

AZ-900 Guia de Estudo

Describe cloud concepts (25–30%):

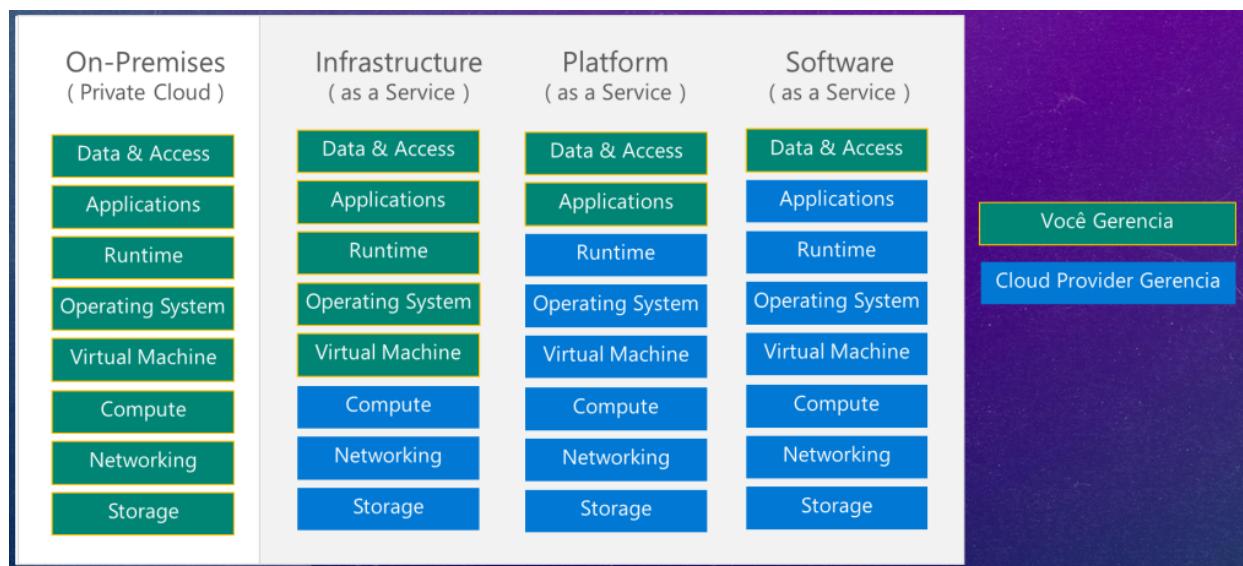
Describe cloud computing

Define cloud computing: Cloud computing engloba um conjunto de serviços e recursos computacionais que são oferecidos ao usuário através de um provedor de nuvem. Esse provedor de nuvem é responsável por armazenar toda a estrutura física que hospeda os serviços e recursos utilizados pelo usuário (datacenters, rede física, etc). Ao utilizar recursos e serviços oferecidos pelos provedores de nuvem, o uso de servidores físicos torna-se indispensável por parte do cliente, gerando uma série de benefícios em termos financeiros e operacionais.

Dependendo do serviço/recurso utilizado, o cliente pode optar em continuar utilizando sua estrutura física junto aos provedores de nuvem.

Describe the shared responsibility model: O modelo de responsabilidade compartilhada é a forma como a Microsoft define e organiza as políticas que ditam a maneira como o cliente e a Azure se relacionam em termos de responsabilidade sobre determinadas partes dos serviços e recursos consumidos e hospedados no provedor de nuvem

O modelo de responsabilidade compartilhada se relaciona diretamente com os tipos de serviços oferecidos pela Azure, sendo eles: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS).



Define cloud models, including public, private, and hybrid: 1) Nuvem pública: a nuvem oferece serviços e recursos que ficam hospedados no mesmo hardware físico, ou seja, oferece recursos compartilhados para os seus diferentes clientes. É acessada via conexão de rede segura (internet). 2) Nuvem privada: Pertencente e operado pela organização que utiliza os recursos da nuvem. As organizações criam um ambiente de nuvem em seu datacenter (on-premise or hosting providers). Precisa ter capacidade de bilhetagem e autoatendimento. 3) Nuvem Híbrida: Combina nuvens públicas e privadas

para permitir que os aplicativos sejam executados no local mais apropriado. [O que é Nuvem Privada – definição | Microsoft Azure](#).

Public Cloud
<ul style="list-style-type: none">• Owned and operated by a third party• Offers computing services including servers and storage• Resources are securely shared between customers• Accessed over the Internet
Private Cloud
<ul style="list-style-type: none">• Cloud dedicated to a single organization• On-premises or hosting providers datacenter• Services and infrastructure on a private network
Hybrid Cloud
<ul style="list-style-type: none">• Combination of public and private clouds• Expands options and flexibility by moving between public and private environments

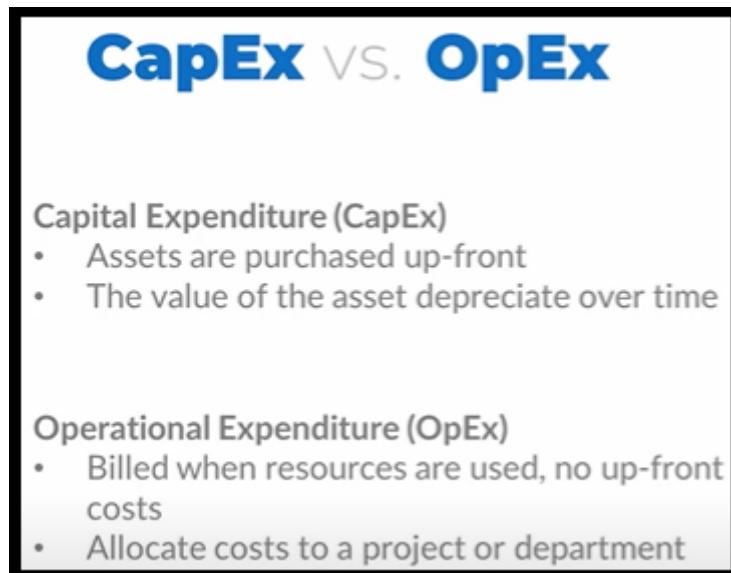
Identify appropriate use cases for each cloud model: Muitas organizações usam nuvens públicas, que fornecem benefícios como alta disponibilidade e capacidade de escalar para atender à demanda elástica, mas, para alguns casos de uso, as nuvens privadas são uma opção melhor: hardware especial ou requisitos de configuração; governança ou requisitos regulatórios, latência de rede, custo. Casos de uso nuvem híbrida: cargas de trabalho não testadas, cloud bursting (black friday), alta disponibilidade e recuperação de desastres, requisitos regulatórios (partes de aplicações permitidas a rodar na nuvem), corretagem de serviços em nuvem (autoatendimento/bilhetagem). [Casos de Uso](#)

Public Cloud
<ul style="list-style-type: none">• Businesses that don't want to manage data centers• Organizations that require scalability and a globally distributed network• Organizations that require details cost accounting for projects or departments
Private Cloud
<ul style="list-style-type: none">• Regulations prevent a move to the public cloud• Physically isolated locations• Large on-premises investment
Hybrid Cloud
<ul style="list-style-type: none">• Combination of public and private clouds• Hybrid can be a transition or end-state• Expands options and flexibility by moving between public and private environments

Describe the consumption-based model: O modelo baseado em consumo (ou pague conforme o uso / pay-as-you-go) é a forma como a Microsoft organiza a cobrança acerca do uso de recursos e serviços oferecidos e hospedados no seu provedor de nuvem. No Azure, você só paga pelos serviços que utilizar, não sendo necessário nenhum investimento inicial (Opex), e podendo os serviços e recursos serem

desativados após o uso ou durante um período de inatividade, o que proporciona ao cliente maior eficiência e economia em seus gastos (Melhor previsão de custos; São fornecidos os preços para serviços e recursos individuais; A cobrança é baseada no uso real)

Compare cloud pricing models: Fixed Price (preço fixo) – compra e implementação de recursos baseado em um pico de demanda (necessidade momentânea de aumento da infraestrutura – requer investimento inicial). Consumption-Based (modelo baseado em consumo – pay-as-you-go – pague apenas pelos recursos que usar. Não gera necessidade de investimento inicial). CapEx vs OpEx:



Describe the benefits of using cloud services:

Describe the benefits of high availability and scalability in the cloud: O benefício de alta disponibilidade da cloud garante aos clientes que suas aplicações estejam disponíveis pelo máximo de tempo possível, protegidas contra intermitências e falhas. O benefício da alta disponibilidade por si só não garante que a aplicação do cliente esteja disponível por todo o tempo, porém o Azure oferece recursos para que seus administradores consigam planejar uma arquitetura em que o SLA da sua aplicação chegue a 99.9%, através de estratégias como availability set, availability zone e disaster recovery. Já o benefício da escalabilidade garante que a aplicação do cliente seja escalada de acordo com a necessidade. Muitas vezes em ambientes on-premises, quando há um aumento pontual da demanda, as empresas fazem grandes investimentos em hardware físico e infraestrutura. Acontece que muitas vezes esse aumento de demanda tende a cair tempo depois, fazendo com que se torne desnecessário o uso dos equipamentos recém adquiridos, tornando assim o investimento ineficiente. Em um provedor de nuvem, é possível que você aumente sua capacidade computacional para atender um pico de demanda pontual (ex: blackfriday), sem ter gasto com CapEx. Após passar esse pico de demanda, você pode retornar ao uso padrão dos recursos computacionais, economizando assim muitos recursos. Em suma, o benefício da escalabilidade garante que a aplicação seja escalável de acordo com a demanda do momento, sendo permitido a ampliação e redução de recursos de forma inteligente.

Describe the benefits of reliability and predictability in the cloud: o benefício da confiabilidade garante que as aplicações hospedadas no Azure possam cumprir os compromissos assumidos com o

cliente. “Devido ao design descentralizado, a nuvem naturalmente dá suporte a uma infraestrutura confiável e resiliente”. Resiliência é a capacidade que um sistema tem de se recuperar de falhas e continuar funcionando. Ela também é um dos pilares do Microsoft Azure Well-Architected Framework. Com um design descentralizado, a nuvem permite que você tenha recursos implantados em várias regiões do mundo. Com essa escala global, mesmo que ocorra um evento catastrófico em uma região, as outras regiões ainda estarão em funcionamento, garantindo a confiabilidade da aplicação junto ao cliente. Já o benefício da previsibilidade permite que você avance em sua aplicação com confiança. A previsibilidade pode se concentrar na previsibilidade de desempenho ou na previsibilidade de custo. Tanto a previsibilidade de desempenho quanto a de custo são bastante influenciadas pelo Microsoft Azure Well-Architected Framework. Ao implantar uma solução criada com base nessa estrutura, você tem uma solução com custo e desempenho previsíveis.

Describe the benefits of security and governance in the cloud: O benefício da segurança garante que você encontre no provedor de nuvem uma alternativa de serviços e recursos que atendam às suas necessidades de segurança. Se você quiser o controle máximo da segurança, a infraestrutura como serviço fornecerá recursos físicos, mas permitirá e exigirá (conforme as novas necessidades de segurança) que você gerencie os sistemas operacionais e o software instalado, incluindo aplicação de patches e manutenção. Se você quiser que a aplicação de patches e a manutenção sejam tratadas automaticamente, as implantações de plataforma como serviço ou software como serviço podem ser as melhores estratégias de nuvem para você. Já o benefício da governança assegura a conformidade da sua aplicação, garantindo que todos os seus recursos implantados atendam aos padrões corporativos e aos requisitos regulatórios governamentais. Além disso, você pode atualizar todos os seus recursos implantados com novos padrões à medida que os padrões são alterados. A auditoria baseada em nuvem ajuda a sinalizar qualquer recurso que esteja fora de conformidade com seus padrões corporativos e fornece estratégias de mitigação.

Describe the benefits of manageability in the cloud: Há dois tipos de capacidade de gerenciamento para computação em nuvem – 1) Gerenciamento da nuvem, que diz respeito a gerenciar seus recursos de nuvem, onde você pode – Escalar automaticamente a implantação de recursos com base na necessidade. Implantar recursos com base em um modelo pré-configurado, removendo a necessidade de configuração manual. Monitorar a integridade dos recursos e substituir automaticamente os recursos com falha. Receber alertas automáticos com base em métricas configuradas, de modo a ficar ciente do desempenho em tempo real. 2) Gerenciamento na nuvem, que diz respeito à maneira de gerenciar seu ambiente de nuvem e seus recursos. Você pode gerenciá-los por meio de – Um portal da Web. Usando uma interface de linha de comando. Usando APIs. Usando o PowerShell.

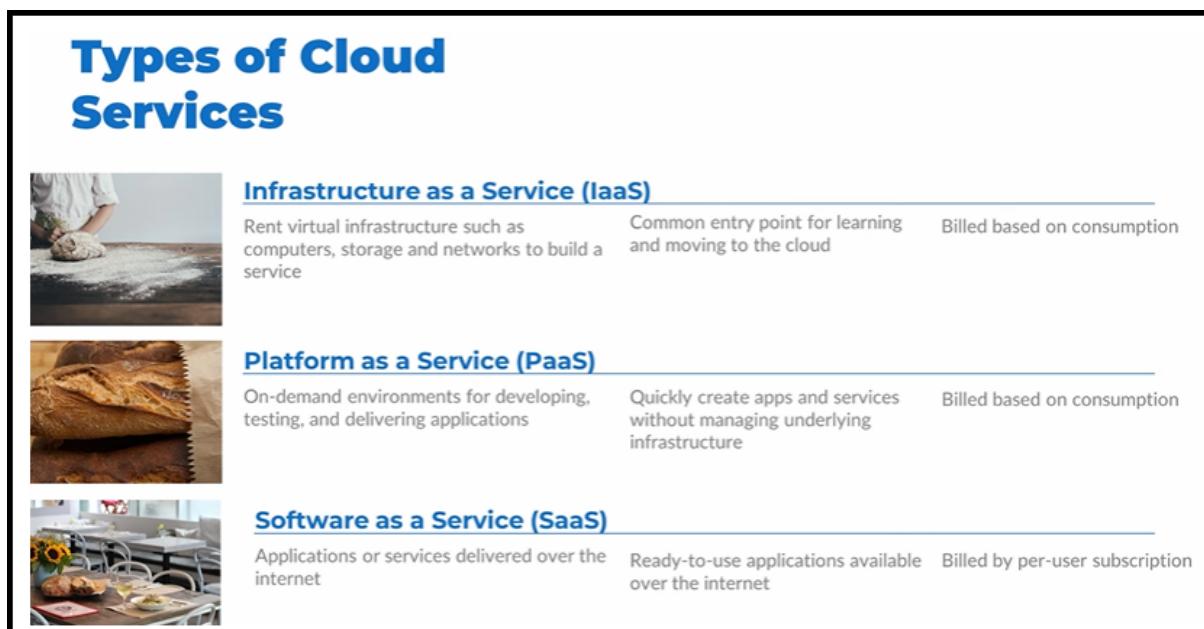
Describe cloud service types

Describe infrastructure as a service (IaaS): infraestrutura como serviço é o “nível mais baixo” de tipo de serviço oferecido pelos provedores de nuvem. Nesse modelo, a camada de responsabilidade do cliente é maior, sendo que o provedor de nuvem apenas fica responsável pela parte de hardware, redes e armazenamento (que são gerenciadas pelo provedor em todos os tipos de serviços). A parte de configurações da VMs, bem como do sistema operacional (além das outras partes que também são gerenciadas em PaaS e SaaS) ficam a cargo do cliente.

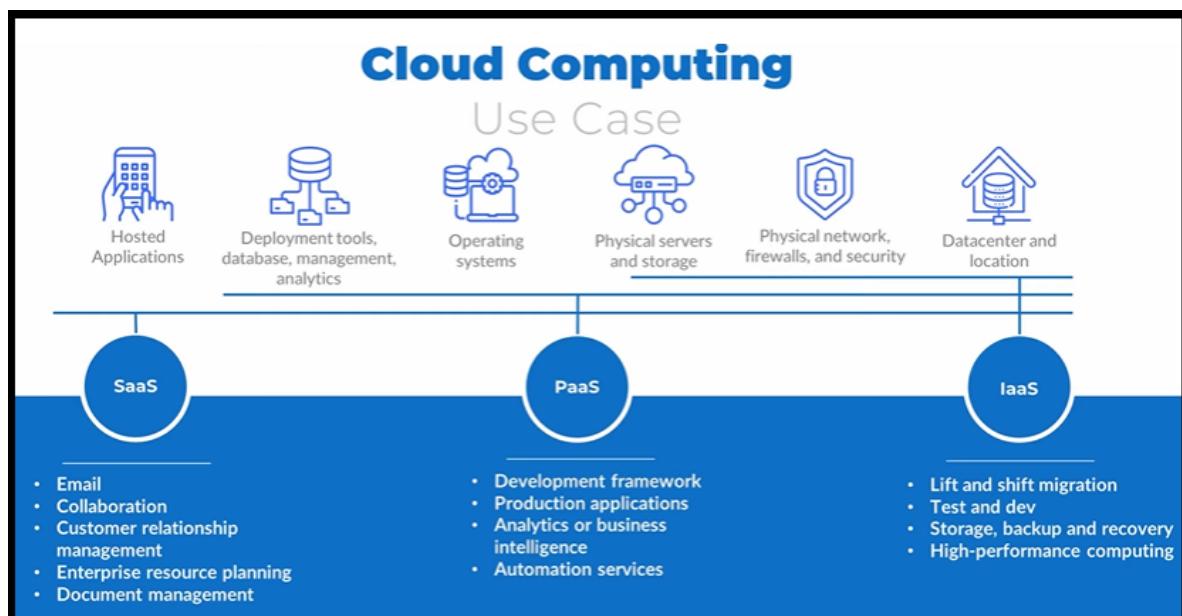
Describe platform as a service (PaaS): plataforma como serviço oferece ao cliente um ambiente para desenvolver e administrar sua aplicação. Nesse modelo, a responsabilidade sobre a camada de

infraestrutura (incluindo as configurações das VMs e sistema operacional) fica a cargo do provedor de nuvem, sendo que a camada de aplicação e de dados e acessos ficam a cargo do cliente.

Describe software as a service (SaaS): software como serviço é o modelo de “mais alto nível”, onde o provedor de nuvem entrega um conjunto de recursos e serviços que constituem um software pronto para o uso do consumidor final (Office 365, por exemplo). Nesse modelo, o cliente apenas fica responsável pelo gerenciamento dos dados e dos acessos dos usuários à aplicação, sendo todas as outras camadas de responsabilidade do provedor de nuvem. Por ser um conjunto de serviços que constituem um software a ser utilizado pelo usuário final, oferece um nível menor de customização a nível de aplicação e infraestrutura. Em compensação, a parte do gerenciamento técnico fica muito mais enxuta.



Identify appropriate use cases for each cloud service (IaaS, PaaS, SaaS):



Describe Azure architecture and services (35-40%):

Describe the core architectural components of Azure

Describe Azure regions, region pairs, and sovereign regions: as regiões do Azure podem ser definidas como um local onde ficam alocados os datacenters físicos do provedor de nuvem. O cliente escolhe em qual região quer hospedar seus serviços e recursos; Cada região tem um custo específico; Quanto mais distante a região tiver do usuário, maior será a latência da aplicação; Conformidade: a Azure possui conformidade com os padrões legais e regulatórios das regiões que hospedam seus datacenters. Instituições de determinada natureza (ex: financeira) possuem padrões específicos e não podem ser hospedadas em uma região diferente da sua de origem, por exemplo; Regiões pares: conjunto de duas regiões que fornece alguns mecanismos para a segurança da aplicação. Como replicação automática para alguns serviços, priorização de recuperação em caso de paralisações e atualização sequencial para minimizar o tempo de inatividade do serviço – Nuvem soberana: As nuvens soberanas do Azure são plataformas isoladas no país com requisitos independentes de autenticação, armazenamento e conformidade. Nuvens soberanas são normalmente usadas dentro dos limites geográficos em que há um requisito estrito de residência de dados.

Describe availability zones: Availability zone é uma estratégia para garantir a disponibilidade/confiabilidade da aplicação. Esse modelo oferece proteção contra falhas de datacenters inteiros. Se a aplicação do usuário estiver alocada em duas ou mais máquinas virtuais e um availability zones for configurado, as máquinas serão alocadas em datacenters (zonas) diferentes. Esse arranjo oferece um SLA de 99.99%. OBS: Geralmente cada região do Azure possui 3 zonas (datacenters) diferentes. ZONA = DATACENTER — racks físicos < zonas (datacenters) < regiões.

Describe Azure datacenters: Os datacenters do Azure são edifícios físicos exclusivos, localizados em todo o mundo, que abrigam um grupo de servidores de computadores em rede. Uma região do Azure é um conjunto de datacenters implantados em um perímetro definido por latência e conectados por meio de uma rede regional dedicada de baixa latência.

Describe Azure resources and resource groups: os grupos de recursos são um agrupamento de recursos utilizados pelo usuário a fim de organizá-los da melhor forma para si. Sua finalidade é mais voltada a fins de organização. Pode ser entendido como um contêiner para gerenciar e agregar recursos em uma única unidade. Já os recursos são os blocos de construção básicos do Azure. Qualquer coisa que o cliente for criar, provisionar, implantar, etc. é um recurso (ex: VMs, VNETs, Storages, etc.).

- Os recursos podem existir em apenas um grupo de recursos. Os recursos podem existir em diferentes regiões. Os recursos podem ser transferidos para diferentes grupos de recursos. Os aplicativos podem utilizar vários grupos de recursos. Os grupos de recursos não podem ser aninhados. Como são organizados os resource groups? Depende, pode ser por ambiente (HML, PRD), por recurso (um só para VM, storage, etc.), por projeto, etc. Ou seja, forma que melhor atenda a estrutura desejada pelo cliente.

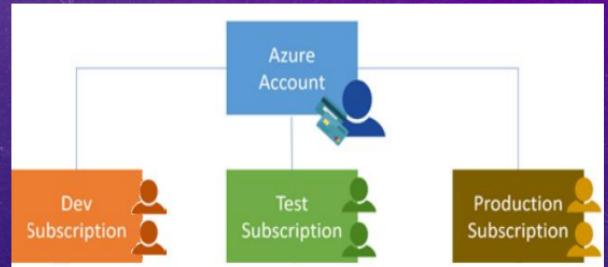


Describe subscriptions: No Azure, as assinaturas são uma unidade de gerenciamento, cobrança e escala. Semelhante a como os grupos de recursos são um modo de organizar logicamente os recursos, as assinaturas permitem organizar logicamente seus grupos de recursos e facilitar a cobrança. Uma assinatura do Azure se vincula a uma conta do Azure. Uma conta pode ter várias assinaturas, mas só é necessário ter uma. Em uma conta com várias assinaturas, você pode usar as assinaturas para configurar diferentes modelos de cobrança e aplicar diferentes políticas de gerenciamento de acesso (definindo limites em relação a produtos, serviços e recursos do Azure). Assinaturas adicionais Azure: Semelhante ao uso de grupos de recursos para separar recursos por função ou acesso, talvez você queira criar assinaturas adicionais para gerenciamento de recursos ou cobrança. Por exemplo, é possível criar assinaturas adicionais para separar ambientes, estruturas organizacionais e cobrança. Tipos de subscriptions – Trial; Estudante, Pay-as-a-go, Enterprise Agreement (grandes empresas).

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

Límite de faturamento: gerar relatórios de faturamento separados e faturas para cada assinatura.

Límite de controle de acesso: gerenciar e controlar o acesso aos recursos que os usuários podem prover com assinaturas específicas.



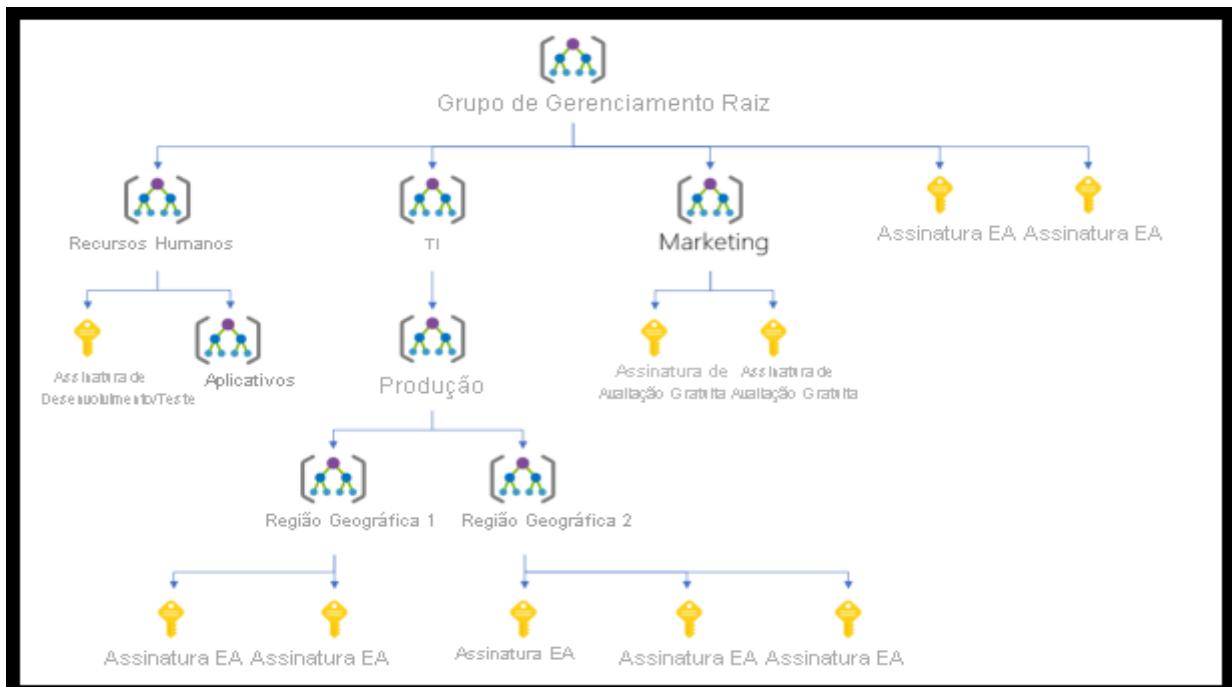
Describe management groups: Os recursos são reunidos em grupos de recursos e os grupos de recursos são reunidos em assinaturas. Os grupos de gerenciamento do Azure fornecem um nível de escopo acima das assinaturas. Você organiza as assinaturas em contêineres chamados grupos de gerenciamento e aplica as condições de governança a esses grupos. Todas as assinaturas em um grupo de gerenciamento herdam automaticamente as condições aplicadas ao grupo de gerenciamento. Os grupos de gerenciamento fornecem gerenciamento corporativo em larga escala, independentemente do tipo de assinaturas que você possa ter. Grupos de gerenciamento podem ser aninhados.

Fatos importantes sobre os grupos de gerenciamento:

- 10.000 grupos de gerenciamento podem ter suporte em um único diretório.
- Uma árvore do grupo de gerenciamento pode dar suporte a até seis níveis de profundidade. Esse limite não inclui o nível raiz nem o nível da assinatura.
- Cada grupo de gerenciamento e assinatura podem dar suporte a somente um pai.

Describe the hierarchy of resource groups, subscriptions, and management groups: recursos < grupo de recursos (resource group) < assinaturas < grupos de gerenciamento (management groups). Os recursos são reunidos em grupos de recursos e os grupos de recursos são reunidos em assinaturas. Os grupos de gerenciamento do Azure fornecem um nível de escopo acima das assinaturas. Você organiza as assinaturas em contêineres chamados grupos de gerenciamento e aplica as condições de governança a esses grupos. Todas as assinaturas em um grupo de gerenciamento herdam automaticamente as condições aplicadas ao grupo de gerenciamento, da mesma forma que os grupos de recursos herdam configurações de assinaturas e os recursos herdam dos grupos de recursos. Os grupos de gerenciamento fornecem

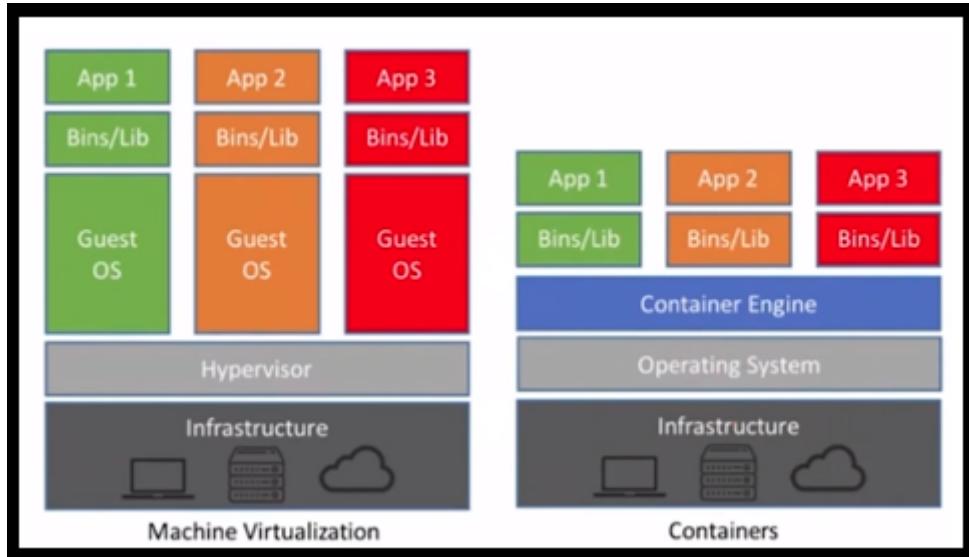
gerenciamento corporativo em larga escala, independentemente do tipo de assinaturas que você possa ter. Grupos de gerenciamento podem ser aninhados.



Describe Azure compute and networking services

Compare compute types, including container instances, virtual machines (VMs), and functions: A principal diferença entre as VMs e contêineres é o ponto onde o nível de virtualização acontece. Enquanto as VMs se caracterizam por ter sua virtualização a nível de hardware, os contêineres têm sua virtualização a nível de sistema operacional. As máquinas virtuais são isoladas a nível de máquina, elas utilizam sistemas operacionais diferentes, ou seja, são independentes umas das outras. Elas podem estar compartilhando o mesmo hardware físico a nível de servidor, porém são virtualizadas de maneira independentes. Já os contêineres são isolados “a nível de processo”. Eles compartilham o mesmo hardware físico e também o mesmo sistema operacional (kernel), e diferente de um computador/SO comum, onde os aplicativos são rodados em um mesmo ambiente (compartilhando os mesmos recursos e podendo interagir entre si), os containers fornecem uma camada de isolamento que fornece um ambiente isolado para os aplicativos (ou partes distintas de um aplicativo) serem rodados. Nesse contexto, os containers permitem que os aplicativos vejam somente o que é necessário para serem rodados, e nada mais. Para os aplicativos, é como se o contêiner fosse um sistema operacional próprio que oferece somente os recursos necessários para aquela aplicação (ou parte de aplicação) rodar, não permitindo que ela interaja com as demais aplicações ou partes de aplicação (que estão alocadas em outros containers). Por conta de sua arquitetura, os containers constituem-se como uma alternativa mais leve e flexível para diversos casos de uso, como aplicações que possuem sua arquitetura baseada em microserviços.

➡️ Containers vs VMs: What's the difference? - VMs (IaaS), Containers (PaaS).

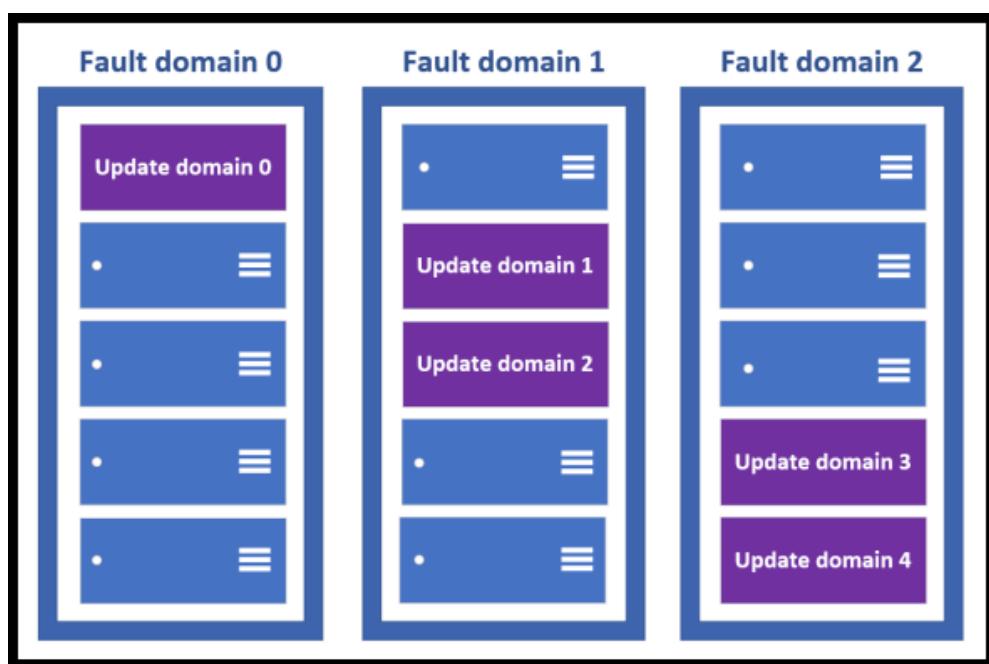


O Azure Functions, por sua vez, é uma opção de computação sem servidor controlada por eventos que não requer a manutenção de máquinas virtuais ou contêineres. Se você criar um aplicativo usando VMs ou contêineres, esses recursos precisarão estar "em execução" para que seu aplicativo funcione. Com o Azure 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. As funções são dimensionadas automaticamente com base na demanda, portanto, podem ser uma boa opção quando a demanda é variável. O Azure Functions executa o código quando este é disparado e desaloca os recursos automaticamente quando a função é concluída. Neste modelo, você só é cobrado pelo tempo de CPU usado durante a execução da função. As funções podem ser sem estado ou com estado. Quando são sem estado (o padrão), elas se comportam como se fossem reiniciadas sempre que respondem a um evento. Quando são com estado (chamadas de Durable Functions), um contexto é passado pela função para acompanhar a atividade anterior.

Describe VM options, including Azure Virtual Machines, Azure Virtual Machine Scale Sets, availability sets, and Azure Virtual Desktop:

- VMs: Com as VMs (Máquinas Virtuais) do Azure, você pode 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. 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. Uma VM do Azure oferece a flexibilidade da virtualização sem a necessidade de comprar e manter o hardware físico que a executa. No entanto, como uma oferta de IaaS, você ainda precisa configurar, atualizar e manter o software executado na VM. Você pode até mesmo criar ou usar uma imagem já criada para provisionar rapidamente VMs. Você pode criar e provisionar uma VM em minutos quando seleciona uma imagem de VM pré-configurada.

- Dimensionar VMs no Azure: Você pode executar VMs únicas para teste, desenvolvimento ou para tarefas secundárias. Ou pode agrupar VMs para fornecer alta disponibilidade, escalabilidade e redundância. O Azure também pode gerenciar o agrupamento de VMs para você com recursos como conjuntos de dimensionamento (sizing set) e conjuntos de disponibilidade (availability set).
- Conjuntos de dimensionamento (Virtual Machine Scale sets): Os conjuntos de dimensionamento permitem que você gerencie, configure e atualize centralmente um grande número de VMs em minutos. O número de instâncias de VM pode aumentar ou diminuir automaticamente em resposta à demanda ou você pode defini-lo para uma escala com base em uma agenda definida. Os conjuntos de dimensionamento de máquinas virtuais também implantam automaticamente um平衡ador de carga para garantir que seus recursos estejam sendo usados com eficiência. Com conjuntos de dimensionamento de máquinas virtuais, você pode criar serviços em grande escala para áreas como computação, big data e cargas de trabalho de contêiner.
- Conjuntos de disponibilidade (Availability Set): Os conjuntos de disponibilidade de máquinas virtuais são outra ferramenta para ajudá-lo a criar um ambiente mais resiliente e altamente disponível. Os conjuntos de disponibilidade foram projetados para garantir que as VMs escalam atualizações e tenham conectividade de rede e energia variadas, impedindo que você perca todas as suas VMs com uma só falha de rede ou energia. Os conjuntos de disponibilidade fazem isso agrupando VMs de duas maneiras: domínio de atualização – a configuração de grupos de domínio de atualização permite que você aplique atualizações sabendo que apenas um agrupamento de domínio de atualização estará offline por vez. Um grupo de atualizações que passa pelo processo de atualização recebe um tempo de 30 minutos para se recuperar antes que a manutenção no próximo domínio de atualização seja iniciada. E domínio de falha – o domínio de falha agrupa suas VMs por origem de energia comum e comutador de rede. Por padrão, um conjunto de disponibilidade dividirá suas VMs em até três domínios de falha. Isso ajuda a proteger contra uma falha de energia física ou de rede, tendo VMs em diferentes domínios de falha (portanto, sendo conectadas a diferentes recursos de energia e rede). Não há nenhum custo adicional para configurar um conjunto de disponibilidade. Você paga apenas pelas instâncias de VM criadas.



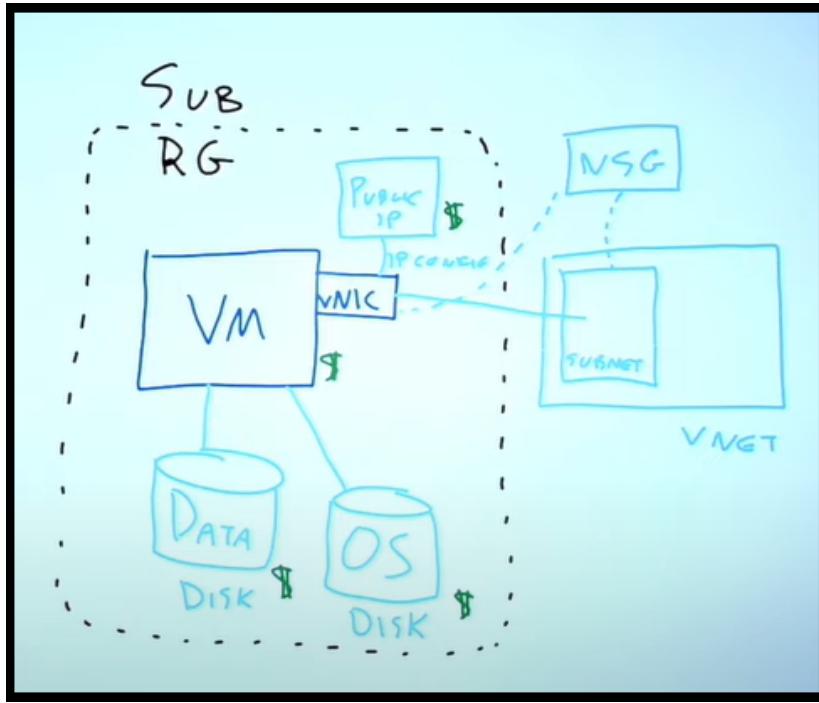
- Exemplos de quando usar VMs: Durante o teste e o desenvolvimento, ao executar aplicativos na nuvem, ao estender seu datacenter para a nuvem, durante a recuperação de desastres.
- Migrar para a nuvem com VMs: As VMs também são uma excelente opção quando você migra de um servidor físico para a nuvem (também conhecido como lift-and-shift). Você pode criar uma imagem do servidor físico e hospedá-la em uma VM com poucas ou nenhuma alteração. Assim como um servidor local físico, você deve manter a VM: você é responsável por manter o sistema operacional e o software instalado
- Azure Virtual Desktop (Área de Trabalho Virtual do Azure): Outro tipo de máquina virtual é a Área de Trabalho Virtual do Azure. A Área de Trabalho Virtual do Azure é um serviço de virtualização de área de trabalho e aplicativos que é executado na nuvem. Ele permite que você use 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 oferece gerenciamento de segurança centralizado para as áreas de trabalho dos usuários com o Azure AD (Azure Active Directory). Você pode habilitar a autenticação multifator para proteger as entradas do usuário. Você também pode proteger o acesso aos dados atribuindo RBACs (controles de acesso baseados em função) granulares aos usuários. Com a Área de Trabalho Virtual do Azure, os dados e aplicativos ficam separados do hardware local. A área de trabalho e os aplicativos reais estão em execução na nuvem, o que significa que o risco de dados confidenciais serem deixados em um dispositivo pessoal é reduzido. Além disso, as sessões de usuário são isoladas em ambientes de sessão única e de várias sessões. A Área de Trabalho Virtual do Azure permite que você use a multisessão do Windows 10 ou Windows 11 Enterprise, o único sistema operacional baseado em cliente Windows que habilita vários usuários simultâneos em uma VM. A Área de Trabalho Virtual do Azure também fornece uma experiência mais consistente com suporte a aplicativos mais amplo em comparação com sistemas operacionais baseados no Windows Server.

Describe resources required for virtual machines: Ao provisionar uma Máquina Virtual, você também terá a oportunidade de escolher os recursos associados a essa VM, incluindo os listados abaixo:

- Tamanho (finalidade, número de núcleos de processador e quantidade de RAM)
- Discos de armazenamento (unidades de disco rígido, unidades de estado sólido etc.)
- Rede (rede virtual, endereço IP público e configuração de porta)

Além disso, a VM criada (assim como todos os recursos do Azure) devem estar vinculadas a uma assinatura e a um grupo de recursos. Outros recursos vinculados e necessários para a criação de VMs são o “OS Disk” (disco de sistema) e o Data Disk (disco de dados), além do NIC (placa de rede - IP público e privado), e a VNET, a(s) subnet(s) e seu filtro de pacotes (NSG) aos quais a VM se comunicará.

 [Describe the Resources Required for Virtual Machines - AZ-900 Certification Course - May 2022 New](#)



Describe application hosting options, including the Web Apps feature of Azure App Service, containers, and virtual machines: Se você precisar hospedar seu aplicativo no Azure, poderá inicialmente recorrer a uma VM (máquina virtual) ou contêineres. Tanto VMs quanto contêineres fornecem excelentes soluções de hospedagem. As VMs oferecem o controle máximo do ambiente de hospedagem e permitem que você configure exatamente como deseja. As VMs também poderão ser o método de hospedagem mais familiar se você for novo na nuvem. Os contêineres, com a capacidade de isolar e gerenciar individualmente diferentes aspectos da solução de hospedagem, também podem ser uma opção robusta e atraente. Há outras opções de hospedagem que você pode usar com o Azure, incluindo o Serviço de Aplicativo do Azure, que 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, permitindo implantações automatizadas do GitHub, Azure DevOps ou qualquer repositório Git para dar suporte a um modelo de implantação contínua. O Serviço de Aplicativo do Azure é um serviço com base em HTTP para hospedagem de aplicativos Web, APIs REST e back-ends móveis. Ele dá suporte a várias linguagens, incluindo .NET, .NET Core, Java, Ruby, Node.js, PHP ou Python. Ele também dá suporte a ambientes Windows e Linux. Com o Serviço de Aplicativo, você pode hospedar os estilos mais comuns de serviço de aplicativos, 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: A implantação e o gerenciamento são integrados à plataforma; Endpoints podem ser protegidos; Sites podem ser dimensionados rapidamente para lidar com cargas de alto tráfego; O balanceamento de carga interno e o gerenciador de tráfego fornecem alta disponibilidade. Todos esses estilos de aplicativos são hospedados na mesma infraestrutura e compartilham esses benefícios. Essa flexibilidade torna o Serviço de Aplicativo a escolha ideal para hospedar aplicativos voltados para a Web.

Describe virtual networking, including the purpose of Azure Virtual Networks, Azure virtual subnets, peering, Azure DNS, Azure VPN Gateway, and Azure ExpressRoute:



O Azure Virtual Network (**VNet**) permite que os recursos do Azure se comuniquem entre si, com a internet e as redes locais.

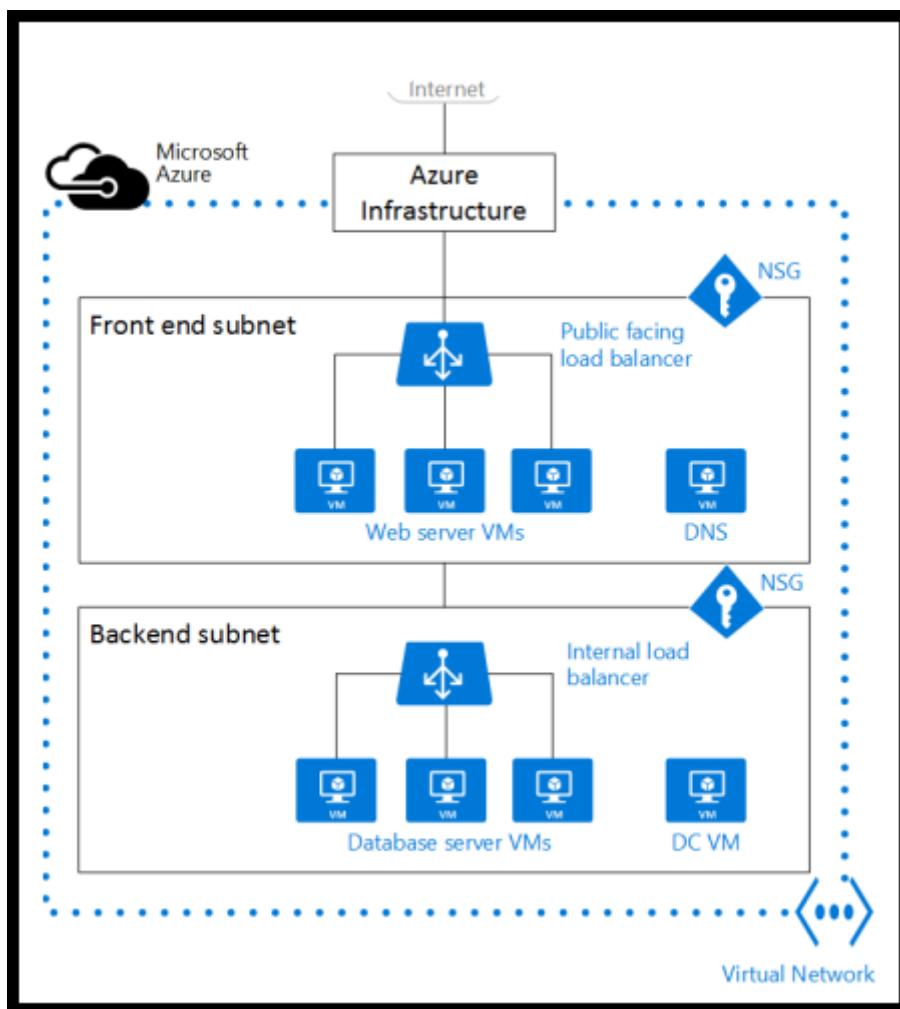


O **Virtual Private Network Gateway (VPN)** é usado para enviar tráfego criptografado entre uma rede virtual do Azure e um local no local pela internet pública.



O **Azure Express Route** estende redes no local para o Azure por uma conexão privada que é facilitada por um provedor de conectividade.

- Redes Virtuais (VNETs) e Subnets (subredes): 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 de rede essenciais: Isolamento e segmentação – A rede virtual do Azure permite criar várias redes virtuais isoladas. Quando você

configura uma rede virtual, define um espaço de endereço IP privado usando intervalos de endereços IP públicos ou privados. O intervalo de IP existe somente na rede virtual e não é roteável pela Internet. Você pode dividir esse espaço de endereços IP em sub-redes e alocar parte do espaço de endereço definido para cada sub-rede nomeada. Para a resolução de nomes, é possível usar o serviço de resolução de nomes interno do Azure. Você também pode configurar a rede virtual para usar um servidor DNS interno ou externo.

Comunicação com a Internet – É possível habilitar conexões de entrada da Internet atribuindo um endereço IP público a um recurso do Azure ou colocar o recurso atrás de um balanceador de carga público.

Comunicação entre recursos do Azure – Convém habilitar recursos do Azure para que se comuniquem entre si com segurança. Você pode fazer isso de duas maneiras:

- As redes virtuais podem conectar não apenas VMs, mas outros recursos do Azure, como Ambiente do Serviço de Aplicativo para Power Apps, Serviço de Kubernetes do Azure e os conjuntos de dimensionamento de máquinas virtuais do Azure.
- Os endpoints podem se conectar a outros tipos de recursos do Azure, como bancos de dados SQL do Azure e contas de armazenamento.

Essa abordagem permite vincular vários recursos do Azure às redes virtuais para melhorar a segurança e fornecer o encaminhamento ideal entre recursos.

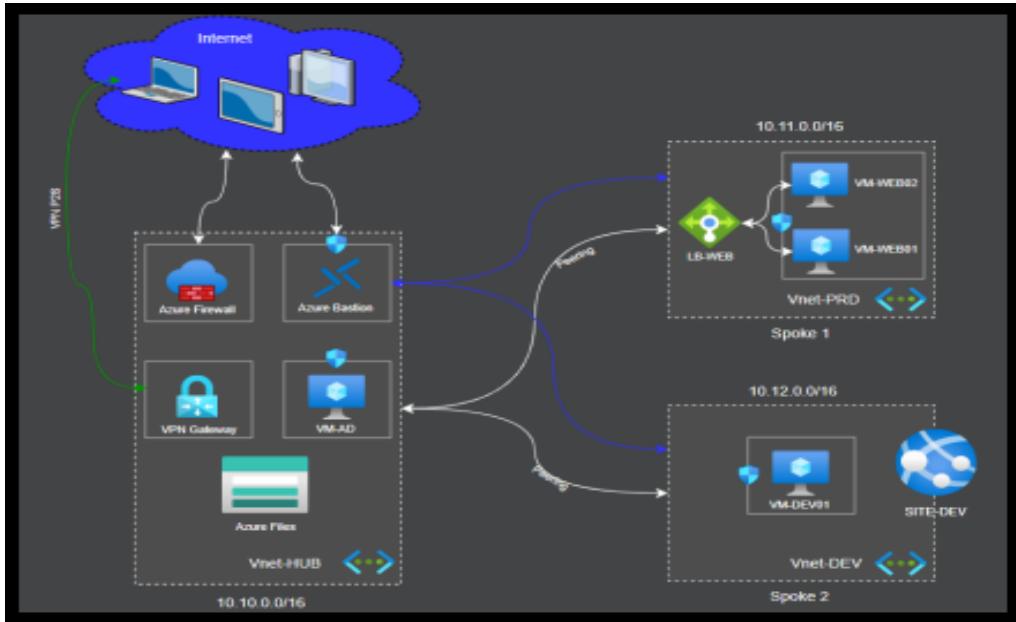
Comunicação com os recursos locais – As redes virtuais do Azure permitem vincular recursos em seu ambiente local e na assinatura do Azure. Na verdade, você pode criar uma rede que abranja os ambientes locais e de nuvem. Há três mecanismos para você obter essa conectividade:

- VPN point to site (PS2) - quando um computador cliente quer se conectar a uma rede virtual do Azure (conexões remotas de teletrabalho);
- VPN site-to-site, conectando a rede virtual do Azure a uma rede local (ambiente on-premises) ;
- Azure ExpressRoute: fornece uma conectividade privada dedicada para o Azure que não passa pela Internet. O ExpressRoute é útil para ambientes em que você precisa de maior largura de banda e níveis de segurança ainda mais altos.

Rotear tráfego de rede: Por padrão, o Azure faz o roteamento de tráfego entre sub-redes em redes virtuais conectadas, em redes locais e na Internet. Você também pode controlar o roteamento e substituir essas configurações criando tabelas de rotas personalizadas e controlando como os pacotes são encaminhados entre as subredes e através do BGP (Border Gateway Protocol).

Filtrar tráfego de rede: As redes virtuais do Azure permitem filtrar o tráfego entre sub-redes usando grupos de segurança de rede e soluções de virtualização de rede.

- Conectar redes virtuais (Peering): Você pode vincular redes virtuais usando o emparelhamento dessas redes. O emparelhamento permite que duas redes virtuais se conectem diretamente entre si. O tráfego de rede entre redes emparelhadas é privado e viaja na rede de backbone da Microsoft, nunca entrando na Internet pública. O emparelhamento permite que os recursos em cada rede virtual se comuniquem entre si. Essas redes virtuais podem estar em regiões separadas, o que permite criar uma rede global interconectada por meio do Azure. As UDR (rotas definidas pelo usuário) permitem controlar as tabelas de roteamento entre sub-redes em uma rede virtual ou entre redes virtuais. Isso permite maior controle sobre o fluxo de tráfego de rede.



- VPNs do Azure (Redes Virtuais Privadas): Uma VPN (rede virtual privada) usa um túnel criptografado dentro de outra rede. As VPNs costumam ser implantadas para conectar duas ou mais redes privadas confiáveis entre si em uma rede não confiável (normalmente a Internet pública). O tráfego é criptografado ao viajar pela rede não confiável para evitar interceptação ou outros ataques. As VPNs podem permitir que as redes compartilhem informações confidenciais de modo seguro e protegido.
- Gateways VPN: Um gateway de VPN é um tipo de gateway de rede virtual. As instâncias do Gateway de VPN do Azure são implantadas em uma subrede dedicada da rede virtual e permitem conectar datacenters locais a redes virtuais por meio de uma conexão site to site; conectar dispositivos individuais a redes virtuais por meio de uma conexão point to site, conectar redes virtuais a outras redes virtuais por meio de uma conexão rede a rede (network-to-network). Ao implantar um gateway de VPN, você especifica o tipo de VPN, que pode ser baseada em política ou em rota. A principal diferença entre esses dois tipos de VPN é como o tráfego a ser criptografado é especificado. No Azure, ambos os tipos de gateways de VPN usam uma chave pré-compartilhada como o único método de autenticação.
- Cenários de alta disponibilidade: Se você está configurando uma VPN para manter suas informações seguras, é importante ter certeza de que ela é uma configuração VPN altamente disponível e tolerante a falhas.
- Cenários de alta disponibilidade: Se você está configurando uma VPN para manter suas informações seguras, é importante ter certeza de que ela é uma configuração VPN altamente disponível e tolerante a falhas. Há alguns modos de maximizar a resiliência do gateway de VPN:

Ativo/em espera

Por padrão, gateways de VPN são implantados como duas instâncias em uma configuração ativa/em espera, mesmo se você vê apenas um recurso de gateway de VPN no Azure. Quando a manutenção planejada ou a interrupção não planejada afeta a instância ativa, a instância de modo de espera assume automaticamente a responsabilidade pelas conexões sem nenhuma intervenção do usuário. Durante esse failover, as conexões são interrompidas, mas normalmente são restauradas em alguns segundos para manutenção planejada e dentro de 90 segundos em caso de interrupções não planejadas.

Ativo/ativo

Com a introdução da compatibilidade com o protocolo de roteamento BGP, você também pode implantar os gateways de VPN em uma configuração ativo/ativo. Nessa configuração, você atribui um endereço IP público exclusivo a cada instância. Em seguida, cria túneis do dispositivo local para cada endereço IP. É possível estender a alta disponibilidade implantando um dispositivo VPN local adicional.

Failover do ExpressRoute

Outra opção de alta disponibilidade é configurar um gateway de VPN como um caminho de failover seguro para conexões ExpressRoute. Os circuitos ExpressRoute têm resiliência integrada. Porém, não são imunes a problemas físicos que afetam os cabos que fornecem conectividade nem a interrupções que afetam toda a localização do ExpressRoute. Em cenários de alta disponibilidade, nos quais há risco associado a uma interrupção de um circuito do ExpressRoute, você também pode provisionar um gateway de VPN que usa a Internet como um método alternativo de conectividade. Dessa forma, você pode garantir que sempre haja uma conexão com as redes virtuais.

Gateways com redundância de zona

Nas regiões que dão suporte a zonas de disponibilidade, os gateways de VPN e os gateways de ExpressRoute podem ser implantados em uma configuração com redundância de zona. Essa configuração oferece resiliência, escalabilidade e maior disponibilidade para os gateways de rede virtual. A implantação de gateways em zonas de disponibilidade do Azure separa de forma física e lógica os gateways em uma região, enquanto protege a conectividade de rede local com o Azure contra falhas no nível da zona. Esses gateways exigem SKUs de gateway diferentes e usam os endereços IP públicos Standard em vez dos Básicos.

- Azure ExpressRoute: O 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. Cada local teria o próprio circuito do ExpressRoute. A conectividade pode ocorrer de uma rede any-to-any (VPN de IP), uma rede Ethernet ponto a ponto ou uma conexão cruzada virtual por meio de um provedor de conectividade em uma colocação. As conexões do ExpressRoute não passam pela Internet pública. Isso permite que as conexões de ExpressRoute ofereçam mais confiabilidade, mais velocidade, latências consistentes e muito mais segurança do que as conexões típicas pela Internet. Recursos e benefícios do ExpressRoute: Conectividade com os serviços de nuvem da Microsoft em todas as regiões da região geopolítica; Conectividade global com os serviços da Microsoft em todas as regiões com o Alcance Global do ExpressRoute (MS 365, MS Dynamics 365, Serviços de Computação do Azure (como VMs), Serviços de nuvem do Azure, como o Azure Cosmos DB e o Armazenamento do Azure); Roteamento dinâmico entre sua rede e a Microsoft por meio do BGP (Border Gateway Protocol); Redundância interna em cada local de emparelhamento para proporcionar maior confiabilidade.

Modelos de conectividade do ExpressRoute

O ExpressRoute dá suporte a quatro modelos que podem ser usados para conectar a rede local à Microsoft Cloud:

- Colocação do CloudExchange
- Conexão Ethernet ponto a ponto
- Conexão qualquer para qualquer
- Direto de sites do ExpressRoute

Considerações sobre segurança

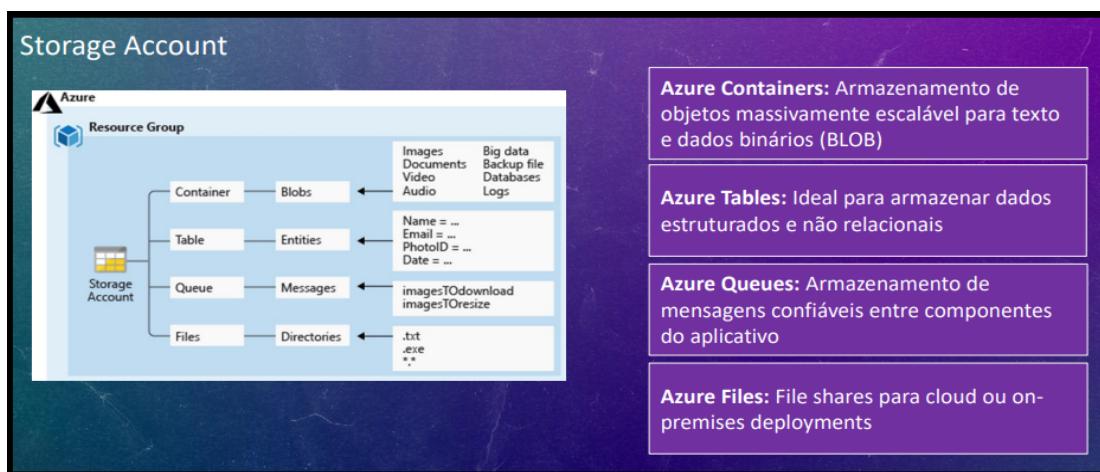
Com o ExpressRoute, os seus dados não passam pela Internet pública e, portanto, não são expostos aos riscos potenciais associados às comunicações da Internet. O ExpressRoute é uma conexão particular de sua infraestrutura local com a infraestrutura do Azure. Mesmo que você tenha uma conexão do ExpressRoute, consultas DNS, verificações de listas de certificados revogados e solicitações da Rede de Distribuição de Conteúdo do Azure ainda serão enviadas pela Internet pública.

- Azure DNS: O 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, tais como: confiabilidade e desempenho, segurança, facilidade do uso, personalizar redes virtuais e registro de alias. Os Domínios DNS no DNS do Azure são hospedados na rede global do Azure de servidores de nomes DNS, fornecendo resiliência e alta disponibilidade. O DNS do Azure usa rede anycast, de modo que cada consulta DNS é respondida pelo servidor DNS mais próximo disponível para fornecer desempenho rápido e alta disponibilidade para seu domínio. Segurança – O DNS do Azure baseia-se no Azure Resource Manager, que fornece recursos como: Azure RBAC (Controle de acesso baseado em função), Log de atividades, Bloqueio de recursos por assinatura, grupo de recursos ou de um recurso específico. Facilidade do uso: O DNS do Azure pode gerenciar os registros DNS para serviços do Azure e também fornece o DNS para recursos externos. O DNS do Azure é integrado ao portal do Azure e usa as mesmas credenciais, cobrança e contrato de suporte que outros serviços do Azure. Como o DNS do Azure está em execução no Azure, você pode gerenciar seus domínios e registros com o portal do Azure, cmdlets do Azure PowerShell e a CLI do Azure multiplataforma. Aplicativos que requerem gerenciamento automatizado de DNS podem se integrar no serviço usando a API REST e os SDKs. O DNS do Azure também dá suporte a domínios DNS privados. Esse recurso permite que você use seus nomes de domínio personalizados em suas redes virtuais privadas, em vez de ficar atrelado aos nomes fornecidos pelo Azure.
- Define public and private endpoints: 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 – 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.

Describe Azure storage services

Compare Azure storage services: O serviço de storage account é responsável pelo armazenamento de dados no Azure. Existem diferentes tipos de serviços de armazenamento no Azure, cada um responsável por armazenar um tipo de dado específico com características específicas.

- Azure containers: armazena objetos massivamente escaláveis para texto e dados binários (BLOBS). É a categoria de armazenamento mais "geral" do Azure, podendo armazenar imagens, vídeos, planilhas, arquivos de backup, base de dados, logs, textos, PDFs, etc. Para acessar um container e consumir os arquivos que ali estão, você deve utilizar o Portal Azure ou consumi-los via API Rest.
- Azure Tables: é o primeiro/mais básico formato de banco de dados não relacional do Azure, fornecendo um armazenamento de chave/atributo com um design sem esquema.
- Azure Queues: armazena mensagens confiáveis entre componentes do aplicativo (messages de microsserviços, por exemplo).
- Files: Diretórios compartilhados (fileserver) na nuvem, podendo ser mapeados em máquinas hospedadas na nuvem ou no ambiente on-premise.



Describe Azure storage tiers: Os dados armazenados na nuvem podem crescer em um ritmo exponencial. Para gerenciar os custos de suas necessidades cada vez maiores de armazenamento, é útil organizar seus dados com base em atributos como frequência de acesso e período de retenção planejado. Os dados armazenados na nuvem podem ser processados de maneira diferente considerando como eles são gerados, processados e acessados durante o tempo de vida. Alguns dados sãoativamente acessados e modificados durante seu ciclo de vida. Alguns dados são acessados com frequência no início do seu tempo de vida, mas esse acesso cai drasticamente à medida que os dados envelhecem. Alguns dados permanecem ociosos na nuvem e raramente são acessados depois de armazenados, talvez nunca. Para acomodar essas diferentes necessidades de acesso, o Azure fornece várias camadas de acesso, que você pode usar para balancear os custos de armazenamento com suas necessidades de acesso. As camadas de acesso (tiers) disponíveis incluem os seguintes tipos abaixo: [obs: os tiers podem ser definidos no blob durante ou após o upload.]

- **Camada de acesso quente:** otimizada para armazenar dados que são acessados com frequência (por exemplo, imagens de seu site).
- **Camada de acesso frio:** otimizada para dados acessados com menos frequência e armazenados por pelo menos 30 dias (por exemplo, faturas de seus clientes).
- **Camada de acesso aos arquivos:** adequada para dados acessados raramente e armazenados por pelo menos 180 dias, com requisitos de latência flexíveis (por exemplo, backups de longo prazo). → somente BLOB

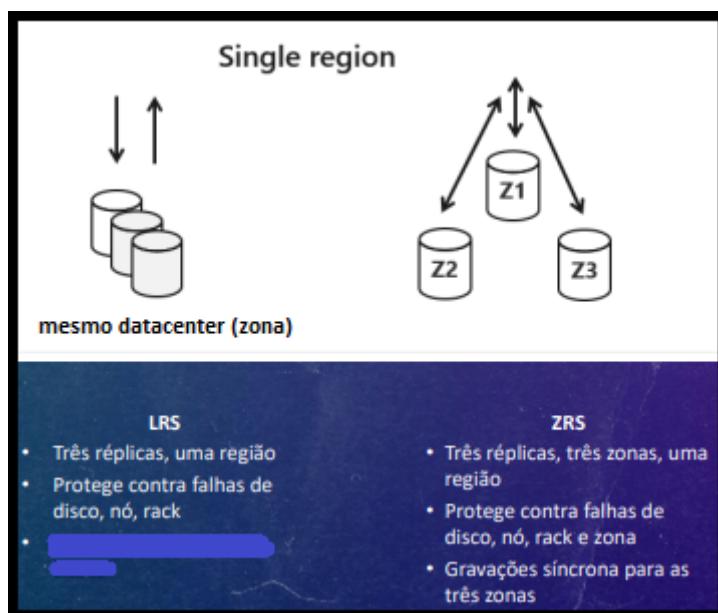


Describe Azure redundancy options: O Armazenamento do Azure sempre armazena várias cópias dos seus dados para que eles fiquem protegidos contra eventos planejados e não planejados, como falhas de hardware transitórias, interrupções de energia ou rede e desastres naturais. A redundância garante que sua conta de armazenamento atenda às suas metas de disponibilidade e durabilidade mesmo diante de falhas. Ao decidir qual opção de redundância é melhor para seu cenário, considere os benefícios comparativos entre custos menores e maior disponibilidade. Os fatores que ajudam a determinar qual opção de redundância você deve escolher incluem: Como os dados são replicados na região primária; Se os dados são replicados em uma segunda região que está geograficamente distante da região primária, para protegê-los contra desastres regionais; Se o aplicativo requer acesso de leitura aos dados replicados na região secundária, caso a região primária não esteja disponível.

- Redundância na região primária: Os dados em uma conta de Armazenamento do Azure são sempre replicados três vezes na região primária. O Armazenamento do Azure oferece duas opções para a replicação dos dados na região primária:

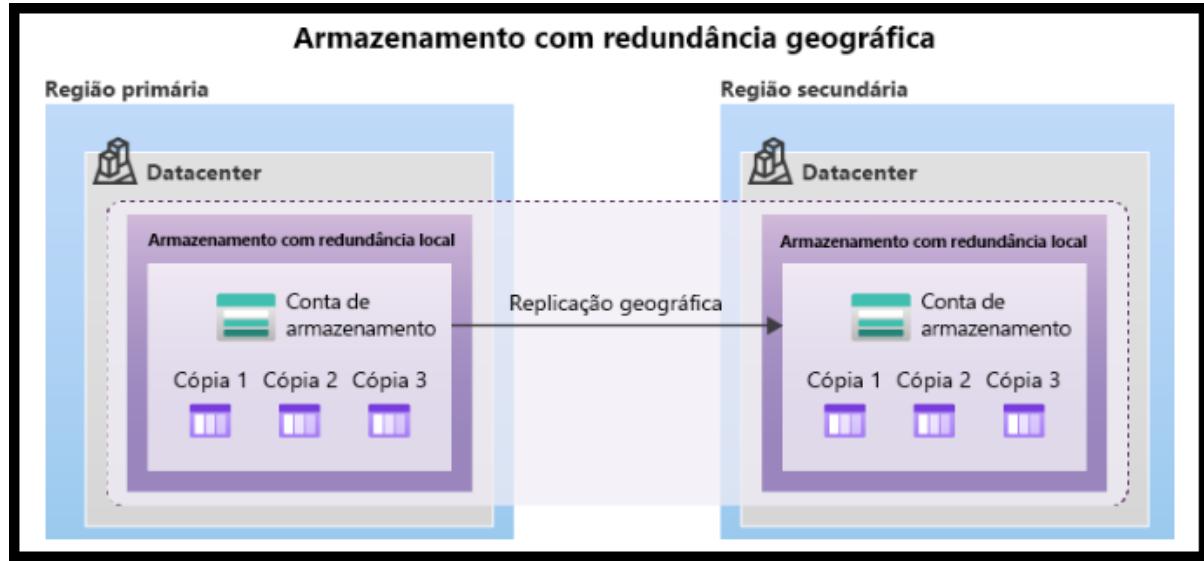
- 1) LRS (armazenamento com redundância local): O LRS replica seus dados três vezes em um único data center (zona) na região primária. É a opção de redundância de menor custo e oferece a menor durabilidade em comparação com outras opções. O LRS protege seus dados contra falhas de unidade e rack do servidor. No entanto, caso ocorra um desastre no data center, como um incêndio ou uma inundação, todas as réplicas de uma conta de armazenamento que use o LRS poderão ser perdidas ou se tornarem irrecuperáveis.

2) ZRS (armazenamento com redundância de zona): Em regiões habilitadas como zonas de disponibilidade, o ZRS (armazenamento com redundância de zona) replica os dados do Armazenamento do Azure de maneira síncrona em três zonas de disponibilidade do Azure na região primária. Com o ZRS, seus dados ainda podem ser acessados por operações de leitura e de gravação, mesmo em caso de não disponibilidade de uma zona. Não é necessário desmontar compartilhamentos de arquivos do Azure dos clientes conectados. Se uma zona se tornar indisponível, o Azure realizará atualizações da rede, como o redirecionamento de DNS. A Microsoft recomenda usar o ZRS na região primária para cenários que exigem alta disponibilidade. O ZRS também é recomendado para restringir a replicação de dados em um país ou uma região para atender aos requisitos de governança de dados.

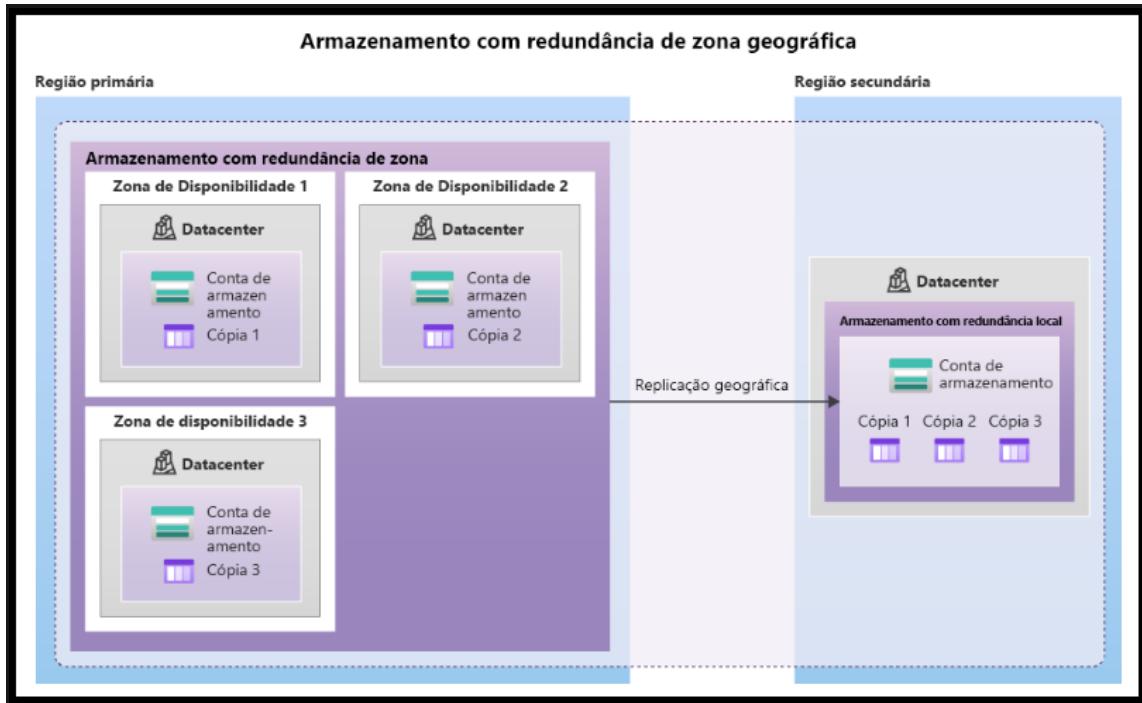


- Redundância em uma região secundária: Para aplicativos que exigem alta durabilidade, você pode optar por também copiar os dados em sua conta de armazenamento para uma região secundária que esteja a centenas de quilômetros de distância da região primária. Se os dados em sua conta de armazenamento forem copiados para uma região secundária, seus dados serão duráveis mesmo no caso de uma falha catastrófica que impeça que os dados na região primária sejam recuperados. Quando você cria uma conta de armazenamento, pode selecionar a região primária para a conta. A região secundária emparelhada é baseada nos Pares de Região do Azure e não pode ser alterada. O Armazenamento do Azure oferece duas opções para copiar seus dados em uma região secundária: GRS (armazenamento com redundância geográfica) e GZRS (armazenamento com redundância de zona geográfica). O GRS é semelhante à execução do LRS em duas regiões, e o GZRS é semelhante à execução de ZRS na região primária e LRS na região secundária. Por padrão, os dados na região secundária não ficam disponíveis para acesso de leitura ou gravação, a menos que haja um failover na região secundária. Se a região primária ficar indisponível, você poderá optar por fazer failover para a região secundária. Após a conclusão do failover, a região secundária se tornará a região primária e você poderá ler e gravar os dados novamente.

3) GRS (armazenamento com redundância geográfica): O GRS copia seus dados de maneira síncrona três vezes em um único local físico na região primária usando LRS. Em seguida, ele copia os dados de maneira assíncrona em um único local físico na região secundária (o par da região) usando LRS.



4) GZRS (armazenamento com redundância de zona geográfica): O GZRS combina a alta disponibilidade fornecida pela redundância entre zonas de disponibilidade com a proteção contra interrupções regionais fornecidas pela replicação geográfica. Os dados em uma conta de armazenamento GZRS são copiados entre três zonas de disponibilidade do Azure na região primária (semelhante ao ZRS) e são replicados em uma região geográfica secundária usando LRS para proteção contra desastres regionais. A Microsoft recomenda o uso do GZRS para aplicativos que exigem consistência, durabilidade e disponibilidade máximas, excelente desempenho e resiliência para recuperação de desastres.



- Acesso de leitura aos dados na região secundária (RA - reading access): O armazenamento com redundância geográfica (com GRS ou GZRS) replica seus dados para outro local físico na região secundária para proteger contra interrupções regionais. Esses dados estarão disponíveis para serem lidos

somente se o cliente ou a Microsoft iniciar um failover da região primária para a secundária. No entanto, se você habilitar o acesso de leitura à região secundária, seus dados estarão sempre disponíveis, mesmo que a região primária esteja sendo executada de maneira ideal. Para obter acesso de leitura para o local secundário, habilite o armazenamento com redundância geográfica com acesso de leitura (RA-GRS) ou o armazenamento com redundância de zona com acesso de leitura (RA-GZRS).

Describe storage account options and storage types: 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. Os dados nesta conta são seguros, altamente disponíveis, duráveis e maciçamente escalonáveis.

Tipo	Serviços com suporte	Opções de redundância	Usage
Uso geral v2 Standard	Armazenamento de Blobs (incluindo Data Lake Storage), Armazenamento 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. Caso deseje obter suporte para o NFS (Network File System) nos Arquivos do Azure, use o tipo de conta de compartilhamentos de arquivos premium.
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 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. Recomendadas para aplicações de escala empresarial ou de alto desempenho. Use esse tipo de conta caso deseje ter uma conta de armazenamento que dê suporte a compartilhamentos 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.

Um dos benefícios de usar uma Conta de Armazenamento do Azure é ter um namespace exclusivo no Azure para seus dados. Para fazer isso, cada conta de armazenamento no Azure deve ter um nome de conta exclusivo no Azure. Ao nomear sua conta de armazenamento, deve-se seguir as seguintes regras: Os nomes da conta de armazenamento devem ter entre 3 e 24 caracteres e podem conter apenas números e letras minúsculas; O nome da sua conta de armazenamento deve ser exclusivo no Azure. Duas contas de armazenamento não podem ter o mesmo nome.

Identify options for moving files, including AzCopy, Azure Storage Explorer and Azure File Sync:

Além da migração em larga escala usando serviços como Migrações para Azure e Azure Data Box, o Azure também tem ferramentas projetadas para ajudar você a mover ou interagir com arquivos individuais ou grupos de arquivos pequenos. Entre essas ferramentas estão AzCopy, Gerenciador de Armazenamento do Azure e Sincronização de Arquivos do Azure.

- AzCopy: O AzCopy é um utilitário de linha de comando que você pode usar para copiar blobs ou arquivos de/para uma conta de armazenamento. Com o AzCopy, você pode carregar arquivos, baixar arquivos, copiar arquivos entre contas de armazenamento e até mesmo sincronizar arquivos. O AzCopy pode até mesmo ser configurado para trabalhar com outros provedores de nuvem para ajudar a mover arquivos entre nuvens.
- Gerenciador de Armazenamento do Azure (Azure Storage Explorer): O Gerenciador de Armazenamento do Azure é um aplicativo autônomo que fornece uma interface gráfica para gerenciar arquivos e blobs em sua Conta do Armazenamento do Azure. Ele funciona em sistemas operacionais Windows, macOS e Linux e usa o AzCopy no back-end para executar todas as tarefas de gerenciamento de arquivos e blobs. Com o Gerenciador de Armazenamento, você pode carregar no Azure, baixar do Azure ou mover entre contas de armazenamento.
- Sincronizador de arquivos do Azure (Azure File Sync): A Sincronização de Arquivos do Azure é uma ferramenta que permite centralizar seus compartilhamentos de arquivos no serviço Arquivos do Azure e manter a flexibilidade, o desempenho e a compatibilidade de um servidor de arquivos do Windows. É quase como transformar o servidor de arquivos do Windows em uma rede de distribuição de conteúdo em miniatura. Depois de instalar a Sincronização de Arquivos do Azure no seu servidor Windows local, ele permanecerá automaticamente sincronizado bidirecionalmente com seus arquivos no Azure:

Com a Sincronização de Arquivos do Azure, você pode:

- Usar qualquer protocolo disponível no Windows Server para acessar seus dados localmente, incluindo SMB, NFS e FTPS.
- Ter tantos caches quantos precisar em todo o mundo.
- Substituir um servidor local com falha instalando a Sincronização de Arquivos do Azure em um novo servidor no mesmo datacenter.
- Configurar a camada de nuvem para que os arquivos acessados com mais frequência sejam replicados localmente, enquanto os arquivos acessados com pouca frequência sejam mantidos na nuvem até que sejam solicitados.

Describe migration options, including Azure Migrate and Azure Data Box: O Azure dá suporte à migração em tempo real de infraestrutura, aplicativos e dados usando o serviço Migrações para Azure, bem como a migração assíncrona de dados usando o Azure Data Box.

- Migrações para Azure (Azure Migrate): O Migrações para Azure é um serviço que ajuda você a migrar de um ambiente local para a nuvem. O Migrações para Azure funciona como um hub para ajudar você a gerenciar a avaliação e a migração do datacenter local para o Azure. Elas fornecem uma plataforma de migração unificada (um único portal para iniciar, executar e acompanhar sua migração para o Azure) e uma variedade de ferramentas (descoberta e avaliação, migração de servidor, integração com outros serviços do Azure e com ferramentas de fornecedores independentes de software - ISVs).

Ferramentas integradas

Além de trabalhar com ferramentas de ISVs, o hub do Migrações para Azure também inclui as seguintes ferramentas para ajudar na migração:

- **Migrações para Azure: Descoberta e avaliação.** Descubra e avalie servidores locais em execução em VMware, Hyper-V servidores físicos para se preparar para a migração para o Azure.
- **Migrações para Azure: Migração de Servidor.** Migr VMs do VMware, VMs do Hyper-V, servidores físicos, outros servidores virtualizados e VMs da nuvem pública para o Azure.
- **Assistente de Migração de Dados.** O Assistente de Migração de Dados é uma ferramenta autônoma criada para avaliar SQL Servers. Ele ajuda a identificar possíveis problemas que bloqueiam a migração. Ele identifica recursos sem suporte e novos recursos dos quais você pode se beneficiar após a migração e o caminho certo para a migração de banco de dados.
- **Serviço de Migração de Banco de Dados do Azure.** Migr bancos de dados locais para VMs do Azure executando SQL Server, Banco de Dados SQL do Azure ou Instâncias Gerenciadas de SQL.
- **Assistente de migração de aplicativo Web.** O Migration Assistant do Serviço de Aplicativo do Azure é uma ferramenta autônoma para avaliar sites locais para migração para o Serviço de Aplicativo do Azure. Use o Migration Assistant para migrar aplicativos Web .NET e PHP para o Azure.
- **Azure Data Box.** Use os produtos Azure Data Box offline para mover grandes quantidades de dados offline para o Azure.

- Azure Data Box: O Azure Data Box é um serviço de migração física que ajuda a transferir grandes quantidades de dados de maneira rápida, barata e confiável. A transferência de dados segura é acelerada com o envio de um dispositivo de armazenamento Data Box proprietário que tem uma capacidade máxima de armazenamento utilizável de 80 terabytes. O Data Box é transportado entre o datacenter por meio de uma empresa regional. Uma caixa robusta protege o Data Box contra danos durante o transporte. Você pode solicitar o dispositivo Data Box pelo portal do Azure para importar dados de ou exportar dados para o Azure. Depois que o dispositivo é recebido, você pode configurá-lo rapidamente usando a IU da Web local, e conectá-lo à sua rede. Depois de terminar a transferência dos dados (para dentro ou para fora do Azure), basta devolver o Data Box. Se você estiver transferindo dados para o Azure, eles serão carregados automaticamente depois que a Microsoft receber o Data Box de volta. Todo o processo é acompanhado de ponta a ponta pelo serviço Data Box no portal do Azure. Casos de uso do Azure Data box: Migração única – Quando um grande volume de dados do local é transferido para o Azure; Movimentação de uma biblioteca de mídia de fitas offline para o Azure para a criação de uma biblioteca de mídia online; Migração do farm de VMs, do SQL Server e de aplicativos para o Azure; Migração de dados históricos para o Azure para análise e relatórios detalhados com o HDInsight; Transferência em massa inicial – quando uma transferência em massa inicial é feita usando o Data Box (semente) seguida por transferências incrementais pela rede; Carregamentos periódicos - quando grandes quantidades de dados são geradas periodicamente e precisam ser movidas para o Azure.

Veja a seguir os vários cenários em que o Data Box pode ser usado para exportar dados do Azure.

- Recuperação de desastre – quando uma cópia dos dados do Azure é restaurada para uma rede local. Em um cenário típico de recuperação de desastre, um grande volume de dados do Azure é exportado para um Data Box. Em seguida, a Microsoft envia esse Data Box, e os dados são restaurados no seu local após um breve período.
- Requisitos de segurança – quando você precisa ser capaz de exportar dados provenientes do Azure devido a requisitos governamentais ou de segurança.
- Migrar de volta para o local ou para outro provedor de serviços de nuvem: quando desejar mover todos os dados de volta para o local ou para outro provedor de serviços de nuvem, exporte os dados por meio do Data Box para migrar as cargas de trabalho.

Depois que os dados do seu pedido de importação são importados no Azure, os discos do dispositivo são apagados, de acordo com os padrões NIST 800-88r1. Para uma ordem de exportação, os discos são apagados quando o dispositivo atinge o datacenter do Azure.

Describe Azure identify, access and security

Describe directory services in Azure, including Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra and Azure Active Directory Domain Services (Azure AD DS): 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.

- Quem usa o Azure AD?

- **Administradores de TI.** Os administradores podem usar o Azure AD para controlar o acesso a aplicativos e recursos com base em seus requisitos de negócios.
- **Desenvolvedores de aplicativos.** Os desenvolvedores podem usar o Azure AD para fornecer uma abordagem baseada em padrões para adicionar funcionalidade a aplicativos que eles criam, como adicionar a funcionalidade de SSO a um aplicativo ou habilitar um aplicativo para trabalhar com as credenciais existentes de um usuário.
- **Usuários.** Os usuários podem gerenciar as respectivas identidades e executar ações de manutenção, como redefinição de senha por autoatendimento.
- **Assinantes do serviço online.** Os assinantes do Microsoft 365, do Microsoft Office 365, do Azure e do Microsoft Dynamics CRM Online já estão usando o Azure AD para autenticação em suas contas.

- O que o Azure AD faz?

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 multifator, uma lista personalizada de senhas banidas e serviços de bloqueio inteligente.
- **Logon único:** o SSO (logon único) permite que você se lembre 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. À medida que os usuários trocam de funções ou saem de uma organização, as modificações de acesso são vinculadas àquela identidade, o que reduz consideravelmente o esforço necessário para alterar ou desabilitar contas.
- **Gerenciamento de aplicativo:** você pode gerenciar seus aplicativos de nuvem e locais usando o Azure AD. Recursos como Proxy de Aplicativo, aplicativos SaaS, o portal Meus Aplicativos e o logon único proporcionam uma experiência do usuário aprimorada.
- **Gerenciamento de dispositivo:** além das contas de pessoas individuais, o Azure AD dá 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 provenientes de dispositivos conhecidos, independentemente da conta de usuário solicitante.

- Azure Active Directory Domain Services (Azure AD DS):

O Azure AD DS (Azure Active Directory Domain Services) é um serviço que fornece serviços de domínio gerenciado, como ingresso no domínio, política de grupo, protocolo LDAP e autenticação Kerberos/NTLM. Assim como o Azure AD permite que você use serviços de diretório sem precisar manter uma infraestrutura de suporte, com Azure AD DS você obtém o benefício dos serviços de domínio sem a necessidade de implantar, gerenciar e corrigir DCs (controladores de domínio) na nuvem.

Um domínio gerenciado do Azure AD DS permite que você execute aplicativos herdados na nuvem que não podem usar métodos de autenticação modernos ou nos quais você não deseja que as pesquisas de diretório sempre voltem para um ambiente de AD DS local. Você pode realizar lift-and-shift desses aplicativos herdados do seu ambiente local para um domínio gerenciado, sem a necessidade de gerenciar o ambiente de AD DS na nuvem.

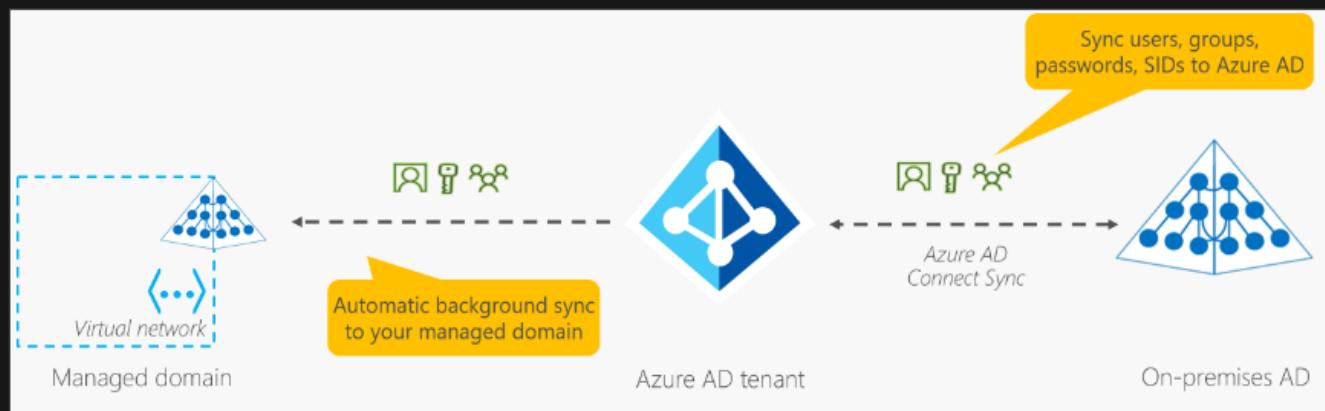
O Azure AD DS integra-se com o seu locatário existente do Azure AD. Essa integração permite que os usuários entrem em serviços e aplicativos conectados ao domínio gerenciado usando as credenciais que eles já têm. Você também pode usar grupos e contas de usuário para proteger o acesso aos recursos. Esses recursos fornecem um lift-and-shift mais suave de recursos locais para o Azure.

- Como funciona o Azure AD DS? Ao criar um domínio gerenciado do Azure AD DS, você define um namespace exclusivo. Esse namespace é o nome de domínio. Dois controladores de domínio do

Windows Server são então implantados na região do Azure que você selecionou. Essa implantação de DCs é conhecida como conjunto de réplicas. Você não precisa gerenciar, configurar nem atualizar esses DCs. A plataforma do Azure manipula os DCs como parte do domínio gerenciado, incluindo backups e a criptografia em repouso usando o Azure Disk Encryption.

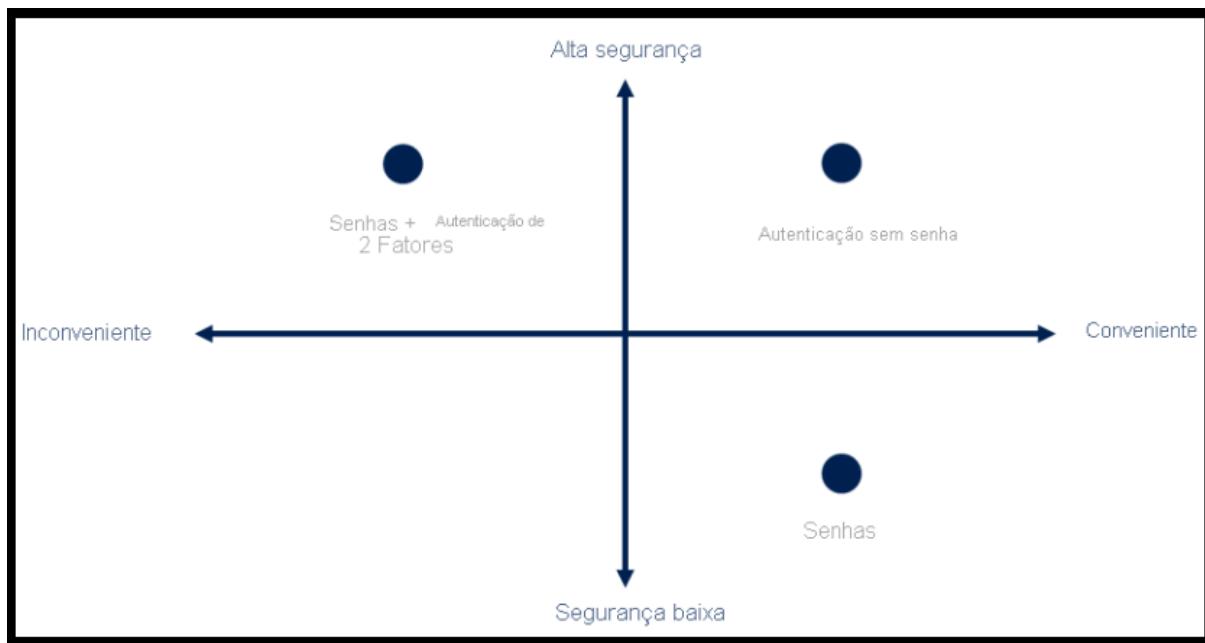
As informações são sincronizadas?

Um domínio gerenciado é configurado para executar uma sincronização unidirecional do Azure AD com o Azure AD DS. É possível criar recursos diretamente no domínio gerenciado, mas eles não são sincronizados com o Azure AD. Em um ambiente híbrido com um ambiente local do AD DS, o Azure AD Connect sincroniza as informações de identidade com o Azure AD, que, por sua vez, é sincronizado com o domínio gerenciado.



Então, aplicativos, serviços e VMs no Azure que se conectam a esse domínio gerenciado poderão usar recursos comuns do Azure AD DS, como o ingresso no domínio, a política de grupo, o LDAP e a autenticação Kerberos/NTLM.

Describe authentication methods in Azure, including single sign-on (SSO), multifactor authentication, and passwordless: Autenticação é o processo de estabelecer a identidade de uma pessoa, um serviço ou um dispositivo. Ela requer que a pessoa, o serviço ou o dispositivo forneça algum tipo de credencial para provar quem são. A autenticação é como apresentar a identidade quando você está viajando. Ela não confirma que você tem a passagem, só prova que você é quem diz ser. O Azure dá suporte a vários métodos de autenticação, incluindo senhas padrão, SSO (logon único), MFA (autenticação multifator) e métodos sem senha. Por muito tempo, a segurança e a conveniência pareciam estar em desacordo entre si. Atualmente, novas soluções de autenticação fornecem segurança e conveniência. O diagrama a seguir mostra o nível de segurança em comparação com a conveniência dos diferentes métodos de autenticação.



- O que é logon único (SSO)? O SSO (logon único) permite que um usuário entre uma vez e use essa credencial para acessar vários recursos e aplicativos de provedores diferentes. Para que o SSO funcione, os diferentes aplicativos e provedores devem confiar no autenticador inicial. Usar SSO nas contas facilita para os usuários gerenciarem suas identidades e para a TI gerenciar os usuários.

- O que é autenticação multifator? A autenticação multifator é o processo de solicitar a um usuário uma forma (ou um fator) adicional de identificação durante o processo de entrada. A MFA ajuda a proteger contra uma exposição de senha em situações em que a senha tenha sido comprometida, mas o segundo fator não. Esses elementos se enquadram em três categorias:

- Algo que o usuário saiba – essa pode ser uma pergunta de desafio.
- Algo que o usuário tenha – pode ser um código enviado para o telefone celular do usuário.
- Algo que o usuário seja – normalmente é algum tipo de propriedade biométrica, como a leitura de impressão digital ou reconhecimento facial.

- O que é autenticação sem senha (passwordless)? Recursos como a MFA são ótimas maneiras de proteger sua organização, mas os usuários geralmente ficam frustrados ao precisar memorizar senhas com a camada de segurança adicional. As pessoas são mais propensas a cumprir os processos de segurança quando é fácil e conveniente fazê-lo. Os métodos de autenticação sem senha são mais convenientes porque a senha é removida e substituída por algo que você tenha, além de algo que você seja ou saiba. A autenticação sem senha precisa ser configurada em um dispositivo para poder funcionar. Por exemplo, seu computador é algo que você tem. Depois de registrado ou inscrito, o Azure agora sabe que ele está associado a você. Agora que o computador é conhecido, uma vez que você forneça algo que você saiba ou seja (como um PIN ou uma impressão digital), você poderá ser autenticado sem usar uma senha.

Cada organização tem necessidades diferentes de autenticação. O Azure e Azure Governamental da Microsoft global oferece estas três opções de autenticação sem senha que se integram ao Azure Active Directory (Azure AD):

- Windows Hello para Empresas
- Aplicativo Microsoft Authenticator
- Chaves de segurança FIDO2

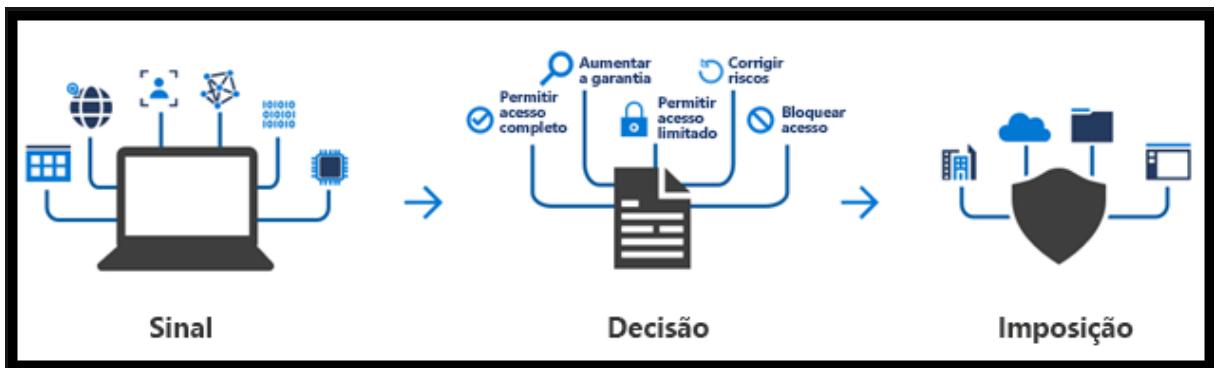
Describe external identities and guest access in Azure: Uma identidade externa é uma pessoa, um dispositivo, um serviço etc. que está fora da sua organização. O recurso Identidades Externas do Azure AD refere-se a todas as maneiras pelas quais você pode interagir com usuários fora da organização com segurança. Se você quiser colaborar com parceiros, distribuidores ou fornecedores, compartilhe seus recursos e defina como os usuários internos poderão acessar organizações externas. Se você é um desenvolvedor que cria aplicativos voltados para o consumidor, pode gerenciar as experiências de identidade dos clientes. As identidades externas podem soar semelhantes ao logon único. Com identidades externas, os usuários externos podem "trazer suas próprias identidades". Se eles tiverem uma identidade digital emitida pela empresa ou pelo governo ou uma identidade social não gerenciada, como o Google ou o Facebook, eles poderão usar as próprias credenciais para entrar. O provedor de identidade do usuário externo gerencia a identidade dele e você gerencia o acesso aos seus aplicativos com o Azure AD ou o Azure AD B2C para manter seus recursos protegidos.

As seguintes funcionalidades compõem identidades externas:

- **Colaboração B2B (Business to business)** – Colabore com usuários externos deixando que eles usem a identidade preferida para entrar nos aplicativos Microsoft ou em outros aplicativos empresariais (aplicativos SaaS, aplicativos personalizados etc.). Os usuários de colaboração B2B são representados em seu diretório, normalmente como usuários convidados.
- **Conexão direta B2B** – estabeleça uma relação de confiança mútua e de duas vias com outra organização do Azure AD para colaboração contínua. Atualmente, o B2B Direct Connect dá suporte Teams canais compartilhados, permitindo que usuários externos acessem seus recursos de dentro de suas instâncias de Teams. Os usuários do B2B Direct Connect não são representados em seu diretório, mas são visíveis de dentro do canal compartilhado Teams e podem ser monitorados em relatórios Teams centro de administração.
- **Azure AD B2C (business to customer)** – Publique aplicativos SaaS modernos ou aplicativos personalizados (exceto aplicativos Microsoft) para consumidores e clientes, usando o Azure AD B2C para gerenciamento de identidades e acesso.

Describe Conditional Access in Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra: O Acesso Condicional é uma ferramenta que o Azure Active Directory usa para permitir (ou negar) o acesso a recursos com base em sinais de identidade. Esses sinais incluem quem é o usuário, onde ele está e de qual dispositivo está solicitando acesso. O acesso condicional ajuda os administradores de TI a: Capacitar os usuários a serem produtivos em qualquer lugar e sempre; Proteger os ativos da organização. O Acesso Condicional também proporciona uma experiência de autenticação multifator mais granular para os usuários. Por exemplo, um segundo fator de autenticação poderá não ser solicitado se o usuário estiver em uma localização conhecida. No entanto, ele poderá ser solicitado se os sinais de conexão do usuário forem incomuns ou se o usuário estiver em uma localização inesperada. Durante a conexão, o acesso condicional coleta sinais do usuário, toma decisões com base nesses sinais e impõe essa

decisão, permitindo ou negando a solicitação de acesso ou solicitando uma resposta de autenticação multifator. O seguinte diagrama ilustra esse fluxo:



O acesso condicional é útil quando você precisa:

- Exija a MFA (autenticação multifator) para acessar um aplicativo, dependendo da função, da localização ou da rede do solicitante. Por exemplo, você pode exigir a MFA para administradores, mas não para usuários regulares ou pessoas que se conectam de fora da rede corporativa.
- Exigir acesso a serviços somente por meio de aplicativos cliente aprovados. Por exemplo, você pode limitar quais aplicativos de email podem se conectar ao serviço de email.
- Exigir que os usuários acessem seu aplicativo somente de dispositivos gerenciados. Um dispositivo gerenciado é um dispositivo que atende os padrões de segurança e conformidade.
- Bloquear o acesso de fontes não confiáveis, como o acesso de locais desconhecidos ou inesperados.

Describe Azure role-based access control (RBAC): o Azure permite controlar o acesso por meio do RBAC do Azure (controle de acesso baseado em função do Azure). O Azure fornece funções internas que descrevem regras de acesso comuns para os recursos de nuvem. Você também pode definir suas funções. Cada função tem um conjunto associado de permissões de acesso relacionadas a essa função. Quando você atribui indivíduos ou grupos a uma ou mais funções, eles recebem todas as permissões de acesso relacionadas. Portanto, se você contratar um novo engenheiro e adicioná-lo ao grupo do RBAC do Azure para engenheiros, ele obterá automaticamente o mesmo acesso que os outros engenheiros do mesmo grupo do RBAC do Azure. Da mesma forma, se você adicionar outros recursos e apontar o RBAC do Azure para eles, todos nesse grupo do RBAC do Azure vão ter as permissões nos novos recursos, bem como nos recursos existentes.

- Como o controle de acesso baseado em função é aplicado a recursos? O controle de acesso baseado em função é aplicado a um escopo, que é um recurso ou um conjunto de recursos ao qual esse acesso se aplica. O diagrama a seguir mostra a relação entre funções e escopos. Um grupo de gerenciamento, uma assinatura ou um administrador de recursos pode receber a função de proprietário, passando a ter maior controle e autoridade. Um observador, que não deve fazer atualizações, pode receber uma função de Leitor para o mesmo escopo, permitindo que ele examine ou observe o grupo de gerenciamento, a assinatura ou o grupo de recursos.

	Função				
	Leitor	Específica do recurso	Personalizada	Colaborador	Proprietário
Escopo	[A] Grupo de gerenciamento				
	[K] Assinatura	Observad...	Usuários gerenciando recursos	Administr...	
	[C] Grupo de recursos				
	[R] Recurso		Processos automatizados		

Observadores, usuários que gerenciam recursos, administradores e processos automatizados ilustram os tipos de usuários ou contas que normalmente são atribuídos a cada uma das várias funções.

O RBAC do Azure é hierárquico, porque quando você permite acesso a um escopo pai, essas permissões são herdadas por todos os filhos. Por exemplo: Quando você atribui a função Proprietário a um usuário no escopo do grupo de gerenciamento, esse usuário pode gerenciar tudo em todas as assinaturas dentro do grupo de gerenciamento; Quando você atribui a função Leitor a um grupo no escopo da assinatura, os membros desse grupo podem ver todos os grupos de recursos e os recursos na assinatura.

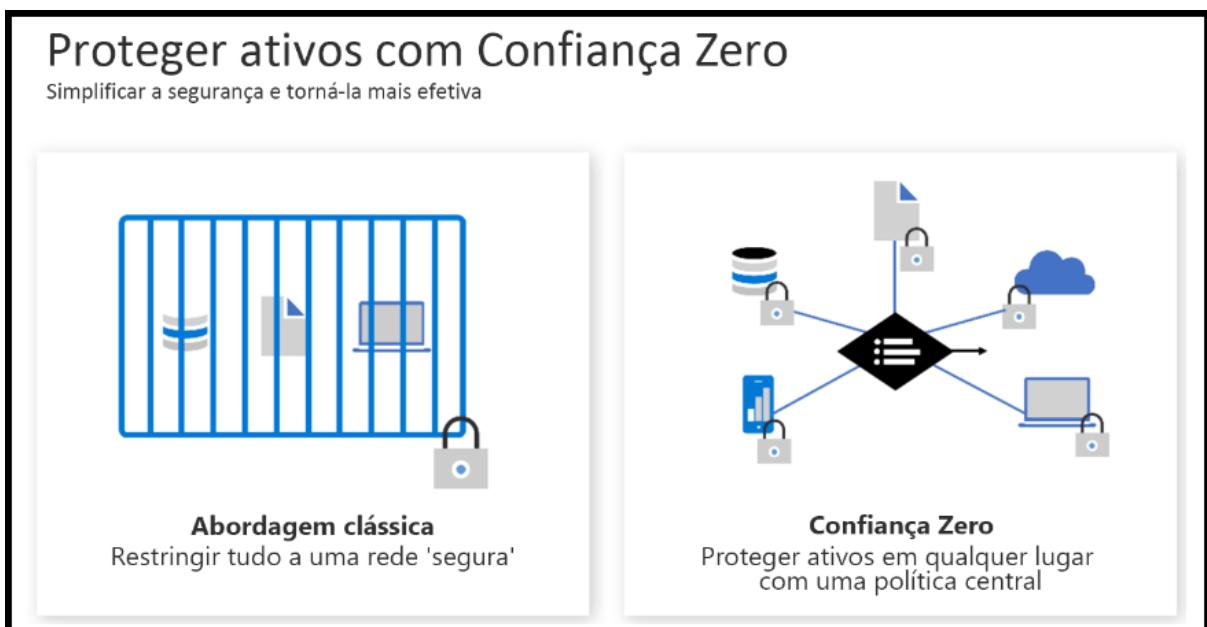
- Como o RBAC do Azure é imposto? O RBAC do Azure é imposto em qualquer ação iniciada em um recurso do Azure que passa pelo Azure Resource Manager. O Resource Manager é um serviço de gerenciamento que fornece um modo de organizar e proteger seus recursos de nuvem. Normalmente, você acessa o Resource Manager no portal do Azure, no Azure Cloud Shell, no Azure PowerShell e na CLI do Azure. O RBAC do Azure não impõe permissões de acesso no nível do aplicativo nem dos dados. A segurança do aplicativo precisa ser realizada pelo aplicativo. O RBAC do Azure usa um modelo de permissão. Quando você recebe uma função, o RBAC do Azure permite que você execute ações dentro do escopo dessa função. Se uma atribuição de função conceder a você permissões de leitura em um grupo de recursos e outra atribuição de função conceder a você permissões de gravação no mesmo grupo de recursos, você terá permissões de gravação e leitura nesse grupo de recursos.

Describe the concept of Zero Trust: A Confiança Zero é um modelo de segurança que pressupõe o pior cenário e protege os recursos com essa expectativa. A Confiança Zero pressupõe uma violação desde o início e verifica cada solicitação como se ela tivesse sido originada em uma rede não controlada. Atualmente, as organizações precisam de um novo modelo de segurança que se adapte efetivamente à complexidade dos ambientes modernos, adote a força de trabalho móvel e proteja pessoas, dispositivos, aplicativos e dados onde quer que eles estejam. Para abordar esse novo mundo da computação, a Microsoft recomenda altamente o modelo de segurança de Confiança Zero, que se baseia nos seguintes princípios orientadores:

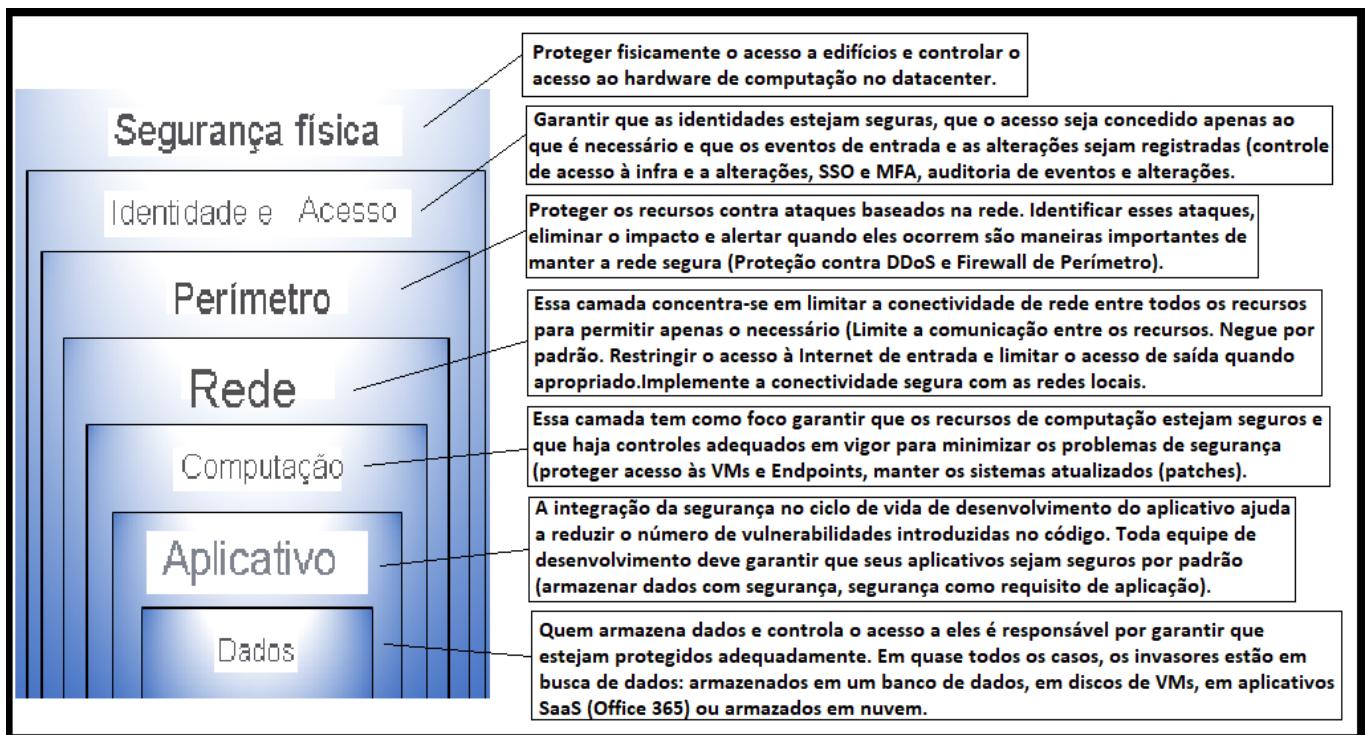
- Verificar de modo explícito – sempre autentique e autorize com base em todos os pontos de dados disponíveis.

- Usar o acesso com o mínimo de privilégios – limite o acesso do usuário com JIT/JEA (Just-In-Time e Just-Enough-Access), políticas adaptáveis baseadas em risco e proteção de dados.
- Pressupor a violação – minimize o raio de alcance e segmente o acesso. Verifique a criptografia de ponta a ponta. UDescribes Consegue a análise para obter visibilidade, promover a detecção de ameaças e aprimorar as defesas.

Tradicionalmente, as redes corporativas eram restritas, protegidas e, em geral, supostamente seguras. Somente computadores gerenciados podiam ingressar na rede, o acesso de VPN era fortemente controlado e os dispositivos pessoais eram frequentemente restritos ou bloqueados. O modelo de Confiança Zero muda completamente esse cenário. Em vez de supor que um dispositivo é seguro porque está dentro da rede corporativa, ele requer que todos se autentiquem. Em seguida, concede acesso com base na autenticação e não na localização.



Describe the purpose of the defense in depth model: O objetivo da defesa em profundidade é proteger as informações e impedir que elas sejam roubadas por pessoas que não estejam autorizadas a acessá-las. Uma estratégia de defesa em profundidade usa uma série de mecanismos para reduzir o avanço de um ataque que busca obter acesso não autorizado aos dados. Você pode visualizar a defesa em profundidade como um conjunto de camadas, com os dados a serem protegidos no centro e todas as outras camadas funcionando para proteger essa camada de dados central. Essa abordagem desacelera um ataque e fornece informações de alerta sobre as quais as equipes de segurança podem agir, automática ou manualmente. Camadas que contemplam a defesa em profundidade:



Describe the purpose of Microsoft Defender for Cloud: O Defender para Nuvem é uma ferramenta de monitoramento para gerenciamento da postura de segurança e proteção contra ameaças. Ele monitora ambientes de nuvem, locais, híbridos e de multinuvem para fornecer diretrizes e notificações com o objetivo de fortalecer sua postura de segurança. O Defender para Nuvem fornece as ferramentas necessárias para proteger seus recursos, acompanhar sua postura de segurança, proteger contra ataques cibernéticos e simplificar o gerenciamento de segurança. A implantação do Defender para Nuvem é fácil e já está integrada nativamente ao Azure. Como o Defender para Nuvem é um serviço nativo do Azure, muitos serviços do Azure são monitorados e protegidos sem a necessidade de qualquer implantação. No entanto, se você também tiver um datacenter local ou estiver operando em outro ambiente de nuvem, o monitoramento dos serviços do Azure poderá não fornecer uma visão completa da sua situação de segurança. Quando necessário, o Defender para Nuvem pode implantar automaticamente um agente do Log Analytics para coletar dados relacionados à segurança. Para computadores do Azure, a implantação é tratada diretamente. Em ambientes híbridos e multinuvem, os planos do Microsoft Defender são estendidos para computadores que não são do Azure com a ajuda do Azure Arc. Além disso, os recursos de GPSN (gerenciamento da postura de segurança na nuvem) são estendidos para computadores multinuvem sem a necessidade de agentes. O Defender para Nuvem também pode proteger recursos em outras nuvens (como AWS e GCP) você conectar uma conta do Amazon Web Services a uma assinatura do Azure, por exemplo.

Proteções nativas do Azure

O Defender para Nuvem ajuda a detectar ameaças em:

- Serviços PaaS do Azure – detecte ameaças que tenham como alvo serviços do Azure, incluindo o Serviço de Aplicativo do Azure, SQL do Azure, Conta de Armazenamento do Azure e outros serviços de dados. Você também pode executar a detecção de anomalias nos logs de atividades do Azure usando a integração nativa com o Microsoft Defender para Aplicativos de Nuvem (anteriormente conhecido como Microsoft Cloud App Security).
- Serviços de dados do Azure – o Defender para Nuvem inclui recursos que ajudam a classificar automaticamente os dados no SQL do Azure. Você também pode obter avaliações de possíveis vulnerabilidades nos serviços de Armazenamento e SQL do Azure e recomendações de como mitigá-las.
- Redes – o Defender para Nuvem ajuda a limitar a exposição a ataques de força bruta. Ao reduzir o acesso às portas de máquina virtual, usando o acesso de VM Just-In-Time, você pode proteger sua rede, impedindo acesso desnecessário. Você pode definir políticas de acesso seguro em portas selecionadas somente para usuários autorizados, endereços IP ou intervalos de endereços IP de origem permitida por um tempo limitado.

Avaliar, proteger e defender

O Defender para Nuvem preenche três necessidades vitais à medida que você gerencia a segurança de seus recursos e cargas de trabalho locais e na nuvem:

- Avaliação contínua – Conheça sua postura de segurança. Identifique e rastreie vulnerabilidades.
- Proteger – Proteja recursos e serviços com o Azure Security Benchmark.
- Defender – Detecte e resolva ameaças a recursos, cargas de trabalho e serviços.



Describe Azure management and governance (30–35%)

Describe cost management in Azure

Describe factors that can affect costs in Azure: O Azure desloca os custos de desenvolvimento de CapEx (despesa de capital) de criar e manter a infraestrutura e instalações para OpEx (despesa operacional) de alugar a infraestrutura conforme necessário, seja computação, armazenamento, rede etc.

Esse custo OpEx pode ser afetado por muitos fatores. Sendo os principais:

Tipo de recurso: Vários fatores influenciam o custo dos recursos do Azure. O tipo de recursos, as configurações do recurso e a região do Azure afetarão o custo de um recurso. Quando você provisiona um recurso do Azure, a plataforma cria instâncias limitadas para esse recurso. Os medidores rastreiam o uso dos recursos e geram um registro de uso para o cálculo da sua fatura (ex: armazenamento de blob, VMs, etc.).

Consumo: O pagamento conforme o uso é um tema consistente em todo o processo, e esse é o modelo de pagamento em nuvem em que você paga pelos recursos usados durante um ciclo de cobrança. No entanto, o Azure também permite que o usuário se comprometa a usar uma quantidade definida de recursos de nuvem com antecedência e receber descontos nesses recursos "reservados", tais como bancos de dados,

computação e armazenamento. Esse modelo permite reconhecer economias significativas em cargas de trabalho confiáveis e consistentes, ao mesmo tempo proporcionando a flexibilidade de aumentar rapidamente seu volume de nuvem à medida que a necessidade surge.

Manutenção: A flexibilidade da nuvem possibilita ajustar rapidamente os recursos com base na demanda. O uso de grupos de recursos pode ajudar a manter todos os seus recursos organizados. Para controlar os custos, é importante manter o ambiente de nuvem (administrar corretamente os recursos e recursos adicionais para não manter recursos desnecessários e ter maior controle sobre os custos de nuvem).

Painel Geografia (localização) do app selecionado: Ao provisionar a maioria dos recursos no Azure, você precisa definir uma região em que o recurso é implantado. Devido a variações como custo de energia, mão de obra, impostos e taxas, os custos de implantar recursos do Azure podem diferir dependendo da região.

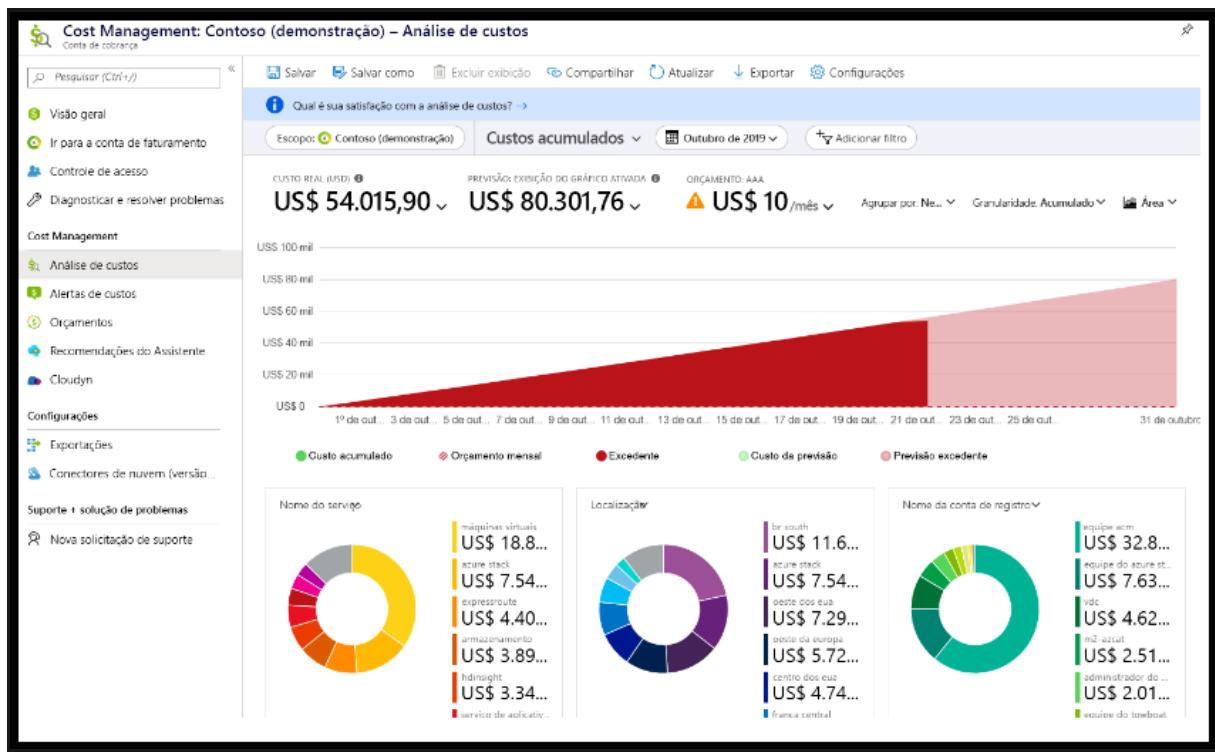
Tráfego de Rede: As zonas de cobrança são um fator para determinar o custo de alguns serviços do Azure. A largura de banda refere-se aos dados que entram e saem dos datacenters do Azure. Algumas transferências de dados de entrada (dados que entram em datacenters do Azure) são gratuitas. Para transferências de dados de saída (dados que saem de data centers do Azure), o preço de transferência de dados é baseado em zonas (Uma zona é um agrupamento geográfico de regiões do Azure para fins de cobrança).

Tipo de Assinatura: Alguns tipos de assinatura do Azure também incluem as concessões de uso, que afetam os custos. Por exemplo, uma assinatura de avaliação gratuita do Azure fornece acesso a vários produtos do Azure gratuitos por 12 meses. Ele também inclui crédito a ser gasto em seus primeiros 30 dias de inscrição. Você obterá acesso a mais de 25 produtos que são sempre gratuitos (com base na disponibilidade de recursos e regiões).

Azure Marketplace: O Azure Marketplace permite comprar soluções e serviços baseados no Azure de fornecedores de terceiros. Isso pode ser um servidor com software pré-instalado e configurado, ou dispositivos de firewall de rede gerenciados ou conectores para serviços de backup de terceiros. Ao comprar produtos por meio do Azure Marketplace, você pode pagar não apenas pelos serviços do Azure que está usando, mas também pelos serviços ou pela experiência do fornecedor de terceiros. As estruturas de cobrança são definidas pelo fornecedor.

Compare the Pricing calculator and the Total Cost of Ownership (TCO) calculator: A calculadora de preços e a calculadora TCO (custo total de propriedade) ajudam a entender possíveis despesas do Azure. Ambas podem ser acessadas pela Internet e permitem criar uma configuração. No entanto, as duas calculadoras têm propósitos muito diferentes. A calculadora de preços foi projetada para fornecer um custo estimado para provisionar recursos no Azure. Você pode obter uma estimativa para recursos individuais, criar uma solução ou usar um cenário de exemplo para ver uma estimativa dos gastos do Azure. O foco da calculadora de preços está no custo dos recursos provisionados no Azure. Já a calculadora de TCO foi projetada para ajudá-lo a comparar os custos para executar uma infraestrutura local versus uma infraestrutura de nuvem do Azure. Com a calculadora de TCO, você insere sua configuração de infraestrutura atual, incluindo servidores, bancos de dados, armazenamento e tráfego de rede de saída. Então a calculadora de TCO compara os custos previstos para seu ambiente atual com um ambiente do Azure que dá suporte aos mesmos requisitos de infraestrutura.

Describe the Azure Cost Management and Billing tool: O Gerenciamento de Custos permite verificar rapidamente os custos de recursos do Azure, criar alertas com base nos gastos com recursos e criar orçamentos que podem ser usados para automatizar o gerenciamento de recursos. A análise de custo é um subconjunto de Gerenciamento de Custos que apresenta um visual rápido para os custos do Azure. Usando a análise de custo, você pode visualizar rapidamente o custo total de várias maneiras, inclusive por ciclo de cobrança, região, recurso etc. Você usa a análise de custos para explorar e analisar seus custos organizacionais. Você pode visualizar os custos agregados por organização para entender onde os custos são acumulados e para identificar tendências de gastos. E você pode ver os custos acumulados ao longo do tempo para estimar tendências de custo mensais, trimestrais ou mesmo anuais em comparação a um orçamento.



Alertas de custo: Os alertas de custo fornecem um só local para verificar rapidamente todos os diferentes tipos de alerta que podem aparecer no serviço de Gerenciamento de Custos. Os três tipos de alertas que podem aparecer são: Alertas de orçamento – Os alertas de orçamento notificam você quando os gastos, com base em uso ou custos, atingem ou excedem o valor definido na condição de alerta do orçamento. Os orçamentos do Gerenciamento de Custos são criados usando o portal do Azure ou a API de Consumo do Azure. Alertas de Crédito – Os alertas de crédito notificam você quando seus compromissos monetários de crédito do Azure são consumidos. Os compromissos monetários se destinam a organizações que têm EAs (Contratos Enterprise). Os alertas de crédito são gerados automaticamente a 90% e a 100% do saldo de crédito do Azure. Alertas de cota de gasto do departamento – Os alertas de cota de gasto do departamento notificam você quando os gastos do departamento atingem um limite fixo da cota. As cotas de gasto são configuradas no Portal do EA. Sempre que um limite é atingido, ele gera um email para os proprietários do departamento no qual os alertas de custo são exibidos. Por exemplo, 50% ou 75% da cota.

Orçamentos: É em um orçamento que você define um limite de gastos para o Azure. Você pode definir orçamentos com base em uma assinatura, grupo de recursos, tipo de serviço ou outros critérios. Ao definir um orçamento, você também define um alerta de orçamento. Quando o orçamento atinge o nível de alerta do orçamento, ele dispara um alerta de orçamento que aparece na área de alertas de custo. Um uso mais avançado de orçamentos permite que as condições orçamentárias disparem a automação que suspende ou modifica recursos depois que a condição de gatilho ocorre.

Describe the purpose of tags: À medida que o seu uso da nuvem aumenta, passa a ser cada vez mais importante manter-se organizado. Uma boa estratégia de organização ajuda você a entender o seu uso da nuvem e pode ajudar a gerenciar os custos. Uma forma de organizar os recursos relacionados é por meio das próprias assinaturas ou também por grupos de recursos. Outra maneira de organizar recursos são as marcas de recursos (tags). As tags fornecem informações extras ou metadados sobre os recursos. Esses metadados são úteis para:

- **Gerenciamento de recursos** As marcas permitem que você localize em recursos associados a cargas de trabalho, ambientes, unidades de negócios e proprietários específicos e realize ações nesses recursos.
- **Gerenciamento e otimização de recursos** As marcas permitem agrupar os recursos para que você possa relatar custos, alocar centros de custos internos, acompanhar orçamentos e prever o custo estimado.
- **Gerenciamento de operações** As marcas permitem que você agrupe os recursos de acordo com o grau de importância da disponibilidade deles para os seus negócios. Esse agrupamento ajuda você a formular SLAs (Contratos de Nível de Serviço). Um SLA é uma garantia de tempo de atividade ou desempenho acordada entre você e seus usuários.
- **Segurança** As marcas permitem que você classifique os dados pelo nível de segurança, como público ou confidencial.
- **Governança e conformidade regulatória** As marcas permitem que você identifique recursos que se alinharam com os requisitos de conformidade regulatória ou de governança, como a ISO 27001. Elas também podem fazer parte dos seus esforços de imposição de padrões. Por exemplo, você pode exigir que todos os recursos sejam marcados com um proprietário ou um nome de departamento.
- **Automação e otimização de carga de trabalho** As marcas podem ajudar você a visualizar todos os recursos que participam de implantações complexas. Por exemplo, você pode marcar um recurso com o nome da carga de trabalho ou do aplicativo associado e usar um software como o Azure DevOps para executar tarefas automatizadas nesses recursos.

Como fazer para gerenciar as marcas de uso (tags)? Você pode adicionar, modificar ou excluir marcas de recursos por meio do Windows PowerShell, da CLI do Azure, dos modelos do Azure Resource Manager, da API REST ou do portal do Azure. Você pode usar o Azure Policy para impor a marcação de regras e convenções. Por exemplo, exija que determinadas marcas sejam adicionadas aos novos recursos à medida que eles forem provisionados. Defina também regras que reaplicam as marcas removidas. As marcas não são herdadas, o que significa que você pode aplicar marcas de um nível sem que elas apareçam automaticamente em um nível diferente, permitindo que você crie esquemas de marcação personalizados que mudam conforme o nível (recurso, grupo de recursos, assinatura etc.).

Um exemplo de estrutura de marcação

Uma marca de recurso consiste em um nome e um valor. Você pode atribuir uma ou mais marcas a cada recurso do Azure.

Nome	Valor
AppName	O nome do aplicativo do qual o recurso faz parte.
CostCenter	O código do centro de custo interno.
Proprietário	O nome do proprietário de negócios responsável pelo recurso.
Ambiente	Um nome de ambiente, como "Prod", "Dev" ou "Test".
Impacto	O grau de importância do recurso para as operações de negócios, como "Crítico", "De alto impacto" ou "De baixo impacto".

Tenha em mente que não é necessário impor a presença de uma marca específica em todos os recursos. Por exemplo, você pode decidir que apenas os recursos críticos tenham a marca Impact. Em seguida, todos os recursos não marcados não serão considerados críticos.

Describe features and tools in Azure for governance and compliance

Describe the purpose of Azure Blueprints: O que acontece quando a nuvem começa a ter mais do que apenas uma assinatura ou um ambiente? Como você pode dimensionar a configuração dos recursos? Como você pode impor configurações e políticas nas novas assinaturas? O Azure Blueprints permite padronizar as implantações de ambiente ou de assinatura de nuvem. Em vez de precisar configurar recursos como o Azure Policy para cada nova assinatura, com o Azure Blueprints você pode definir configurações e políticas repetíveis que são aplicadas à medida que as assinaturas são criadas. Você precisa de um novo ambiente de teste/desenvolvimento? O Azure Blueprints permite implantar um novo ambiente de Teste/Desenvolvimento com configurações de segurança e conformidade já definidas. Dessa forma, as equipes de desenvolvimento podem criar e implantar rapidamente novos ambientes com a certeza de que estão cumprindo os requisitos organizacionais.

O que são artefatos? Cada componente na definição de blueprint é conhecido como um artefato. É possível que os artefatos não tenham parâmetros adicionais (configurações). Um exemplo é a política Implantar detecção de ameaças nos servidores SQL, que não requer nenhuma configuração adicional. Os artefatos também podem conter um ou mais parâmetros que você pode configurar. Você pode especificar o valor de um parâmetro ao criar a definição de blueprint ou atribuí-la a um escopo. Com isso, você pode manter um blueprint padrão, mas ter a flexibilidade de especificar os parâmetros de configuração relevantes em cada escopo no qual a definição é atribuída.

O Azure Blueprints implanta um novo ambiente com base em todos os requisitos, as configurações e as definições dos artefatos associados. Os artefatos podem incluir itens como:

- Atribuições de função
- Atribuições de política
- Modelos do Azure Resource Manager
- Grupos de recursos

Como o Azure Blueprints ajuda a monitorar as implantações?

O Azure Blueprints inclui o controle de versão, o que permite que você crie uma configuração inicial e depois faça atualizações, atribuindo uma nova versão à atualização. Com o controle de versão, você pode fazer pequenas atualizações e acompanhar quais implantações usaram qual conjunto de configuração.

Com o Azure Blueprints, a relação entre a definição do blueprint (o que deve ser implantado) e a atribuição do blueprint (o que foi implantado) é preservada. Em outras palavras, o Azure cria um registro que associa um recurso ao blueprint que o define. Essa conexão ajuda você a acompanhar e auditar suas implantações.

Describe the purpose of Azure Policy: O Azure Policy é um serviço do Azure que permite criar, atribuir e gerenciar políticas que controlam ou auditam os recursos. Essas políticas impõem regras diferentes sobre as configurações dos recursos, de modo que essas configurações permaneçam em conformidade com os padrões corporativos.

Como o Azure Policy define as políticas? O Azure Policy permite que você defina políticas individuais e grupos de políticas relacionadas, conhecidas como iniciativas. O Azure Policy avalia seus recursos e realça os que não estão em conformidade com as políticas criadas por você. Ele também pode impedir a criação de recursos sem conformidade.

As Políticas do Azure podem ser definidas em cada nível, permitindo que você defina políticas em um recurso específico, um grupo de recursos, uma assinatura e assim por diante. Além disso, as Políticas do Azure são herdadas, portanto, se você definir uma política em um nível superior, ela será aplicada automaticamente a todos os agrupamentos que se enquadram no pai. Por exemplo, se você definir um Azure Policy em um grupo de recursos, todos os recursos criados nesse grupo de recursos receberão automaticamente a mesma política.

O Azure Policy vem com definições de iniciativa e política internas para Armazenamento, Rede, Computação, Central de Segurança e Monitoramento. Por exemplo, se você definir uma política que permita o uso de apenas um tamanho de VM (máquina virtual) em seu ambiente, essa política será invocada quando você criar uma VM e sempre que você redimensionar as VMs existentes. O Azure Policy também avalia e monitora todas as VMs atuais em seu ambiente, incluindo VMs que foram criadas antes da criação da política.

Em alguns casos, ele pode corrigir automaticamente os recursos e as configurações sem conformidade para garantir a integridade do estado dos recursos. Por exemplo, se todos os recursos de determinado grupo de recursos precisarem ser marcados com AppName e um valor igual a "SpecialOrders", o Azure Policy aplicará automaticamente essa marca se ela estiver ausente. No entanto, você ainda manterá o controle total do seu ambiente. Se houver um recurso específico que você não deseja que o Azure Policy corrija automaticamente, poderá sinalizar esse recurso como uma exceção e a política não o corrigirá automaticamente.

Além disso, o Azure Policy se integra ao Azure DevOps aplicando as políticas de pipeline de entrega e integração contínua que se pertencem às fases pré e pós-implantação dos seus aplicativos.

O que são iniciativas do Azure Policy? Uma iniciativa do Azure Policy é uma forma de agrupar políticas relacionadas. A definição de iniciativa contém todas as definições de política para ajudar a acompanhar seu estado de conformidade para atingir uma meta maior. Por exemplo, o Azure Policy inclui uma iniciativa chamada Habilitar o Monitoramento na Central de Segurança do Azure. A meta dele é

monitorar todas as recomendações de segurança disponíveis para todos os tipos de recursos do Azure na Central de Segurança do Azure.

Com essa iniciativa, as seguintes definições de política são incluídas:

- **Monitorar um banco de dados SQL não criptografado na Central de Segurança** Essa política monitora servidores e bancos de dados SQL não criptografados.
- **Monitorar vulnerabilidades de SO na Central de Segurança** Esta política monitora servidores que não atendem à linha de base de vulnerabilidade do sistema operacional configurado.
- **Monitorar o Endpoint Protection ausente na Central de Segurança** Essa política monitora servidores que não têm um agente de proteção de ponto de extremidade instalado.

Na verdade, a iniciativa Habilitar o Monitoramento na Central de Segurança do Azure contém mais de 100 definições de política separadas.

Describe the purpose of resource locks: Um bloqueio de recurso impede que os recursos sejam excluídos ou alterados acidentalmente. Mesmo com as políticas do controle de acesso baseado em função do Azure (RBAC do Azure) em vigor, ainda há um risco de que as pessoas com o nível correto de acesso possam excluir recursos de nuvem críticos. Os bloqueios de recursos podem ser aplicados a recursos individuais, grupos de recursos ou até mesmo a toda uma assinatura. Os bloqueios de recursos são herdados, o que significa que, se você colocar um bloqueio de recurso em um grupo de recursos, todos os recursos do grupo de recursos também terão o bloqueio de recurso aplicado. Os bloqueios de recursos podem ser gerenciados no portal do Azure, no PowerShell, na CLI do Azure ou em um modelo do Azure Resource Manager.

Tipos de Bloqueios de Recursos

Há dois tipos de bloqueios de recursos, um que impede que os usuários excluam e outro que impede que os usuários alterem ou excluam um recurso.

- A exclusão significa que os usuários autorizados ainda poderão ler e modificar um recurso, mas não poderão excluir o recurso.
- `ReadOnly` significa que os usuários autorizados poderão ler um recurso, mas não poderão excluir ou atualizar o recurso. Aplicar esse bloqueio é semelhante ao restringir todos os usuários autorizados para as permissões concedidas pela função Leitor.

Como fazer para excluir ou alterar um recurso bloqueado?

Embora o bloqueio ajude a evitar alterações acidentais, você ainda poderá fazer alterações seguindo um processo de duas etapas.

Para modificar um recurso bloqueado, primeiro, você precisará remover o bloqueio. Depois de remover o bloqueio, aplique qualquer ação que você tenha permissões para executar. Os bloqueios de recursos se aplicam independentemente das permissões de RBAC. Mesmo que você seja o proprietário do recurso, ainda precisará remover o bloqueio para realizar a atividade bloqueada.

Describe the purpose of the Service Trust Portal: O Portal de Confiança do Serviço da Microsoft é um local que oferece acesso a vários conteúdos, ferramentas e outros recursos sobre práticas de segurança, privacidade e conformidade da Microsoft. O Portal de Confiança do Serviço da Microsoft é um local que oferece acesso a vários conteúdos, ferramentas e outros recursos sobre práticas de segurança, privacidade e conformidade da Microsoft. O Portal de Confiança do Serviço contém detalhes sobre a implementação de controles e processos da Microsoft que protegem nossos serviços na nuvem e os dados do cliente.

encontrados neles. Para acessar alguns dos recursos do Portal de Confiança do Serviço, é preciso entrar como usuário autenticado com sua conta de serviços em nuvem da Microsoft (conta da organização do Azure Active Directory). Você precisará examinar e aceitar o contrato de confidencialidade da Microsoft dos materiais de conformidade.

Os recursos e o conteúdo do Portal de Confiança do Serviço podem ser acessados no menu principal. As categorias do menu principal são:

- **O Portal de Confiança do Serviço** fornece um hiperlink de acesso rápido para retornar à página inicial do Portal.
- **Documentos Confiáveis** fornecem uma grande quantidade de informações de design e implementação de segurança. A meta das informações é facilitar o cumprimento dos objetivos de conformidade regulatória entendendo como os serviços do Microsoft Cloud mantêm seus dados seguros. Os Documentos Confiáveis têm subitens, incluindo: Relatórios de Auditoria, Proteção de Dados e Azure Stack.
- **Setores & Regiões** fornecem informações de conformidade específicas do setor e da região sobre os serviços do Microsoft Cloud.
- **Links da Central de Confiabilidade** para a Central de Confiabilidade da Microsoft. A Central de Confiabilidade fornece mais informações sobre segurança, conformidade e privacidade no Microsoft Cloud. Essas incluem: informações sobre os recursos dos serviços do Microsoft Cloud que você pode usar para atender a requisitos específicos do Regulamento Geral sobre a Proteção de Dados; documentação útil para sua prestação de contas do GDPR; e documentação útil para entender as medidas técnicas e organizacionais que a Microsoft vem tomando para dar suporte ao GDPR.
- **Os recursos** fornecem acesso a mais recursos, como o Centro de Segurança e Conformidade, informações sobre Datacenters Globais da Microsoft e perguntas frequentes.
- **A Minha Biblioteca** permite salvar (ou fixar) documentos para serem acessados rapidamente na página Minha Biblioteca. Você também pode configurar para receber notificações quando os documentos em Minha Biblioteca forem atualizados.

Describe features and tools for managing and deploying Azure resources

Describe the Azure portal: O portal do Azure é um console unificado baseado na Web que fornece uma alternativa para as ferramentas de linha de comando. Com o portal do Azure, você pode gerenciar a assinatura do Azure usando uma interface gráfica do usuário. Você pode:

- Compile, gerencie e monitore tudo, desde aplicativos Web simples a implantações em nuvem complexas
- Crie painéis personalizados para ter uma exibição organizada dos recursos
- Configure opções de acessibilidade para ter a experiência ideal

O portal do Azure foi projetado para ter resiliência e disponibilidade contínua. Ele mantém uma presença em todos os datacenters do Azure. Essa configuração torna o portal do Azure resiliente a falhas de datacenters individuais e evita a lentidão da rede ao se manter perto dos usuários. O portal do Azure é atualizado continuamente e não requer nenhum tempo de inatividade para atividades de manutenção.

Describe Azure Cloud Shell, including Azure CLI and Azure PowerShell:

Azure Cloud Shell: O Azure Cloud Shell é uma ferramenta de shell baseada em navegador que permite criar, configurar e gerenciar recursos do Azure usando um shell. O Azure Cloud Shell dá suporte ao Azure PowerShell e à CLI (Interface de Linha de Comando) do Azure, que é um shell bash. É possível acessar o Azure Cloud Shell por meio do portal do Azure selecionando o ícone do Cloud Shell.

- É uma experiência de shell baseada em navegador sem a necessidade de instalação ou configuração local.
- Ele é autenticado em suas credenciais do Azure, portanto, quando você faz logon, ele sabe inherentemente quem você é e quais permissões você tem.
- Você escolhe o shell com o qual está mais familiarizado; o Azure Cloud Shell dá suporte ao Azure PowerShell e à CLI do Azure (que usa o Bash).

Azure PowerShell: O Azure PowerShell é um shell com o qual desenvolvedores, DevOps e profissionais de TI podem executar comandos chamados de command-lets (cmdlets). Esses comandos chamam a API REST do Azure para realizar tarefas de gerenciamento no Azure. Os cmdlets podem ser executados de modo independente para lidar com alterações pontuais ou ser combinados para ajudar a orquestrar ações complexas como:

- A configuração, desinstalação e manutenção de rotina de um único recurso ou de vários recursos conectados.
- A implantação de uma infraestrutura inteira, que pode conter dezenas ou centenas de recursos, de um código imperativo.

A captura dos comandos em um script torna o processo repetível e automatizado. Além de estar disponível por meio do Azure Cloud Shell, você pode instalar e configurar o Azure PowerShell em plataformas Windows, Linux e Mac.

O que é a CLI do Azure?

A CLI do Azure é funcionalmente equivalente ao Azure PowerShell, sendo a principal diferença a sintaxe dos comandos. Enquanto o Azure PowerShell usa comandos do PowerShell, a CLI do Azure usa comandos Bash.

A CLI do Azure fornece os mesmos benefícios de lidar com tarefas separadas ou orquestrar operações complexas por meio do código. Ele também pode ser instalado nas plataformas Windows, Linux e Mac, bem como por meio do Azure Cloud Shell.

Devido às semelhanças em termos de funcionalidade e acesso entre o Azure PowerShell e a CLI do Azure baseada em Bash, a questão se resume basicamente à linguagem com a qual você está mais familiarizado.

Describe the purpose of Azure Arc: O gerenciamento de ambientes híbridos e de várias nuvens pode se complicar rapidamente. O Azure oferece uma série de ferramentas para provisionar, configurar e monitorar recursos do Azure. E quanto aos recursos locais em uma configuração híbrida ou aos recursos de nuvem em uma configuração de várias nuvens? Ao utilizar o ARM (Azure Resource Manager), o Arc permite estender a conformidade e o monitoramento do Azure para suas configurações híbridas e multinuvem. O Azure Arc simplifica a governança e o gerenciamento ao fornecer uma plataforma de gerenciamento local e de várias nuvens consistente.

O Azure Arc fornece uma forma centralizada e unificada para:

- Gerenciar todo o seu ambiente projetando os recursos que não são do Azure no ARM.
- Gerencie máquinas virtuais híbridas e de várias nuvens, clusters do Kubernetes e bancos de dados como se eles estivessem em execução no Azure.
- Use as funcionalidades familiares de gerenciamento e serviços do Azure, independentemente de onde eles estejam hospedados.
- Continuar usando a ITOps tradicional, introduzindo práticas de DevOps para dar suporte a novos padrões nativos de nuvem no seu ambiente.
- Configurar localizações personalizadas como uma camada de abstração no cluster de Kubernetes habilitado para Azure Arc e nas extensões de cluster.

O que o Azure Arc pode fazer fora do Azure?

Atualmente, o Azure Arc permite que você gerencie os seguintes tipos de recursos hospedados fora do Azure:

- Servidores
- Clusters do Kubernetes
- Serviços de Dados do Azure
- SQL Server
- Máquinas virtuais (versão prévia)

Describe Azure Resource Manager and Azure Resource Manager templates (ARM templates): O ARM (Azure Resource Manager) é o serviço de implantação e gerenciamento do Azure. Ele fornece uma camada de gerenciamento que lhe permite criar, atualizar e excluir recursos em sua conta do Azure. Sempre que você faz qualquer coisa com seus recursos do Azure, o ARM está envolvido.

Quando um usuário envia uma solicitação de ferramentas, APIs ou SDKs do Azure, o ARM recebe a solicitação. O ARM se autentica e autoriza a solicitação. Então, o ARM envia a solicitação para o serviço do Azure, que executa a ação solicitada. Você vê resultados e recursos consistentes em todas as diferentes ferramentas porque todas as solicitações são tratadas por meio da mesma API.

Benefícios do Azure Resource Manager

Com o Azure Resource Manager, você pode:

- Gerenciar sua infraestrutura por meio de modelos declarativos em vez de scripts. Um modelo do Resource Manager é um arquivo JSON que define o que você deseja implantar no Azure.
- Implantar, gerenciar e monitorar todos os recursos da sua solução como um grupo em vez de tratá-los individualmente.
- Reimplantar a solução durante o ciclo de vida de desenvolvimento e ter confiança de que os recursos serão implantados em um estado consistente.
- Definir as dependências entre os recursos para que eles sejam implantados na ordem correta.
- Aplicar o controle de acesso a todos os serviços porque o RBAC é integrado nativamente à plataforma de gerenciamento.
- Aplicar marcas aos recursos para organizar de modo lógico todos os recursos em sua assinatura.
- Esclarecer a cobrança da organização exibindo os custos de um grupo de recursos que compartilham a mesma marca.

Modelos de ARM

A infraestrutura como código é um conceito em que você gerencia sua infraestrutura como linhas de código. Usar o Azure Cloud Shell, o Azure PowerShell ou a CLI do Azure são alguns exemplos de uso de código para implantar a infraestrutura de nuvem. Modelos do ARM são outro exemplo de infraestrutura como código em ação.

Ao usar os modelos do ARM, você pode descrever os recursos que deseja usar em um formato JSON declarativo. Com um modelo do ARM, o código de implantação é verificado antes da execução de qualquer código. Isso garante que os recursos serão criados e conectados corretamente. Em seguida, o modelo orquestra a criação desses recursos em paralelo. Ou seja, se você precisar de 50 instâncias do mesmo recurso, todas as 50 instâncias serão criadas ao mesmo tempo.

No fim das contas, o desenvolvedor, o DevOps profissional ou o profissional de TI precisa apenas definir o estado desejado e a configuração de cada recurso no modelo do ARM e o modelo fará o resto. Os modelos podem até mesmo executar scripts do PowerShell e Bash antes ou depois da configuração de um recurso.

Benefícios de usar modelos do ARM

Os modelos do ARM proporcionam muitos benefícios ao planejar a implantação de recursos do Azure. Alguns desses benefícios incluem:

- **Sintaxe declarativa:** Os modelos ARM permitem criar e implantar uma infraestrutura inteira do Azure de forma declarativa. A sintaxe declarativa significa que você declara o que deseja implantar, mas não precisa escrever os comandos de programação e a sequência de fato para implantar os recursos.
- **Resultados repetidos:** Implante repetidamente sua infraestrutura em todo seu ciclo de vida de desenvolvimento e com a confiança de que seus recursos são implantados em um estado consistente. Você pode usar o mesmo modelo do ARM para implantar vários ambientes de desenvolvimento/teste, sabendo que todos os ambientes são iguais.
- **Orquestração:** Você não precisa se preocupar com as complexidades das operações de ordenação. O Azure Resource Manager orquestra a implantação dos recursos interdependentes para que eles sejam criados na ordem correta. Quando possível, o Azure Resource Manager implanta recursos em paralelo para que suas implantações sejam concluídas mais rapidamente do que as implantações seriais. Você implanta o modelo por meio de um comando, em vez de vários comandos imperativos.
- **Arquivos modulares:** Você pode dividir seus modelos em componentes menores e reutilizáveis e vinculá-los no momento da implantação. Também é possível aninhar um modelo em outro modelo. Por exemplo, você pode criar um modelo para uma pilha de VM e então aninhar esse modelo dentro de modelos que implantam ambientes inteiros, e essa pilha de VM será consistentemente implantada em cada um dos modelos de ambiente.
- **Extensibilidade:** com scripts de implantação, você pode adicionar scripts do PowerShell ou Bash aos seus modelos. Os scripts de implantação estendem sua capacidade de configurar recursos durante a implantação. Um script pode ser incluído no modelo ou armazenado em uma fonte externa e referenciado no modelo. Os scripts de implantação oferecem a capacidade de concluir a configuração de seu ambiente de ponta a ponta em um único modelo ARM.

Describe monitoring tools in Azure

Describe the purpose of Azure Advisor: O Assistente do Azure avalia seus recursos do Azure e faz recomendações para ajudar a melhorar a confiabilidade, a segurança e o desempenho, alcançar a excelência operacional e reduzir os custos. O Assistente do Azure foi projetado para ajudar você a poupar tempo na otimização da nuvem. O serviço de recomendação inclui ações sugeridas que você pode adotar imediatamente, adiar ou ignorar. As recomendações estão disponíveis por meio do portal do Azure e da API, e é possível configurar notificações para alertar você sobre novas recomendações. Quando você está no portal do Azure, o painel do Assistente exibe recomendações personalizadas para todas as suas

assinaturas. Você pode usar filtros para selecionar recomendações para assinaturas, grupos de recursos ou serviços específicos. As recomendações são divididas em cinco categorias:

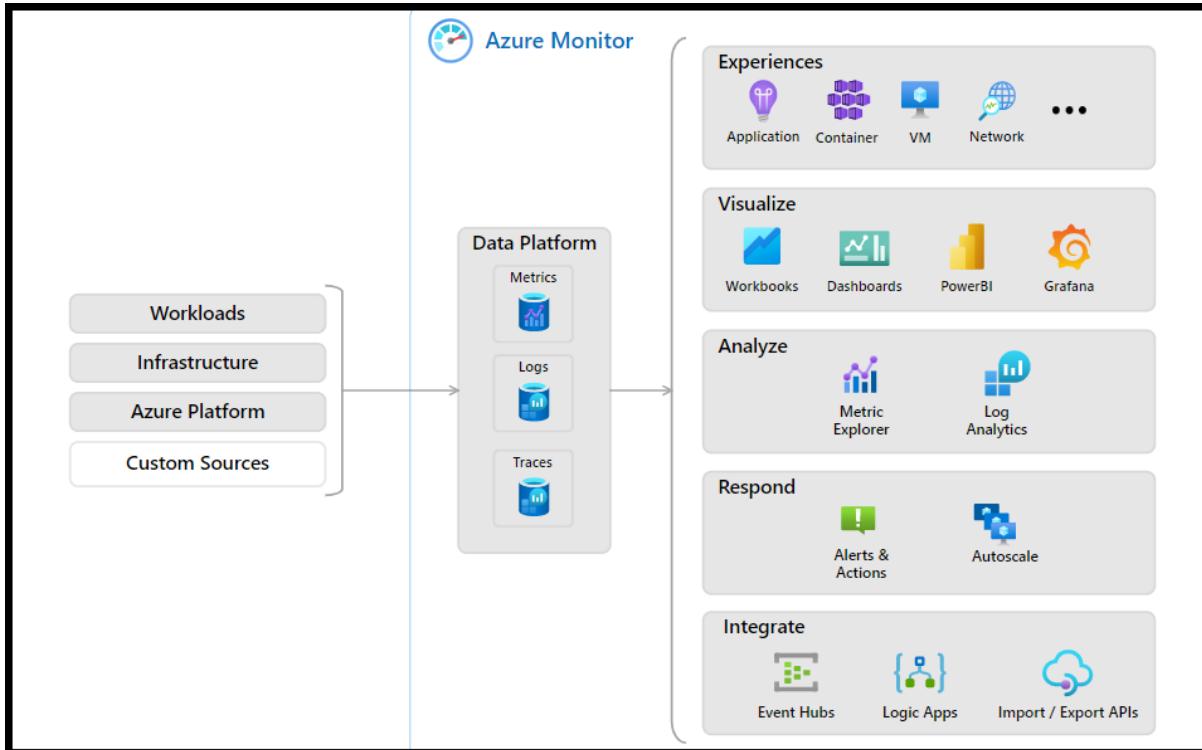
- A **confiabilidade** é usada para garantir e aprimorar a continuidade dos seus aplicativos comercialmente críticos.
- A **segurança** é usada para detectar ameaças e vulnerabilidades que podem levar a violações de segurança.
- O **desempenho** é usado para melhorar a velocidade de seus aplicativos.
- A **excelência operacional** é usada para ajudar você a obter eficiência de processo e fluxo de trabalho, capacidade de gerenciamento de recursos e melhores práticas de implantação.
- O **custo** é usado para otimizar e reduzir os gastos gerais do Azure.

Describe Azure Service Health: A Integridade do Serviço do Azure ajuda você manter o controle do recurso do Azure, tanto os recursos especificamente implantados quanto o status geral do Azure. A integridade do serviço do Azure faz isso combinando três serviços diferentes do Azure:

- **O Status do Azure** é uma visão geral do status do Azure em todo o globo. O status do Azure informa sobre interrupções de serviço no Azure na página Status do Azure . A página é uma exibição global da integridade de todos os serviços do Azure em todas as regiões do Azure. É uma boa rápida para incidentes com impacto generalizado.
- **A Integridade do Serviço** fornece uma visão mais restrita dos serviços e das regiões do Azure. Ela se concentra nos serviços e regiões do Azure que você está usando. Esse é o melhor lugar onde procurar serviços que afetam as comunicações sobre interrupções, atividades de manutenção planejada e outros avisos de integridade, porque a experiência autenticada da Integridade do Serviço sabe quais serviços e recursos você usa atualmente. Você até pode configurar alertas da Integridade do Serviço para ser notificado quando problemas de serviço, manutenção planejada ou outras alterações puderem afetar os serviços e as regiões do Azure que você usa.
- **O Resource Health** é uma exibição personalizada dos recursos reais do Azure. Ele fornece informações sobre a integridade de cada um de seus recursos de nuvem, como uma instância de máquina virtual específica. Usando o Azure Monitor, você também pode configurar alertas para notificá-lo de alterações de disponibilidade para seus recursos de nuvem.

Usando o Status do Azure, a Integridade do serviço e a Integridade do recurso, a Integridade do Serviço do Azure fornece uma visão completa do ambiente do Azure desde o status global dos serviços e regiões do Azure até recursos específicos. Além disso, os alertas históricos são armazenados e ficam acessíveis para revisão posterior. Algo que você inicialmente pensou ser uma anomalia simples e se transformou em uma tendência, pode ser prontamente revisado e investigado graças aos alertas históricos. Por fim, caso uma carga de trabalho que você está executando seja afetada por um evento, a Integridade do Serviço do Azure fornecerá links para suporte.

Describe Azure Monitor, including Log Analytics, Azure Monitor alerts, and Application Insights: O Azure Monitor é uma plataforma para coletar dados sobre seus recursos, analisar esses dados, visualizar as informações e até mesmo agir com base nos resultados. O Azure Monitor pode monitorar recursos do Azure, seus recursos locais e até mesmo recursos de várias nuvens, como máquinas virtuais hospedadas com um provedor de nuvem diferente. O diagrama a seguir ilustra o nível de abrangência do Azure Monitor:



À esquerda fica uma lista das fontes dos dados de registro em log e de métrica que podem ser coletados em cada camada na arquitetura do aplicativo, indo do aplicativo ao sistema operacional e à rede. No centro, os dados de registro em log e de métricas são armazenados em repositórios centrais. À direita, os dados são usados de várias maneiras. Você pode exibir o desempenho histórico e em tempo real em cada camada da arquitetura ou ver informações agregadas e detalhadas. Os dados são exibidos em diferentes níveis para públicos-alvo diferentes. É possível exibir relatórios de alto nível no painel do Azure Monitor ou criar modos de exibição personalizados usando consultas do Power BI e do Kusto. Além disso, os dados podem ser usados para ajudar você a reagir a eventos críticos em tempo real, por meio de alertas entregues às equipes por SMS, email etc. Outra opção é usar limites a fim de disparar a funcionalidade de dimensionamento automático para escalar conforme a demanda.

Azure Log Analytics

O Log Analytics do Azure é a ferramenta do portal do Azure em que você escreverá e executará consultas de log nos dados coletados pelo Azure Monitor. O Log Analytics é uma ferramenta robusta que dá suporte a consultas simples e complexas e à análise de dados. Você pode escrever uma consulta simples que retorna um conjunto de registros e usar os recursos do Log Analytics para classificá-los, filtrá-los e analisá-los. Você pode escrever uma consulta avançada para executar a análise estatística e visualizar os resultados em um gráfico a fim de identificar uma tendência específica. Independentemente de você trabalhar com os resultados das suas consultas de maneira interativa ou usá-las com outros recursos do Azure Monitor, como alertas de consulta de log ou pastas de trabalho, o Log Analytics é a ferramenta que você usará para escrever e testar essas consultas.

Alertas do Azure Monitor

Os Alertas do Azure Monitor são formas automatizadas de se manter informado caso o Azure Monitor detecte um limite sendo ultrapassado. Você define as condições de alerta, as ações de notificação e, em seguida, os Alertas do Azure Monitor notificam quando um alerta é disparado. Dependendo da sua configuração, os Alertas do Azure Monitor também podem tentar uma ação corretiva.

Os alertas podem ser configurados para monitorar os logs e disparar sob determinados eventos de log ou podem ser definidos para monitorar métricas e disparar caso determinadas métricas sejam ultrapassadas. Por exemplo, você poderia definir um alerta baseado em métrica para notificá-lo quando o uso da CPU em uma máquina virtual excedesse 80%. As regras de alerta baseadas em métricas fornecem alertas quase em tempo real baseados em valores numéricos. As regras baseadas em logs permitem uma lógica complexa entre os dados de várias fontes.

Os Alertas do Azure Monitor usam grupos de ações para configurar a quem notificar e quais ações tomar. Um grupo de ações é simplesmente uma coleção de preferências de notificação e ação que você associa a um ou vários alertas. O Azure Monitor, a Integridade do Serviço e o Assistente do Azure usam grupos de ações para notificar você sobre um alerta que foi disparado.

Application Insights

O Application Insights, um recurso do Azure Monitor, monitora seus aplicativos Web. O Application Insights consegue monitorar aplicativos que esteja em execução no Azure, localmente ou em outro ambiente de nuvem.

Há duas maneiras de configurar o Application Insights para ajudar a monitorar seu aplicativo. Você pode instalar um SDK em seu aplicativo ou usar o agente do Application Insights. O agente do Application Insights é compatível com C#.NET, VB.NET, Java, JavaScript, Node.js e Python.

Depois que o Application Insights estiver em execução, você poderá usá-lo para monitorar uma ampla variedade de informações, como:

- As taxas, tempos de resposta e taxas de falha de solicitação
- Taxas de dependência, tempos de resposta e taxas de falha: para mostrar se os serviços externos estão desacelerando o desempenho
- Exibições de página e o desempenho de carregamento relatados por navegadores dos usuários
- Chamadas AJAX de páginas da web, incluindo taxas, tempos de resposta e taxas de falha
- Contagens de sessão e usuários
- Contadores de desempenho de máquinas de servidor Linux ou Windows server, como CPU, memória e uso da rede

O Application Insights não só ajuda a monitorar o desempenho do seu aplicativo, mas você também pode configurá-lo para enviar periodicamente solicitações sintéticas para seu aplicativo, permitindo que você verifique o status e monitore o aplicativo mesmo durante períodos de baixa atividade.