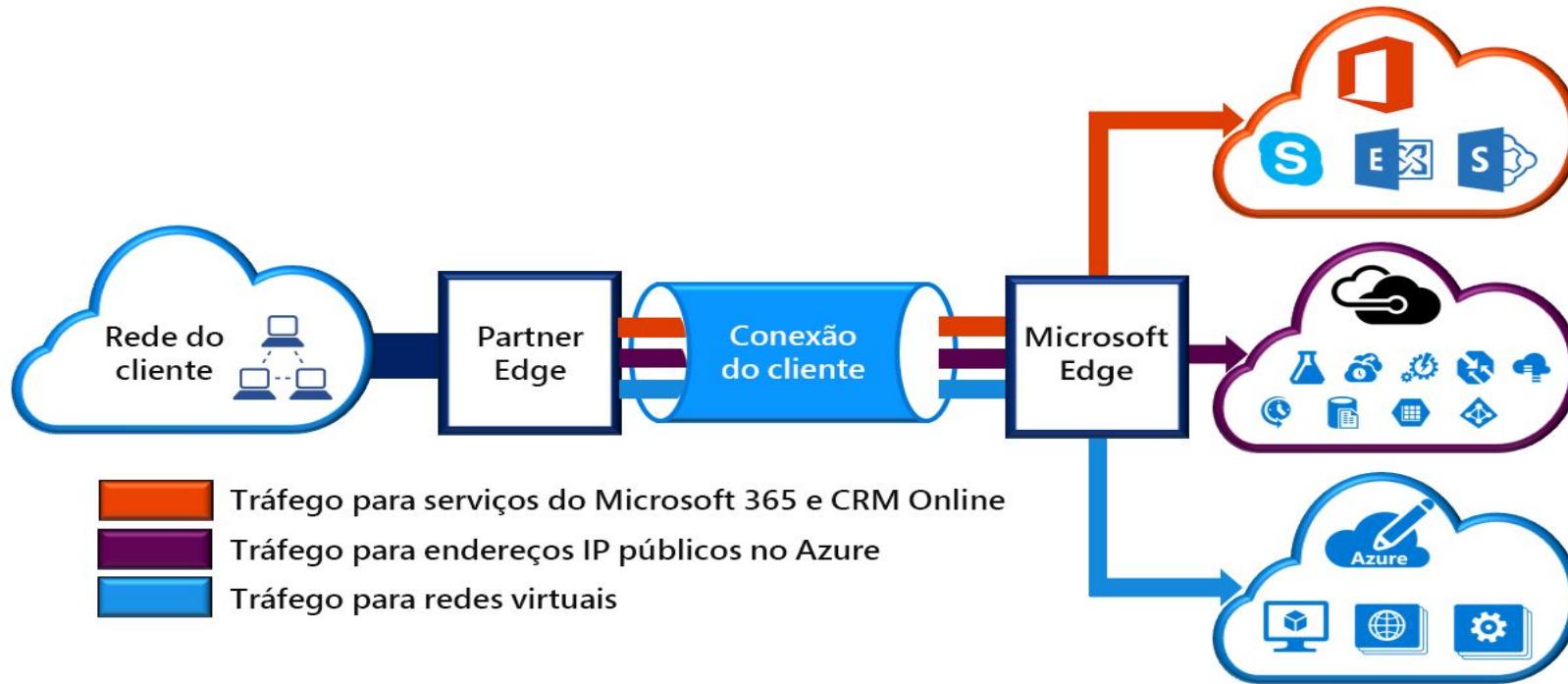


Serviços de rede do Azure: Gateway de VPN



O **Gateway de VPN** é usado para enviar tráfego criptografado entre uma rede virtual do Azure e uma no local pela Internet pública.

Serviços de rede do Azure: ExpressRoute



O **ExpressRoute** estende as redes locais para o Azure por meio de uma conexão privada facilitada por um provedor de conectividade.



DNS do Azure

- Confiabilidade e desempenho aproveitando uma rede global de servidores de nome DNS usando a rede Anycast.
- A segurança do DNS do Azure baseia-se no gerenciador de recursos do Azure, habilitando o controle de acesso baseado em função e o monitoramento e o registro em log.
- Facilidade de uso para gerenciar seus recursos externos e do Azure com um único serviço DNS.
- As redes virtuais personalizáveis permitem que você use nomes de domínio privados e totalmente personalizados em suas redes virtuais privadas.
- Os registros de alias dão suporte a conjuntos de registros de alias para apontar diretamente para um recurso do Azure.

Armazenamento



Armazenamento: domínio de objetivo

Descrever os benefícios e o uso

- Comparar os serviços de armazenamento do Azure.
- Descrever as camadas de armazenamento.
- Descrever as opções de redundância.
- Descrever as opções de conta de armazenamento e os tipos de armazenamento.
- Identificar opções para mover arquivos, incluindo o AzCopy, o Gerenciador de Armazenamento do Azure e a Sincronização de Arquivos do Azure.
- Descrever as opções de migração, incluindo as Migrações para Azure e o Azure Data Box.

Contas de armazenamento

- Deve ter um globalmente nome exclusivo.
- Fornecer acesso à Internet em todo o mundo.
- Determinar os serviços de armazenamento e as opções de redundância.



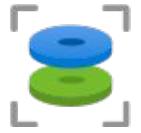
Redundância de armazenamento

Configuração de redundância	Implantação	Durabilidade
LRS (armazenamento com redundância local)	Datacenter individual na região primária	11 noves
ZRS (armazenamento com redundância de zona)	Três zonas de disponibilidade na região primária	12 noves
GRS (armazenamento com redundância geográfica)	Datacenter único no primário e região secundária	16 noves
GZRS (armazenamento com redundância de zona geográfica)	Três zonas de disponibilidade na região primária e um único datacenter na região secundária	16 noves

Serviços de armazenamento do Azure



Blob do Azure: otimizado para o armazenamento de quantidades massivas de dados não estruturados, como texto ou dados binários.



Disco do Azure: fornece discos para máquinas virtuais, aplicativos e outros serviços acessarem e utilizarem.



Fila do Azure: serviço de armazenamento de mensagens que fornece armazenamento e recuperação para grandes quantidades de mensagens, cada uma com até 64 KB.



Arquivos do Azure: configura um compartilhamento de arquivos de rede altamente disponível que pode ser utilizado usando o protocolo Bloco de Mensagens do Servidor.



Tabelas do Azure: fornece uma opção de chave/atributo para o armazenamento de dados estruturados não relacionais com um design sem esquema.

Pontos de extremidade públicos do serviço de armazenamento

Serviço de armazenamento	Ponto de extremidade público
Armazenamento de Blobs	<code>https://<storage-account-name>.blob.core.windows.net</code>
Data Lake Storage Gen2	<code>https://<storage-account-name>.dfs.core.windows.net</code>
Arquivos do Azure	<code>https://<storage-account-name>.file.core.windows.net</code>
Armazenamento de filas	<code>https://<storage-account-name>.queue.core.windows.net</code>
Armazenamento de Tabelas	<code>https://<storage-account-name>.table.core.windows.net</code>

Camadas de acesso de armazenamento do Azure

Frequente	Esporádico	Frio	Arquivo Morto
Otimizada para armazenamento de dados acessados com frequência.	Otimizada para armazenamento de dados acessados com pouca frequência e armazenados por pelo menos 30 dias.	Otimizado para o armazenamento de dados acessados com pouca frequência e armazenados por pelo menos 90 dias.	Otimizada para armazenamento de dados acessados raramente e armazenados por pelo menos 180 dias com requisitos de latência flexíveis.

Exercício: criar um armazenamento de blobs

Crie uma conta de armazenamento com um contêiner de armazenamento de blobs. Trabalhar com arquivos de blobs.

1. Crie uma conta de armazenamento.
2. Crie um contêiner de blob.
3. Carregue e acessar um blob.



Migrações para Azure

- Plataforma de migração unificada.
- Intervalo de ferramentas integradas e autônomas.
- Avaliação e migração.



Azure Data Box

- Armazenar até 80 terabytes de dados.
- Mova os backups de recuperação de desastre para o Azure.
- Proteja seus dados em uma caixa robusta durante o trânsito.
- Migre dados do Azure para conformidade ou necessidades regulatórias.
- Migre dados para o Azure de locais remotos com conectividade limitada ou sem conectividade.



Opções de gerenciamento de arquivos

AzCopy

- Utilitário de linha de comando.
- Copiar blobs ou arquivos de ou para sua conta de armazenamento.
- Sincronização em uma direção.

Gerenciador de Armazenamento do Azure

- Interface gráfica do usuário (de modo semelhante ao Windows Explorer).
- Compatível com o Windows, MacOS e Linux.
- Usa o AzCopy para lidar com operações de arquivo.

Sincronização de Arquivos do Azure

- Sincroniza os arquivos do Azure e locais de forma bidirecional.
- A camada de nuvem mantém os arquivos acessados com frequência no local, enquanto libera espaço.
- Reprovisionamento rápido de um servidor local que falhou (instalação e ressincronização).

Identidade, acesso e segurança

Identidade, acesso e segurança: domínio de objetivo

Descrever os benefícios e o uso

- Descrever os serviços de diretório no Azure, incluindo o Microsoft Entra ID e o Microsoft Entra Domain Services.
- Descrever métodos de autenticação no Azure, incluindo SSO (logon único), MFA (autenticação multifator) e sem senha.
- Descrever as identidades externas e o acesso de convidado no Azure.
- Descrever o Acesso Condicional do Entra.
- Descrever o controle de acesso baseado em função (RBAC).
- Descrever o conceito de Confiança Zero.
- Descrever a finalidade do modelo de defesa em profundidade.
- Descrever a finalidade do Microsoft Defender para Nuvem.

ID do Microsoft Entra

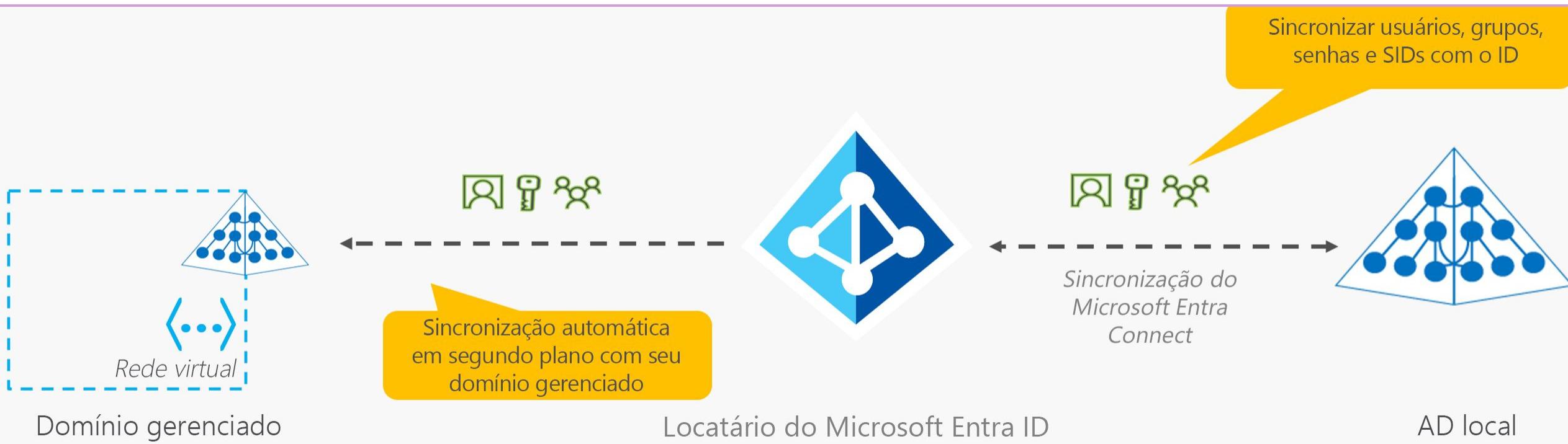
O Microsoft Entra ID

é o serviço de gerenciamento de identidades e acesso baseado em nuvem do Microsoft Azure.

- Autenticação (os funcionários entram para acessar os recursos).
- Logon único (SSO)
- Gerenciamento de aplicativos.
- Negócios para Negócios (B2B).
- Gerenciamento de dispositivos.



Microsoft Entra Domain Services



- Obtenha os benefícios dos serviços de domínio baseados em nuvem sem gerenciar os controladores de domínio.
- Execute aplicativos herdados (que não podem utilizar os padrões de autenticação modernos) na nuvem.
- Sincronizar automaticamente a partir do Microsoft Entra ID.

Comparar aautenticação e autorização

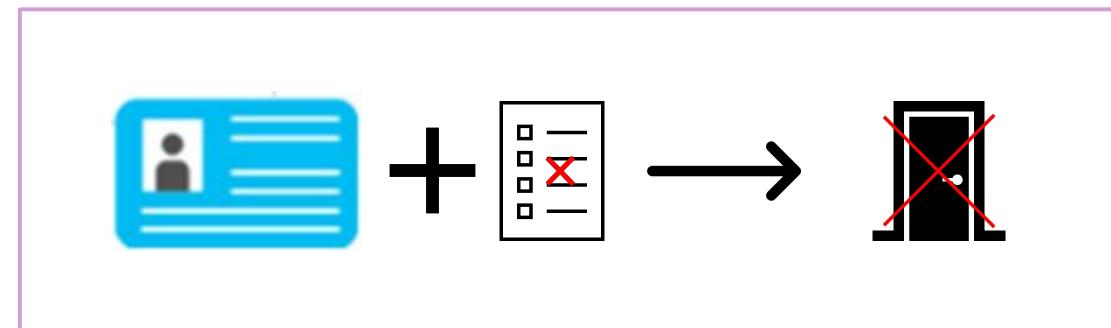
Autenticação

- Identifica a pessoa ou serviço buscando acesso a um recurso.
- Solicita credenciais de acesso legítimo.
- Base para criar princípios de identidade e controle de acesso seguros.



Autorização

- Determina o nível de acesso de uma pessoa ou serviço autenticado.
- Define quais dados eles podem acessar e o que podem fazer com eles.



Autenticação multifator



Fornece segurança adicional para as identidades, exigindo dois ou mais elementos para autenticação completa.

- Algo que você sabe .. Algo que você possui .. Algo que você é

B2B do Microsoft Entra External ID

Colaboração B2B



parceiros, fornecedores,
outros colaboradores

convite ou
inscrição para
autoatendimento

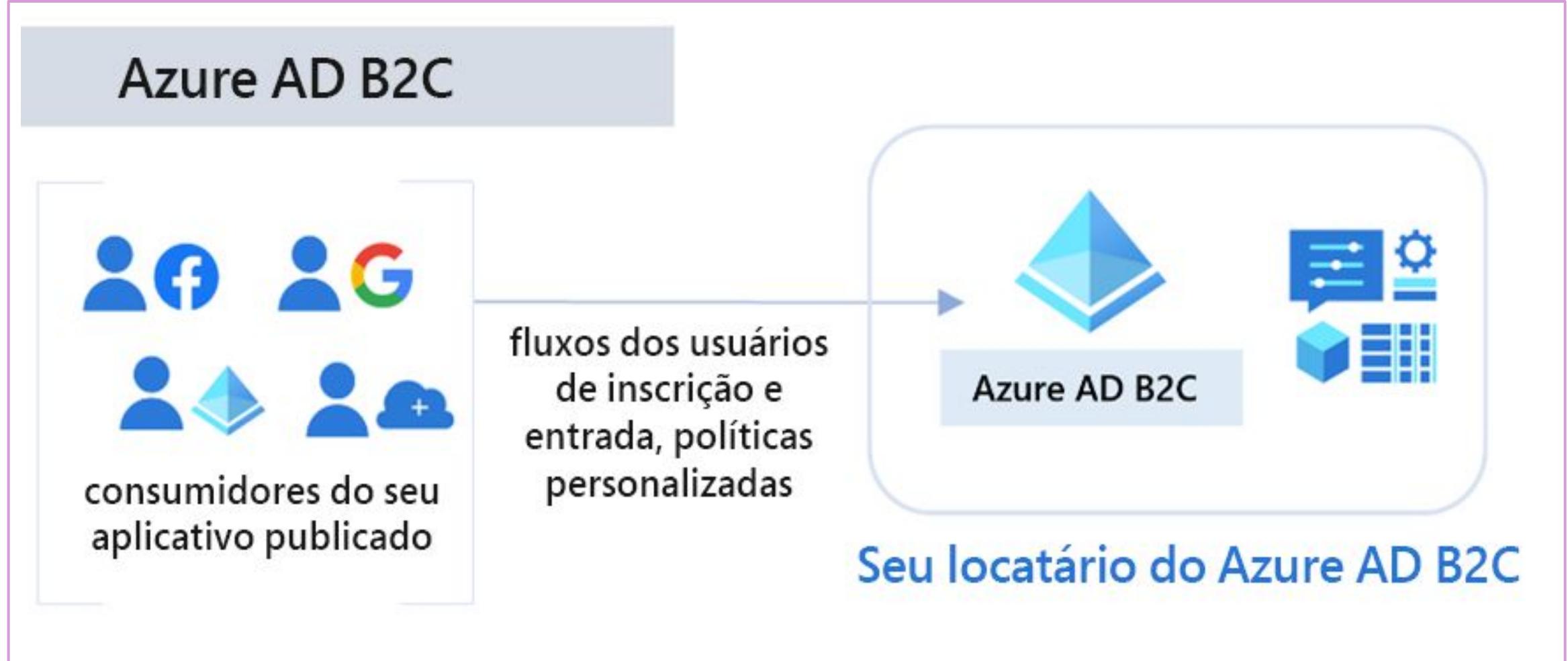


ID externa do Microsoft Entra



Seu locatário

B2C do Identidades Externas do Azure AD

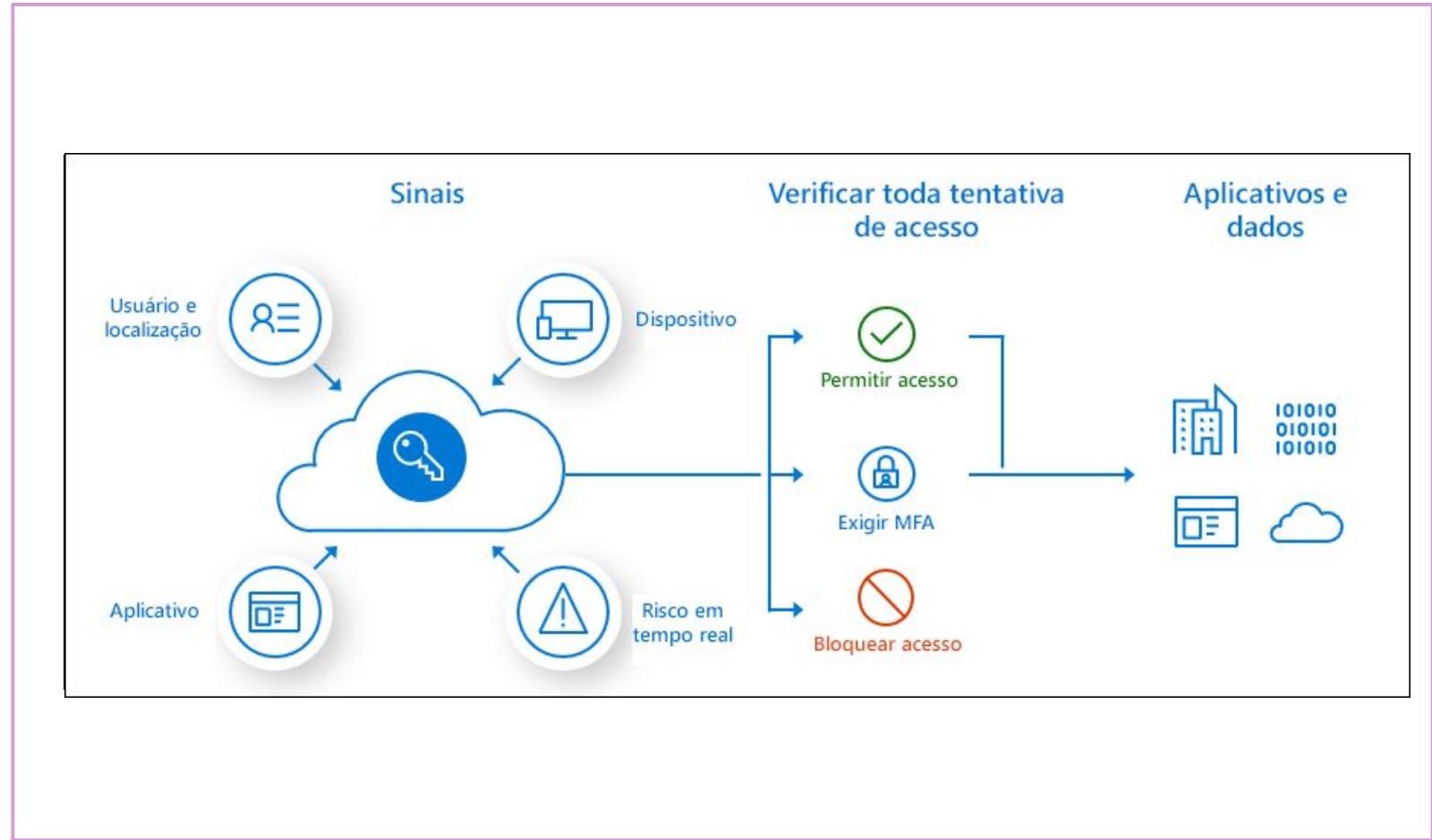


Acesso Condisional

O Acesso Condisional

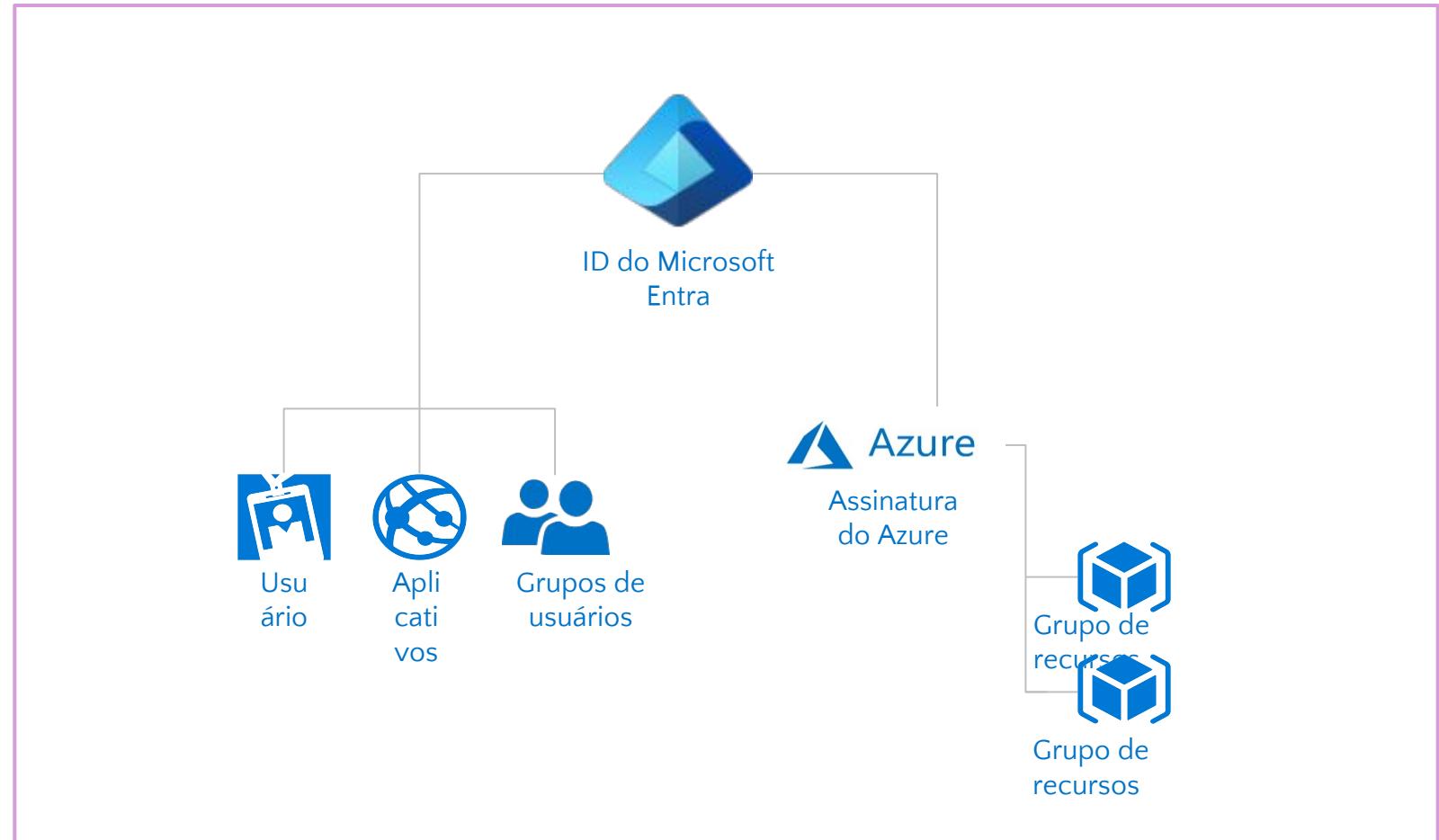
é utilizado para reunir sinais, tomar decisões e impor políticas organizacionais.

- Associação de usuário ou grupo
- Local do IP
- Dispositivo
- Aplicativo
- Detecção de risco



Controle de acesso baseado em função

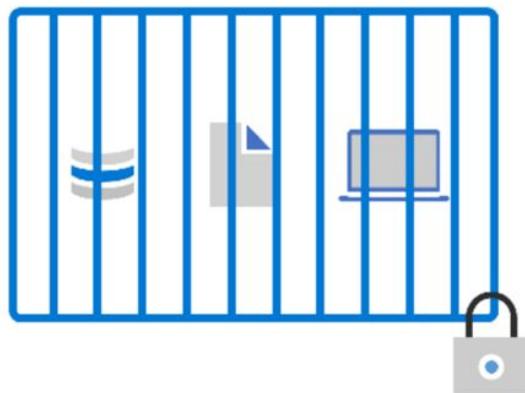
- Gerenciamento de acesso de granularidade fina.
- Divida as tarefas dentro da equipe e conceda somente a quantidade de acesso de que os usuários precisam para trabalhar.
- Habilite o acesso ao portal do Azure e o controle de acesso aos recursos.



Confiança Zero

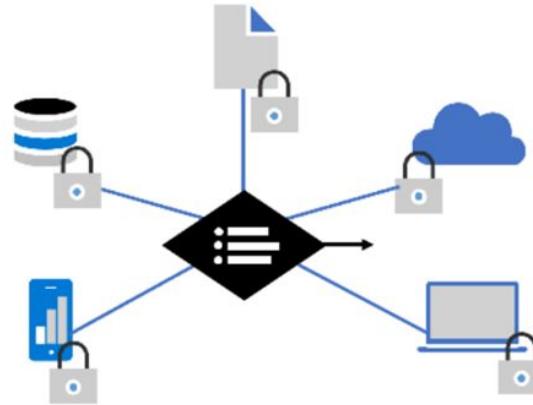
Proteja os ativos onde eles estiverem com a Confiança Zero

Simplifique e torne a segurança mais eficaz



Abordagem clássica

Restringe tudo a uma rede 'segura'

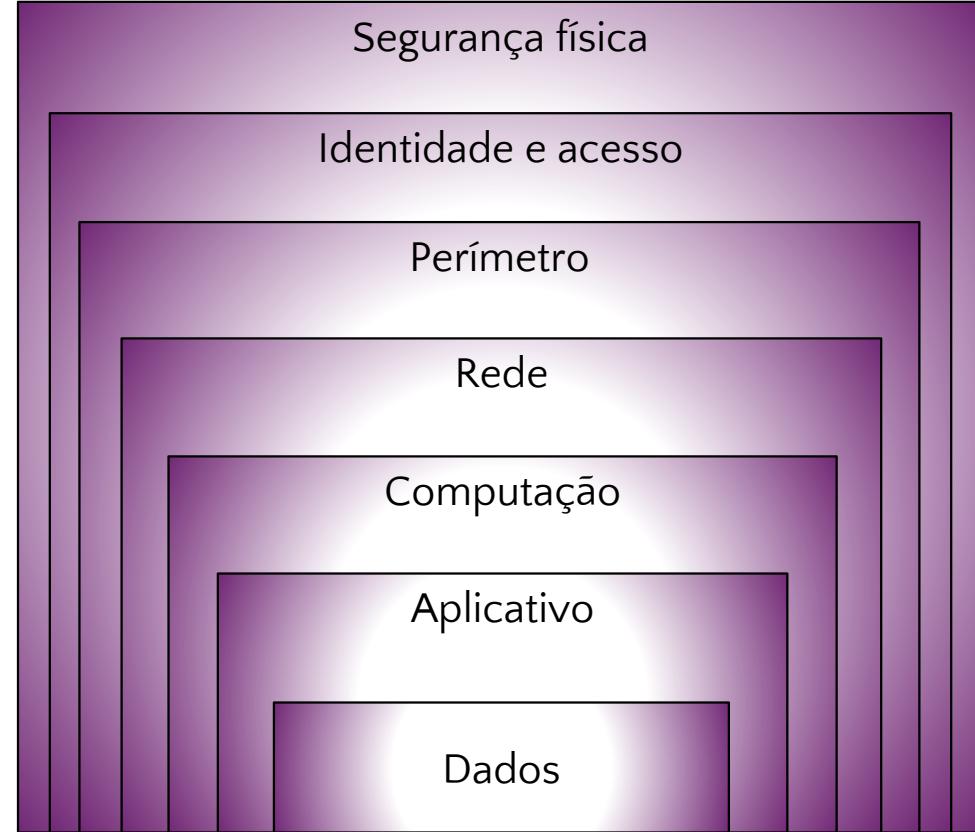


Confiança Zero

Protege os ativos em qualquer lugar com uma política central

Proteção completa

- Uma abordagem em camadas para proteger sistemas de computador.
- Fornece vários níveis de proteção.
- Ataques contra uma camada são isolados das camadas subsequentes.



Microsoft Defender para Nuvem

O Microsoft Defender para Nuvem é um serviço de monitoramento que fornece proteção contra ameaças nos datacenters do Azure e locais.

- Fornece recomendações de segurança.
- Detectar e bloquear malware.
- Analisar e identificar ataques potenciais.
- Controle de acesso just-in-time para portas.

The screenshot shows the Microsoft Defender for Cloud general overview dashboard. At the top, it displays key metrics: 2 Assinaturas do Azure, 8 Recursos avaliados, 9 Recomendações ativas, and 38 Alertas de segurança. Below these are four main cards:

- Postura de segurança:** Shows 9/9 Não atribuído and 0/0 Vencido. A pie chart indicates 55% CLASSIFICAÇÃO... with Azure at 55%, AWS at ~15%, and GCP at ~30%. A link to "Explore sua postura de segurança >" is provided.
- Conformidade regulatória:** Shows Azure Security Benchmark (28 de 43 controles passados), PCI DSS 3.2.1 (35/43), and SOC TSP (12/13). It also lists "Padrões normativos de conformidade mais baixos por controles passados". A link to "Melhorar a conformidade >" is provided.
- Proteções da carga de trabalho:** Shows 100% Cobertura de recursos and Alerts por severidade (High: 4, Medium: 13, Low: 25).
- Gerenciador de Firewall:** Shows a diagram of a firewall icon. It includes the text "Proteger sua rede com o Gerenciador de firewall" and "Um serviço de gerenciamento de segurança de rede central para configurar e gerenciar políticas de Firewall em assinaturas e locatários".

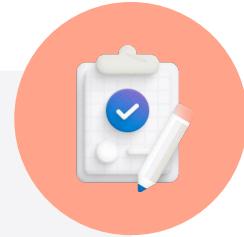
On the right side, there are two sections:

- Atualizar para o plano Novos Contêineres:** Describes the native cloud security for Kubernetes resources, including environmental protection, vulnerability assessment, and runtime threat protection. It mentions the "novo plano" which combines existing plans with new and improved features. A link to "Clique aqui para atualizar >" is provided.
- Pasta de trabalho de estimativa de custo para o plano do contêiner:** Provides an estimate of cost for the container plan based on AKS and connected Kubernetes clusters via Azure Arc. It includes links to "Exibir no repositório GitHub >" and "Implantação de modelo de ARM >".

At the bottom, there is a section titled "Recomendações mais predominantes (por recursos)" with the following items:

- 2 O acesso público da conta de armazenamento não deve ser perm...
- 2 A conta de armazenamento deve usar uma conexão de link privado...
- 1 As recomendações da proteção de rede adaptável devem ser apli...
- 1 As portas de gerenciamento devem ser fechadas nas máquinas vir...

Revisão do roteiro de aprendizagem 02



Módulos do Microsoft Learn (learn.microsoft.com/training)

- Infraestrutura física e de gerenciamento do Microsoft Azure
- Serviços de computação e rede
- Serviços de armazenamento
- Identidade, acesso e segurança