Strecht Simulados · Guia de preparação



Guia de preparação AZ-900

Tudo o que a prova cobra, organizado por domínio: conceitos-chave, comparações que confundem, pegadinhas reais, gatilhos do enunciado, questões comentadas e um plano para chegar pronto ao exame.

3
capítulos por domínio

21
questões comentadas

70%
nota de corte

6
provas completas no curso

ANTES DE COMEÇAR

Como usar este guia

Este guia foi feito para ser estudado junto com as 6 provas completas do curso AZ-900: o guia explica o que cai e onde estão as armadilhas; as provas treinam o ritmo e mostram o que você ainda não domina.

Quando	O que fazer
Semana 1	Faça o teste diagnóstico (página seguinte) e leia os capítulos 1 e 2. No fim da semana, faça a Prova 1 do curso no tempo do exame.
Semana 2	Leia os demais capítulos, começando pelos domínios em que você errou mais no diagnóstico. Faça as provas 2 e 3.
Semana 3	Releia os alertas de pegadinha e as tabelas de comparação. Faça as provas 4 e 5 e revise cada erro pela explicação.
Semana 4	Estude a folha de cola, faça a Prova 6 e refaça as provas abaixo de 80%. Agende o exame quando estiver acima de 80% em todas (a nota de corte é 70%).

Mapa do exame

Cada prova do curso tem 50 questões e 45 minutos, no formato do exame. Referência de aprovação: 70%.

Domínio (capítulo)	Peso	Neste guia
1. Descrever a arquitetura e os serviços do Azure	35-40%	18 conceitos · 14 pegadinhas
2. Descrever conceitos de nuvem	25-30%	18 conceitos · 14 pegadinhas
3. Descrever o gerenciamento e a governança do Azure	30-35%	18 conceitos · 14 pegadinhas

Como ler os capítulos: os **tópicos-chave** são o que mais cai; a **tabela de memorização** separa o que a prova costuma confundir; os **alertas de prova** mostram as armadilhas das alternativas erradas; os **gatilhos** ligam palavras do enunciado à resposta; e o **checklist** diz se você está pronto para o domínio.

Estude um pouco todo dia, de graça

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o "não confunda" de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

DIAGNÓSTICO

Você já sabe isso?

Responda às 9 questões sem consultar nada. As respostas, com a explicação e o capítulo para revisar, estão no fim do guia. Comece o estudo pelos capítulos em que errou.

D1 · Descrever a arquitetura e os serviços do Azure

Uma empresa guarda documentos acessados poucas vezes por ano, que devem ficar ao menos 90 dias armazenados e precisam ser lidos na hora quando solicitados. Qual camada de acesso de blobs tem o menor custo para esse caso?

A. Camada de arquivo (Archive)
B. Camada quente (Hot)
C. Camada fria (Cold)
D. Camada premium de blocos

D2 · Descrever a arquitetura e os serviços do Azure

Uma empresa quer oferecer aos funcionários desktops Windows acessíveis de qualquer dispositivo, com os dados guardados na nuvem. Qual serviço atende a essa necessidade?

A. Azure Container Instances
B. Azure Virtual Desktop
C. Azure App Service
D. Azure Functions

D3 · Descrever a arquitetura e os serviços do Azure

Os usuários esquecem a senha com frequência e abrem muitos chamados no suporte. Qual recurso do Microsoft Entra ID reduz esses chamados?

A. Grupo de gerenciamento raiz
B. Bloqueio de recurso CanNotDelete
C. Emparelhamento de redes virtuais
D. Redefinição de senha por autoatendimento

D4 · Descrever conceitos de nuvem

Uma aplicação mantém o tempo de resposta estável nos picos porque adiciona instâncias e distribui a carga entre elas. Qual benefício da nuvem é esse?

A. Modelo de despesa CapEx
B. Nuvem privada dedicada
C. Previsibilidade de desempenho
D. Soberania dos dados locais

D5 · Descrever conceitos de nuvem

Uma empresa quer pagar pela capacidade de computação apenas pelo tempo em que ela for usada, sem investimento inicial em servidores. Qual característica da nuvem atende a esse objetivo?

A. Compra antecipada de servidores próprios
B. Contrato de hardware dedicado por cinco anos
C. Modelo baseado em consumo
D. Modelo de licenciamento perpétuo

D6 · Descrever conceitos de nuvem

Uma loja virtual precisa adicionar servidores automaticamente durante a Black Friday e removê-los quando a demanda cair. Qual benefício da nuvem é esse?

A. Governança
B. Previsibilidade
C. Portabilidade
D. Elasticidade

D7 · Descrever o gerenciamento e a governança do Azure

Uma empresa quer desconto assumindo um gasto fixo por hora em computação por um ou três anos, podendo trocar tamanhos de VM e regiões. Qual opção atende?

A. Reserva de VM de um tamanho e região fixos
B. Máquinas Virtuais Spot do Azure
C. Plano de economia do Azure para computação
D. Orçamento criado no Cost Management

D8 · Descrever o gerenciamento e a governança do Azure

Um banco de dados de produção não pode ser excluído por engano, nem mesmo por quem tem permissão de Proprietário. Qual recurso ajuda nesse caso?

A. Alerta de custo do Cost Management
B. Tag de recurso com o valor produção
C. Bloqueio de recurso do tipo CanNotDelete
D. Recomendação do Azure Advisor

D9 · Descrever o gerenciamento e a governança do Azure

Um projeto de testes terminou, e todos os seus recursos estão em um único grupo de recursos. Qual é a forma mais simples de removê-los?

A. Mover os recursos para outro grupo e esperar
B. Aplicar uma tag de exclusão em cada recurso
C. Excluir a assinatura inteira da empresa no portal
D. Excluir o grupo de recursos inteiro

01

CAPÍTULO 1 · 35-40% DA PROVA

Descrever a arquitetura e os serviços do Azure

Este é o domínio mais pesado (35-40%) e o mais largo: infraestrutura física (regiões, pares, zonas), hierarquia de organização, computação, rede, armazenamento, identidade e segurança. A prova traz um requisito bem específico e quatro serviços do Azure como alternativas, e quase sempre três deles servem para outra coisa; preciso saber a função de cada serviço em uma frase. Onde mais erro: redundância do armazenamento (GRS x RA-GRS x GZRS), camadas de acesso (Cold x Archive), VPN x ExpressRoute, ACI x AKS x Container Apps e os produtos do Microsoft Entra (Connect, Domain Services, External ID). No RBAC, a herança para baixo e o acesso negado por padrão derrubam muita gente.

Neste capítulo
18 tópicos-chave · 14 pegadinhas · 8 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Regiões, regiões emparelhadas, regiões soberanas e serviços globais

A maioria dos recursos é regional e a disponibilidade dos serviços varia de uma região para outra; a escolha considera latência, conformidade, serviços disponíveis e preço. Pares de regiões ficam em geral a pelo menos 300 milhas e servem para priorizar a recuperação e escalonar as atualizações. Regiões soberanas são instâncias isoladas: Azure Government para órgãos dos EUA e Azure na China operado pela 21Vianet. Microsoft Entra ID, Azure Front Door, Traffic Manager e Azure DNS são globais.

Zonas de disponibilidade e conjuntos de disponibilidade

Zonas são datacenters fisicamente separados na mesma região, com energia, rede e refrigeração independentes; regiões com zonas têm no mínimo três e protegem contra a falha de um datacenter. Serviço zonal (como uma VM) fica fixo em uma zona; serviço com redundância de zona (como o ZRS) se replica entre zonas automaticamente. Sem zonas, o conjunto de disponibilidade distribui VMs por domínios de falha (racks com energia e rede próprias) e domínios de atualização, protegendo contra falhas de hardware e manutenções, mas não contra falha regional.

Grupos de gerenciamento e assinaturas

Hierarquia: grupo de gerenciamento raiz > grupos de gerenciamento > assinaturas > grupos de recursos > recursos. Grupos de gerenciamento aplicam políticas e RBAC a várias assinaturas de uma vez; admitem até seis níveis de profundidade (sem contar a raiz e as assinaturas) e até 10 mil grupos por diretório. A assinatura é o limite de cobrança e de acesso; uma conta pode ter várias assinaturas, e cada assinatura confia em um único locatário.

Grupos de recursos e recursos

Recurso é qualquer item gerenciável, como VM, rede ou banco. O grupo de recursos é um contêiner lógico: cada recurso pertence a um único grupo, grupos não podem ser aninhados, recursos podem ser movidos e excluir o grupo exclui tudo dentro dele. Grupos de recursos ficam dentro de uma única assinatura.

Máquinas virtuais e variações

Criar uma VM gera recursos associados: disco gerenciado do SO, interface de rede ligada a uma rede virtual e, opcionalmente, IP público e NSG. Conjuntos de dimensionamento de VMs rodam muitas VMs idênticas com balanceamento e escala automática e podem ser distribuídos entre zonas. O Host Dedicado do Azure oferece servidor físico exclusivo para conformidade e isolamento; VMs Spot usam capacidade ociosa compartilhada.

Azure Virtual Desktop

Entrega desktops Windows centralizados na nuvem, acessíveis de vários dispositivos, com os dados na nuvem. Suporta Windows 11 e Windows 10 multissessão: várias sessões de usuários na mesma VM reduzem custo. Com RemoteApp, publica só um aplicativo, sem entregar o desktop completo.

Contêineres: ACI, AKS e Container Apps

Contêineres virtualizam o SO, compartilham o kernel do host, iniciam em segundos e são mais leves que VMs, mas as VMs isolam mais. Azure Container Instances é a forma mais simples de rodar um contêiner, sem VM nem orquestrador. AKS é Kubernetes gerenciado para orquestrar muitos contêineres, com administração de cluster e nós; Azure Container Apps é plataforma sem servidor para microsserviços, com escala por eventos, inclusive até zero, sem gerenciar cluster.

Serviço de Aplicativos, Azure Functions e Logic Apps

O Serviço de Aplicativos (App Service) é PaaS para aplicativos web (.NET, Java, Node.js, Python), APIs REST, WebJobs e back-ends móveis, em Windows ou Linux, com escala automática, slots de implantação e certificados gerenciados. Azure Functions é serverless orientado a código, acionado por gatilhos como HTTP, filas, blobs e temporizador, cobrado por execução. Logic Apps é serverless orientado a fluxos, com designer visual e conectores prontos.

Rede virtual, sub-redes, NSG e emparelhamento

A rede virtual é privada, isolada e regional, com espaço de endereços privado (como 10.0.0.0/16) dividido em sub-redes; sub-redes da mesma rede já se comunicam pelas rotas do sistema. O NSG tem regras de permissão e negação de entrada e saída e é associado a sub-redes ou interfaces de rede. O emparelhamento liga redes virtuais (regional ou global) pelo backbone da Microsoft, nunca sub-redes da mesma rede.

Gateway de VPN e ExpressRoute

O Gateway de VPN envia tráfego criptografado (IPsec) pela internet pública: site a site liga uma rede inteira, como uma filial; ponto a site liga um único computador, como o notebook de quem está em home office. O ExpressRoute é uma conexão privada com a Microsoft que não passa pela internet, estabelecida por meio de um provedor de conectividade parceiro; o ExpressRoute Direct é a opção dedicada de alta capacidade.

Azure DNS, ponto de extremidade privado, Bastion, Firewall e DDoS

O Azure DNS hospeda zonas públicas e privadas (vinculadas a redes virtuais), mas não registra domínios nem emite certificados. Ponto de extremidade privado (Private Link) dá a um serviço, como uma conta de armazenamento, um IP privado na rede virtual. O Azure Bastion permite RDP e SSH pelo navegador, via TLS, sem IP público nas VMs; o Azure Firewall é firewall gerenciado, com estado e centralizado para várias redes; o Azure DDoS Protection protege contra negação de serviço distribuída.

Conta de armazenamento

Reúne Blob Storage (objetos, imagens, vídeos, backups), Azure Files (compartilhamentos SMB e NFS), Queue Storage (mensagens assíncronas entre componentes) e Table Storage (dados NoSQL chave-atributo); discos de VM são outro serviço, o Azure Managed Disks (HDD Standard, SSD Standard, SSD Premium, Ultra). A recomendada para a maioria dos cenários é a Standard de uso geral v2. O nome tem de 3 a 24 caracteres, só letras minúsculas e números, e é único em todo o Azure porque compõe o endereço, como contoso.blob.core.windows.net.

Camadas de acesso de blobs

Hot (frequente), Cool (esporádica) e Cold (fria) são online; Archive é offline e exige reidratar o blob para uma camada online antes de ler, o que pode levar horas. Quanto mais fria, menor o custo de armazenamento e maior o custo de acesso; Cool, Cold e Archive têm períodos mínimos de 30, 90 e 180 dias, com cobrança por exclusão antecipada. Políticas de gerenciamento do ciclo de vida movem blobs entre camadas automaticamente.

Redundância do armazenamento

LRS: três cópias síncronas em um datacenter, menor custo, sem proteção contra perda do datacenter. ZRS: cópias síncronas em três zonas da região primária. GRS: LRS na primária + cópia assíncrona em região secundária, acessível só após failover; GZRS: três zonas na primária + cópia para a secundária. RA-GRS e RA-GZRS permitem ler a secundária a qualquer momento, sem esperar o failover.

Movimentação e migração de dados

AzCopy copia arquivos para o Storage por linha de comando e scripts; o Azure Storage Explorer é a interface gráfica local (Windows, macOS, Linux) e usa o AzCopy por baixo. O Azure File Sync centraliza arquivos no Azure Files com cache em servidores Windows das filiais. A família Azure Data Box transfere fisicamente grandes volumes quando a rede é lenta, e o Azure Migrate descobre, avalia e migra servidores em um só lugar.

Microsoft Entra ID e serviços relacionados

O Entra ID é serviço de identidade na nuvem, baseado em protocolos web, sem controladores de domínio do cliente e sem GPOs e OUs nativos; o locatário é a instância dedicada do Entra ID da organização. O Microsoft Entra Connect (ou Cloud Sync) sincroniza usuários e grupos do AD local para a identidade híbrida. O Entra Domain Services oferece LDAP e Kerberos gerenciados para aplicações legadas; o Entra External ID atende parceiros (colaboração B2B com as próprias credenciais) e consumidores (login com redes sociais).

Autenticação, MFA, sem senha e Acesso Condicional

Autenticação (AuthN) confirma quem é; autorização (AuthZ) define o que pode fazer. MFA combina fatores de tipos diferentes (algo que você sabe, tem e é); métodos sem senha são Windows Hello para Empresas, Microsoft Authenticator e chaves FIDO2, sendo FIDO2 resistente a phishing. O Acesso Condicional usa sinais como usuário, localização/IP, estado do dispositivo, aplicativo e risco para permitir, bloquear ou exigir MFA, e exige licença premium; sem ela, os padrões de segurança ativam MFA básica e bloqueiam autenticação herdada. SSO e redefinição de senha por autoatendimento completam o pacote.

RBAC, Zero Trust e defesa em profundidade

No RBAC o acesso é negado por padrão e só existe com função atribuída; atribuições são herdadas para baixo, do grupo de gerenciamento até o recurso (menor escopo). Funções básicas: Proprietário (tudo, inclusive conceder acesso), Colaborador (tudo, menos conceder acesso) e Leitor (só visualizar); quando nenhuma serve, cria-se função personalizada. Zero Trust: verificar explicitamente, privilégio mínimo e presumir violação. Defesa em profundidade, de fora para dentro: física, identidade e acesso, perímetro (DDoS, firewall de borda), rede, computação, aplicação e dados; o Microsoft Defender for Cloud avalia a postura (Secure Score, baseado no Microsoft Cloud Security Benchmark) no Azure, local e outras nuvens.

Macetes para memorizar

Redundância

L = Local (1 datacenter), Z = Zonas, G = Geo (outra região), GZ = os dois; RA na frente = Read Access na secundária.

Camadas de blob

Mais fria: guarda barato, lê caro. Cool/Cold/Archive = 30/90/180 dias. Archive: reidratar antes de ler.

Hierarquia

Grupo de gerenciamento > assinatura > grupo de recursos > recurso; permissão desce, nunca sobe.

Defesa em profundidade

De fora para dentro: Físico, Identidade, Perímetro, Rede, Computação, Aplicação, Dados (dados no centro).

Zero Trust

Verificar sempre, privilégio mínimo, presumir violação.

AuthN x AuthZ

AuthN: quem é você. AuthZ: o que você pode fazer.

Sem senha

Hello, Authenticator e FIDO2 (a chave física resistente a phishing).

VPN

Ponto a site = um ponto (notebook); site a site = um site inteiro (filial). Sem internet = ExpressRoute.

Tabela de memorização: não confunda

Quando é...	...e quando é
VPN site a site Túnel IPsec criptografado que passa pela internet pública, ligando uma rede local inteira à rede virtual.	**ExpressRoute** Conexão privada que não passa pela internet, contratada por meio de um provedor de conectividade parceiro.
Grupo de segurança de rede (NSG) Regras básicas de permissão e negação aplicadas a uma sub-rede ou interface de rede.	**Azure Firewall** Firewall gerenciado, com estado e inteligência contra ameaças, para filtrar de forma centralizada o tráfego entre várias redes virtuais e a internet.
Azure Container Instances Rodar um contêiner rápido e simples, sem VM e sem orquestrador.	**AKS / Container Apps** Orquestrar dezenas de microsserviços: AKS com Kubernetes gerenciado e controle do cluster; Container Apps sem gerenciar cluster, com escala até zero.
Azure Functions Escrever código disparado por eventos (HTTP, fila, blob, temporizador).	**Logic Apps** Montar fluxos de integração em designer visual com conectores prontos.

Zonas de disponibilidade Sobreviver à falha de um datacenter inteiro dentro da região.	**Conjunto de disponibilidade** Região sem zonas: proteger contra falha de rack/hardware e manutenções planejadas com domínios de falha e de atualização.
Camada Cool/Cold Dados raros que precisam ser lidos na hora; Cold é a online mais barata para retenção de 90 dias ou mais.	**Camada Archive** Backups raramente acessados em que esperar horas pela reidratação é aceitável; menor custo de armazenamento e leitura mais cara.
Funções do Microsoft Entra Controlar o acesso a recursos do diretório, como usuários e grupos.	**Funções do RBAC do Azure** Controlar o acesso a recursos do Azure, como VMs e contas de armazenamento.

Números que caem

Item	Valor
Zonas de disponibilidade em uma região que oferece o recurso	**no mínimo três**
Profundidade da hierarquia de grupos de gerenciamento	**até seis níveis (sem contar o grupo raiz e as assinaturas)**
Grupos de gerenciamento por diretório	**até 10 mil**
Distância típica entre regiões emparelhadas	**pelo menos 300 milhas**
Nome da conta de armazenamento	**3 a 24 caracteres, só minúsculas e números, único em todo o Azure**
Período mínimo das camadas Cool, Cold e Archive	**30, 90 e 180 dias**
Cópias do LRS	**três cópias síncronas em um único datacenter**
Faixas privadas usadas em redes virtuais	**10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16**
Ponto de extremidade de blobs da conta contoso	**contoso.blob.core.windows.net**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Pedir emparelhamento, IP público ou Gateway de VPN para duas VMs em sub-redes da mesma rede virtual conversarem.
Como não cair: Sub-redes da mesma rede virtual já se comunicam; emparelhamento é entre redes virtuais, e para restringir usa-se NSG.

⚠ **Alerta de prova:** Escolher Archive para dados raros que precisam ser lidos na hora, por ser a camada mais barata.
Como não cair: Archive é offline e exige reidratação que pode levar horas; leitura imediata pede Cool ou Cold.

⚠ **Alerta de prova:** Achar que a camada Hot cobra multa por exclusão antes de 30 dias.
Como não cair: Exclusão antecipada vale para Cool (30), Cold (90) e Archive (180 dias).

⚠ **Alerta de prova:** Marcar GRS para ler a região secundária antes do failover.
Como não cair: No GRS a cópia secundária só fica acessível após o failover; leitura a qualquer momento é RA-GRS ou RA-GZRS.

⚠ **Alerta de prova:** Achar que ZRS protege contra a queda de uma região inteira.
Como não cair: ZRS fica nas zonas da mesma região; zonas + outra região é GZRS.

⚠ **Alerta de prova:** Aceitar nomes de conta de armazenamento com hífen, sublinhado ou maiúsculas, ou achar que a unicidade é por assinatura ou grupo de recursos.
Como não cair: Só minúsculas e números, de 3 a 24 caracteres, únicos em todo o Azure.

⚠ **Alerta de prova:** Escolher Container Instances para orquestrar dezenas de microsserviços, ou AKS para rodar um contêiner simples.
Como não cair: ACI é contêiner individual sem orquestração; orquestração é AKS (ou Container Apps sem cluster).

⚠ **Alerta de prova:** Achar que conjunto de disponibilidade protege contra falha regional, exclusão acidental ou DDoS.
Como não cair: Ele protege contra falhas de hardware e manutenções no datacenter; região exige outra região, exclusão pede bloqueios e backups, DDoS pede DDoS Protection.

⚠ **Alerta de prova:** Escolher Acesso Condicional para um locatário sem licença premium que quer MFA rápida para todos.
Como não cair: Acesso Condicional exige licença premium; sem ela, use os padrões de segurança do Entra ID.

⚠ **Alerta de prova:** Considerar SMS ou senha + data de nascimento como autenticação sem senha ou MFA.
Como não cair: SMS é segundo fator, não sem senha; MFA exige fatores de tipos diferentes, e data de nascimento ou segunda senha são o mesmo tipo (algo que você sabe).

⚠ **Alerta de prova:** Achar que um usuário novo do locatário vê os recursos como Leitor por padrão.
Como não cair: No RBAC o acesso é negado até haver atribuição de função em algum escopo.

⚠ **Alerta de prova:** Dar Colaborador para quem precisa conceder acesso, ou Proprietário para resolver falta de função adequada.
Como não cair: Entre as funções básicas, só o Proprietário concede acesso; se nenhuma função interna serve, crie uma função personalizada e respeite o privilégio mínimo.

⚠ **Alerta de prova:** Achar que o Azure DNS registra novos domínios ou emite certificados.
Como não cair: O Azure DNS hospeda a zona; o domínio é comprado em um registrador.

⚠ **Alerta de prova:** Achar que contêineres isolam mais que VMs ou que cada um tem SO completo.
Como não cair: Contêineres compartilham o kernel do host; quem tem SO completo e isolamento mais forte é a VM.

Como cai na prova

📝 **Como cai:** Requisito de conectividade com quatro serviços de rede nas alternativas.
Como resolver: Identifique origem e destino: um computador (ponto a site), uma rede local (site a site ou ExpressRoute, conforme passe ou não pela internet), duas redes virtuais (emparelhamento), serviço PaaS por IP privado (ponto de extremidade privado), administração de VM sem IP público (Bastion).

📝 **Como cai:** Cenário de armazenamento com frequência de acesso, prazo de leitura e tolerância a falhas.
Como resolver: Decida a camada pela frequência e pela necessidade de leitura imediata (Archive só se horas forem aceitáveis) e a redundância pelo tamanho da falha: disco/servidor (LRS), datacenter (ZRS), região (GRS/GZRS), leitura na secundária (RA-).

📝 **Como cai:** Cenário de identidade pede o produto do Entra certo.
Como resolver: Sincronizar AD local = Connect; LDAP/Kerberos legado = Domain Services; parceiros ou consumidores = External ID; MFA por contexto = Acesso Condicional; MFA sem licença premium = padrões de segurança; menos chamados de senha = autoatendimento.

📝 **Como cai:** Pergunta de RBAC sobre função, escopo ou herança.
Como resolver: Escolha a menor função no menor escopo; lembre que a atribuição vale para o escopo e todos os filhos, que, entre as funções básicas, só o Proprietário concede acesso e que sem atribuição não há acesso.

📝 **Como cai:** Requisito de resiliência pede o recurso certo.
Como resolver: Falha de rack/manutenção sem zonas = conjunto de disponibilidade; falha de datacenter = zonas de disponibilidade; falha de região = outra região (par de regiões); escala + resiliência = conjunto de dimensionamento entre zonas.

📝 **Como cai:** Escolha do serviço de computação por cenário.
Como resolver: Controle do SO = VM; muitas VMs iguais com escala = conjunto de dimensionamento; web/API gerenciada = App Service; evento/agendamento = Functions; fluxo visual = Logic Apps; contêiner simples = ACI; Kubernetes = AKS; desktop ou app Windows remoto = AVD.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
RDP/SSH pelo portal sem expor VMs com IP público	**Azure Bastion**
Conexão privada com o datacenter, sem passar pela internet	**Azure ExpressRoute (via provedor de conectividade)**
Filial com túnel IPsec criptografado pela internet	**Gateway de VPN site a site**
Funcionário em home office conectando o notebook à rede virtual	**VPN ponto a site**
Redes virtuais em regiões diferentes pelo backbone da Microsoft	**Emparelhamento global de redes virtuais**
Acessar conta de armazenamento por IP privado, sem endpoint público	**Ponto de extremidade privado**
Nomes internos entre redes virtuais sem expor na internet	**Zonas privadas do Azure DNS**
VMs em servidor físico exclusivo por conformidade	**Host Dedicado do Azure**
Centenas de VMs idênticas que aumentam e diminuem com a carga	**Conjuntos de dimensionamento de VMs**
Aplicação legada com LDAP e Kerberos, sem controladores de domínio próprios	**Microsoft Entra Domain Services**
Mesmas credenciais no AD local e no Entra ID	**Microsoft Entra Connect**
Consultores de parceiro com as próprias credenciais; consumidores com Google/Facebook	**Microsoft Entra External ID (B2B; para clientes)**
Muitos TB para enviar e internet lenta	**Azure Data Box**
Arquivos centralizados no Azure Files com cache nas filiais	**Azure File Sync**

🎯 Se você lembrar de só uma coisa deste capítulo...

- Archive é offline: reidratar antes de ler; leitura imediata e barata para dado raro é Cold.
- GRS só lê a secundária após failover; RA-GRS lê a qualquer momento; GZRS = zonas + outra região.
- ExpressRoute não passa pela internet; VPN passa, criptografada.
- RBAC: negado por padrão, herdado para baixo; entre as funções básicas, só o Proprietário concede acesso.
- Acesso Condicional exige licença premium; sem ela, padrões de segurança.

Essenciais para a prova (checklist)

☐ Sei a diferença entre região, par de regiões, região soberana e zona de disponibilidade.

☐ Sei a ordem da hierarquia do Azure e o que cada nível faz (políticas em escala, cobrança e acesso, ciclo de vida).

☐ Sei escolher entre VM, conjunto de dimensionamento, Host Dedicado, App Service, Functions, Logic Apps, ACI, AKS, Container Apps e AVD.

☐ Sei escolher entre VPN ponto a site, VPN site a site, ExpressRoute, emparelhamento, ponto de extremidade privado e Bastion.

☐ Sei para que servem Blob, Files, Queue, Table e Disks e as regras de nome da conta de armazenamento.

☐ Sei comparar Hot, Cool, Cold e Archive em custo, acesso e período mínimo.

☐ Sei o que LRS, ZRS, GRS, GZRS e as variantes RA protegem.

☐ Sei associar Entra Connect, Domain Services, External ID, Acesso Condicional e padrões de segurança aos seus cenários.

☐ Sei as funções Proprietário, Colaborador e Leitor, a herança de escopo e quando criar função personalizada.

☐ Sei a ordem das camadas da defesa em profundidade e os três princípios do Zero Trust.

Questões de revisão do capítulo

R1.1 · Descrever a arquitetura e os serviços do Azure

Qual serviço fornece os discos de sistema operacional e de dados para as máquinas virtuais do Azure?

A. Azure Managed Disks
B. Azure Table Storage
C. Azure Queue Storage
D. Azure DNS privado

R1.2 · Descrever a arquitetura e os serviços do Azure

No modelo Confiança Zero (Zero Trust), o que significa o princípio de presumir a violação?

A. Confiar em quem está dentro da rede corporativa da empresa
B. Segmentar o acesso para limitar o alcance de um possível ataque
C. Dispensar a verificação de dispositivos gerenciados pela TI
D. Liberar o acesso depois que o usuário entra pela primeira vez

R1.3 · Descrever a arquitetura e os serviços do Azure

Qual é a diferença entre o Azure Functions e os Aplicativos Lógicos do Azure?

A. O Functions usa VMs; o Logic Apps usa clusters Kubernetes
B. O Functions roda código; o Logic Apps monta fluxos em designer
C. O Functions usa designer; o Logic Apps exige código compilado
D. O Functions é IaaS; o Logic Apps é um serviço de SaaS pronto

R1.4 · Descrever a arquitetura e os serviços do Azure

Uma aplicação precisa ler os dados da região secundária mesmo antes de um failover da conta de armazenamento. Qual opção de redundância permite isso?

A. Geográfica com acesso de leitura (RA-GRS)
B. Redundância de zona (ZRS)
C. Geográfica sem acesso de leitura (GRS)
D. Redundância local (LRS)

Respostas comentadas

R1.1. A) Azure Managed Disks

Por quê: Azure Disks oferece discos gerenciados de diferentes desempenhos, como HDD Standard, SSD Standard, SSD Premium e Ultra.

✗ B) Incorreta. O Table Storage guarda dados NoSQL.
✗ C) Incorreta. O Queue Storage guarda mensagens.
✗ D) Incorreta. O Azure DNS resolve nomes.

> **Dica de prova:** Disco de VM: Azure Disks.

R1.2. B) Segmentar o acesso para limitar o alcance de um possível ataque

Por quê: Os princípios do Zero Trust são verificar explicitamente, usar acesso com privilégio mínimo e presumir a violação, limitando o raio de impacto.

✗ A) Incorreta. O Zero Trust não confia na rede como perímetro.
✗ C) Incorreta. Dispositivos também são verificados.
✗ D) Incorreta. A verificação é contínua, não só na primeira entrada.

> **Dica de prova:** Presumir violação: segmentar e limitar o estrago.

R1.3. B) O Functions roda código; o Logic Apps monta fluxos em designer

Por quê: Os dois são sem servidor. O Azure Functions é orientado a código; o Logic Apps é orientado a fluxos de trabalho, com designer e conectores prontos.

✗ A) Incorreta. Nenhum dos dois exige gerenciar VMs ou clusters.
✗ C) Incorreta. Os papéis estão invertidos.
✗ D) Incorreta. Os dois são serviços sem servidor.

> **Dica de prova:** Functions: código. Logic Apps: fluxo visual.

R1.4. A) Geográfica com acesso de leitura (RA-GRS)

Por quê: As opções com acesso de leitura (RA-GRS e RA-GZRS) permitem ler da região secundária sem esperar o failover.

✗ B) Incorreta. O ZRS replica só entre zonas da mesma região.
✗ C) Incorreta. No GRS, a cópia secundária só fica acessível após o failover.
✗ D) Incorreta. O LRS não tem cópia em outra região.

> **Dica de prova:** Ler a região secundária a qualquer momento: RA-GRS.

02

CAPÍTULO 2 · 25-30% DA PROVA

Descrever conceitos de nuvem

Aqui eu preciso dominar o vocabulário básico da nuvem: modelos de implantação (pública, privada, híbrida e multinuvem), modelos de serviço (IaaS, PaaS, SaaS e serverless), responsabilidade compartilhada, CapEx x OpEx e os benefícios da nuvem. A prova quase sempre traz um cenário curto e pede o nome do conceito, então o segredo é ligar a palavra-chave do enunciado ao termo certo. Onde mais erro é na troca de pares parecidos: escalabilidade x elasticidade, scale in x scale down, híbrida x multinuvem, alta disponibilidade x recuperação de desastres. Também caio quando a pergunta é quem é responsável por algo em SaaS ou PaaS: dados, dispositivos, contas e identidades são sempre do cliente. Vale cerca de 25-30% da prova, então cada ponto aqui é barato de ganhar.

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Computação em nuvem e economia de escala

Computação em nuvem é a entrega de serviços de computação, como servidores, armazenamento, bancos de dados, rede, software e análise, pela internet. Software instalado só nos computadores, servidores comprados para o escritório ou técnicos terceirizados no datacenter local não são nuvem. O provedor compra hardware em enorme escala e repassa parte da economia: isso é economia de escala, que reduz o custo por unidade.

Modelo baseado em consumo (pay-as-you-go)

O cliente paga pelos recursos conforme os utiliza, sem custo inicial de infraestrutura e sem contrato mínimo longo. A cobrança acompanha o consumo real no período, e a capacidade acompanha a demanda em vez de ficar ociosa esperando o pico. Permite começar pequeno e parar de pagar se o projeto for encerrado; descontos por compromisso, como reservas, são opcionais.

CapEx e OpEx

CapEx (despesa de capital) é o investimento antecipado em ativos físicos, como servidores, racks, equipamentos de rede e salas refrigeradas, que passam a ser patrimônio e são depreciados ao longo dos anos. OpEx (despesa operacional) é o gasto com serviços conforme o uso, lançado no próprio período em que ocorre, como o consumo mensal de VMs. A nuvem tende a converter gastos de CapEx em OpEx.

Nuvem pública

O provedor é dono da infraestrutura física e a mantém; o cliente não compra, instala nem mantém hardware e não faz investimento inicial. É multilocatário: os recursos físicos são compartilhados por vários clientes, protegidos por isolamento lógico entre locatários (não por datacenter ou servidor separado por cliente). A limitação é ter menos controle sobre o hardware e sua localização física.

Nuvem privada

Recursos usados por uma única organização, com mais controle sobre hardware, segurança e políticas próprias. Pode ficar no datacenter da empresa ou ser hospedada por um provedor, desde que dedicada. O preço é custo inicial maior, mais responsabilidade pela manutenção física e escala limitada ao hardware disponível.

Nuvem híbrida

Combina o ambiente local (ou nuvem privada) com a nuvem pública, operando de forma integrada, e permite decidir onde cada carga roda. Cenários clássicos: manter parte dos dados no datacenter por exigência regulatória, aproveitar um datacenter recém-renovado e absorver picos sazonais na nuvem pública quando a capacidade local acaba (cloud bursting). Não elimina CapEx, porque o ambiente local continua exigindo investimento, e atende IaaS, PaaS e SaaS.

Multinuvem

Uso de mais de um provedor de nuvem pública ao mesmo tempo, por exemplo Azure e outro provedor para aplicações diferentes, sem exigir ambiente local. O Azure Arc ajuda a gerenciar ambientes multinuvem e híbridos a partir do Azure. Não confundir com nuvem soberana, que é uma instância isolada para governos e requisitos nacionais.

Modelo de responsabilidade compartilhada

A responsabilidade do cliente diminui do ambiente local para IaaS, PaaS e SaaS; no local, tudo é da própria organização. Em qualquer modelo de nuvem, informações e dados, dispositivos (móveis e PCs), contas e identidades são sempre do cliente. Segurança física do datacenter, hardware e rede física são sempre do provedor.

IaaS (infraestrutura como serviço)

O provedor gerencia o hardware físico, a rede física e os hosts; o cliente gerencia do sistema operacional para cima: patches do SO, antivírus dentro da VM, aplicações, dados e regras de firewall e controles de rede das VMs. É o modelo de maior controle (e maior responsabilidade) entre os serviços de nuvem. Ideal para lift-and-shift sem mudar a aplicação, instalar drivers ou alterar configurações do SO e cargas legadas; exemplos: Máquinas Virtuais e Hosts Dedicados do Azure.

PaaS (plataforma como serviço)

Plataforma gerenciada para desenvolver ou hospedar aplicações e dados: o provedor cuida do SO, runtime, middleware e patches da plataforma; o cliente cuida do código, das configurações, dos dados, das contas e identidades. Exemplos: Banco de Dados SQL do Azure e Serviço de Aplicativos. Desvantagem: menos controle sobre o SO e o runtime e, em geral, exige adaptar a aplicação.

SaaS (software como serviço)

Software pronto, acessado pelo navegador ou aplicativo, cobrado em geral por assinatura mensal ou anual por usuário; exemplos: Microsoft 365, Dynamics 365, e-mail e CRMs. É o modelo em que o cliente tem a menor parte das responsabilidades: o provedor cuida da aplicação, rede, SO e hardware. Desvantagem: menor possibilidade de personalização; quem acessa o quê (por exemplo, compartilhamento externo) continua sendo decisão do cliente.

Computação sem servidor (serverless)

Os servidores existem, mas o provedor os gerencia, junto com a escala e a disponibilidade; o cliente foca no código e não tem acesso ao SO. A execução é orientada a eventos (filas, timers, HTTP), escala automaticamente e, no plano de consumo, cobra pelas execuções, não pela capacidade reservada. Exemplos no Azure: Azure Functions e Aplicativos Lógicos do Azure (Logic Apps); ideal para demanda irregular.

Alta disponibilidade e SLA

Alta disponibilidade é manter o serviço acessível mesmo com falhas, eliminando pontos únicos de falha com redundância, várias instâncias em zonas diferentes e balanceador. O SLA expressa o percentual de disponibilidade garantido; não define preço, treinamento nem número de administradores, e nunca garante 100%. Cada 9 a mais reduz a indisponibilidade permitida: 99% ≈ 7,2 h/mês, 99,9% ≈ 43 min/mês, 99,99% ≈ 4 min/mês.

Escalabilidade vertical e horizontal

Vertical é mudar o tamanho de uma mesma instância (mais ou menos CPU e memória): scale up e scale down. Horizontal é mudar o número de instâncias: scale out (adicionar) e scale in (remover). A vertical tem teto no tamanho da maior instância e pode causar interrupção; a horizontal cresce somando instâncias, normalmente com balanceamento, e ainda aumenta a disponibilidade.

Elasticidade

É a escalabilidade acontecendo automaticamente, acompanhando a demanda: adicionar servidores na Black Friday e removê-los quando a demanda cai. Dispensa compra antecipada de servidores de reserva, porque os recursos vêm sob demanda. Escalabilidade é poder ajustar; elasticidade é ajustar sozinho.

Confiabilidade e recuperação de desastres

Confiabilidade é a capacidade de um sistema se recuperar de falhas e continuar funcionando; a nuvem ajuda com presença global, zonas e regiões, mas a arquitetura resiliente continua sendo desenhada pelo cliente. Recuperação de desastres restaura o serviço após eventos graves, como perder uma região inteira, replicando dados para outra região com plano de failover. Backup semanal ajuda na recuperação, mas não é disponibilidade contínua.

Previsibilidade

Previsibilidade de desempenho vem de escala automática, balanceamento e alta disponibilidade, mantendo o tempo de resposta estável nos picos. Previsibilidade de custo vem de estimar e acompanhar gastos: calculadora de preços antes da implantação, Cost Management, orçamentos e alertas depois. Desligar o monitoramento de custos reduz a previsibilidade.

Gerenciabilidade, governança e agilidade

Gerenciabilidade inclui gerenciar a nuvem (escala automática, monitoramento, alertas, implantação com modelos) e gerenciar na nuvem (portal, CLI, APIs e PowerShell). Governança é aplicar políticas, modelos padronizados e auditoria para manter padrões e conformidade. Agilidade é provisionar e liberar recursos rapidamente, de semanas para minutos, como em ambientes de teste criados e apagados a cada sprint.

Macetes para memorizar

💡 Sempre do cliente

DDCI é sempre seu: Dados, Dispositivos, Contas e Identidades, em IaaS, PaaS ou SaaS.

💡 Modelos de serviço

IaaS: do SO para cima é seu. PaaS: só código e dados. SaaS: só usar (e cuidar de dados e acessos). Mais controle = mais responsabilidade.

💡 Direções da escala

Up/Down mexe no TAMANHO (vertical); Out/In mexe na QUANTIDADE (horizontal).

💡 SLA

Cada 9 a mais corta a indisponibilidade: 99% ≈ 7,2 h; 99,9% ≈ 43 min; 99,99% ≈ 4 min por mês.

💡 CapEx x OpEx

CapEx = Compra antecipada + depreciação; OpEx = Operação paga no mês pelo que usou.

💡 Híbrida x multinuvem

Híbrida = local + pública. Multi = várias públicas.

💡 Serverless

Servidor existe, mas não é problema seu: evento chega, função roda, você paga quando roda.

Tabela de memorização: não confunda

Quando é...	...e quando é
IaaS Precisa controlar o SO, instalar driver ou software específico, migrar sem alterar a aplicação (lift-and-shift) ou rodar carga legada; o cliente aplica patches do SO.	**PaaS** Quer publicar código ou usar banco gerenciado sem cuidar de SO e servidores; o provedor aplica os patches da plataforma, ao custo de menos controle sobre SO e runtime.
PaaS A empresa desenvolve a própria aplicação e quer só uma plataforma gerenciada para hospedá-la.	**SaaS** A empresa quer usar um software pronto (CRM, e-mail, Microsoft 365) sem desenvolver nem hospedar nada, aceitando pouca personalização.
Nuvem híbrida Há ambiente local ou privado combinado com nuvem pública: dados mantidos localmente por regra, aproveitamento de datacenter existente, picos absorvidos no Azure.	**Multinuvem** Há dois ou mais provedores de nuvem pública ao mesmo tempo, sem exigência de ambiente local.
Nuvem privada Precisa de mais controle e isolamento, recursos dedicados a uma organização (mesmo que no datacenter de um provedor), aceitando custo inicial e escala limitada.	**Nuvem pública** Quer zero investimento inicial, escala rápida, pagamento por uso e manutenção física pelo provedor, aceitando hardware compartilhado e menos controle físico.
Escala vertical (up/down) Troca a VM por outra com mais CPU e memória, ou reduz o tamanho da mesma VM à noite.	**Escala horizontal (out/in)** Adiciona instâncias iguais quando o tráfego cresce ou passa de dez para três instâncias quando a demanda cai.
Escalabilidade O enunciado fala da capacidade de aumentar ou reduzir recursos, vertical ou horizontalmente.	**Elasticidade** O enunciado enfatiza que o ajuste é automático e acompanha a demanda, como na Black Friday.
Alta disponibilidade Manter o serviço no ar em falhas comuns, com várias instâncias em zonas diferentes e balanceador.	**Recuperação de desastres** Voltar a operar após evento grave, como perder a região principal, com dados replicados e plano de failover em outra região.

Números que caem

Item	Valor
SLA de 99% (indisponibilidade máxima por mês)	**cerca de 7,2 horas**
SLA de 99,9% (indisponibilidade máxima por mês)	**cerca de 43 minutos**
SLA de 99,99% (indisponibilidade máxima por mês)	**cerca de 4 minutos**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Marcar nuvem soberana quando a empresa precisa manter dados no próprio datacenter por regulação e usar a nuvem para o resto.
Como não cair: Nuvem soberana é instância isolada para governos e requisitos nacionais; local por regra + nuvem para o resto é nuvem híbrida.

⚠ **Alerta de prova:** Achar que nuvem híbrida exige dois provedores públicos diferentes.
Como não cair: Dois provedores públicos é multinuvem; híbrida é local ou privada + pública.

⚠ **Alerta de prova:** Escolher PaaS ou serverless para migrar servidores rapidamente sem mudar a aplicação.
Como não cair: PaaS costuma exigir adaptar a aplicação e funções exigem reescrever; migrar sem mudar e com controle do SO é IaaS.

⚠ **Alerta de prova:** Achar que nuvem privada só existe no datacenter da própria empresa.
Como não cair: O que define a privada é ser dedicada a uma organização, onde quer que esteja, inclusive no datacenter de um provedor.

⚠ **Alerta de prova:** Considerar colocation como nuvem pública por tirar o servidor do prédio.
Como não cair: Em colocation a empresa aluga o espaço, mas o servidor continua sendo dela; só na nuvem pública o provedor compra e mantém o hardware.

⚠ **Alerta de prova:** Classificar Hosts Dedicados ou o Serviço de Kubernetes do Azure como SaaS ou PaaS só por serem serviços do Azure.
Como não cair: Hosts Dedicados são servidores físicos exclusivos na camada de IaaS; AKS é serviço de contêineres gerenciado; SaaS são produtos prontos como Microsoft 365 e Dynamics 365.

⚠ **Alerta de prova:** Confundir scale down com scale in quando o número de instâncias diminui.
Como não cair: Menos instâncias é scale in (horizontal); instância menor é scale down (vertical).

⚠ **Alerta de prova:** Achar que uma única VM grande com mais memória e processadores é alta disponibilidade.
Como não cair: Uma única VM continua sendo ponto único de falha; alta disponibilidade exige redundância, como várias instâncias em zonas diferentes com balanceador.

⚠ **Alerta de prova:** Acreditar que escalabilidade garante que a aplicação nunca fique indisponível.
Como não cair: Escalabilidade ajusta capacidade à carga; manter o serviço no ar é disponibilidade, outro benefício.

⚠ **Alerta de prova:** Achar que o SLA informa o preço mensal ou que o provedor garante 100% de disponibilidade.
Como não cair: O SLA informa o percentual de disponibilidade garantido, sempre abaixo de 100%.

⚠ **Alerta de prova:** Em SaaS como o Microsoft 365, achar que a Microsoft define quem pode compartilhar arquivos ou que os dados deixam de ser do cliente.
Como não cair: Dados, dispositivos, contas, identidades e configuração de acesso são sempre do cliente; a Microsoft cuida da aplicação, rede, SO e hardware.

⚠ **Alerta de prova:** Achar que, em IaaS, a Microsoft configura as regras de firewall da rede virtual do cliente.
Como não cair: A Microsoft cuida da rede física; as regras e controles de rede das VMs são do cliente em IaaS.

⚠ **Alerta de prova:** Achar que serverless não é cobrado, ou que tem custo fixo mensal.
Como não cair: No plano de consumo paga-se pelas execuções e recursos usados; o plano provisionado é que cobra pela capacidade reservada.

⚠ **Alerta de prova:** Achar que a nuvem pública separa clientes com datacenter, servidor físico ou cabeamento exclusivo.
Como não cair: O padrão é hardware compartilhado com isolamento lógico entre locatários; host dedicado existe, mas como opção paga.

Como cai na prova

📝 **Como cai:** Cenário descreve o que a empresa precisa controlar (ou não) e pede o modelo de serviço.
Como resolver: Pergunte: precisa mexer no SO? IaaS. Só publica código ou usa banco gerenciado? PaaS. Só usa software pronto? SaaS. Código disparado por evento e pago por execução? Serverless.

📝 **Como cai:** Pergunta quem é responsável por algo (patch do SO, firewall, dispositivos, compartilhamento) em um modelo específico.
Como resolver: Físico (datacenter, hardware, rede física) é sempre do provedor; dados, dispositivos, contas e identidades são sempre do cliente; o SO é do cliente em IaaS e do provedor em PaaS e SaaS.

📝 **Como cai:** Cenário curto pede o nome do benefício da nuvem.
Como resolver: Ache a palavra-chave: ajuste automático = elasticidade; estimar custo/desempenho = previsibilidade; voltar a operar após falha = confiabilidade; alertas e escala automática = gerenciabilidade; políticas e conformidade = governança; semanas para minutos = agilidade.

📝 **Como cai:** Cenário mistura local, provedor e governo e pede o modelo de implantação.
Como resolver: Local + pública = híbrida; várias públicas = multinuvem; dedicada a uma organização = privada; requisitos de governo com isolamento = soberana.

📝 **Como cai:** Escolha DUAS sobre CapEx/OpEx, consumo ou nuvem pública.
Como resolver: Elimine as alternativas com compra antecipada, valor fixo, contrato longo ou capacidade para o pico; sobram as de pagar conforme o uso e sem custo inicial.

📝 **Como cai:** Cálculo de indisponibilidade a partir do SLA.
Como resolver: Use a tabela: 99% ≈ 7,2 h, 99,9% ≈ 43 min, 99,99% ≈ 4 min por mês; as alternativas erradas costumam ser os valores dos SLAs vizinhos.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Parte dos dados precisa ficar no datacenter por exigência legal; o resto vai para a nuvem	**Nuvem híbrida**
Datacenter próprio + Azure para absorver picos sazonais quando a capacidade local acaba	**Nuvem híbrida (cloud bursting)**
Azure e outro provedor público ao mesmo tempo	**Multinuvem (gerenciada com Azure Arc)**
Infraestrutura dedicada só a uma empresa, mesmo no datacenter do provedor	**Nuvem privada**
Não quer mais comprar, instalar nem manter hardware	**Nuvem pública**
Migrar sem alterar a aplicação, instalar driver, alterar configurações do SO	**IaaS com máquinas virtuais**
Publicar código ou usar banco/análise gerenciados sem cuidar de SO e servidores	**PaaS**
Software pronto pelo navegador, CRM, e-mail, assinatura por usuário	**SaaS**
Eventos, mensagens de fila, demanda irregular, pagar só pelas execuções	**Serverless (Azure Functions)**
Fluxo montado em designer visual com conectores (e-mail, SharePoint, SaaS)	**Aplicativos Lógicos do Azure (Logic Apps)**
Levar ambientes VMware ao Azure sem refatorar e com as mesmas ferramentas	**Azure VMware Solution**

Adicionar e remover servidores automaticamente conforme a demanda	**Elasticidade**
Estimar custo e desempenho; calculadora, orçamentos e alertas	**Previsibilidade**
Escala automática e alertas de saúde; portal, CLI, APIs, PowerShell; implantar com modelos	**Gerenciabilidade (políticas e conformidade = governança)**

🎯 Se você lembrar de só uma coisa deste capítulo...

- Dados, dispositivos, contas e identidades são do cliente em qualquer modelo; segurança física é sempre do provedor.
- Nuvem privada pode estar no datacenter do provedor: o que importa é ser dedicada a uma organização.
- Scale in/out = quantidade de instâncias; scale up/down = tamanho da instância.
- Serverless = provedor gerencia servidores, escala por eventos e cobra por execução (Functions e Logic Apps).
- A nuvem converte CapEx em OpEx; OpEx é lançado no período, CapEx é depreciado.

Essenciais para a prova (checklist)

☐ Sei classificar Máquinas Virtuais e Hosts Dedicados como IaaS, Banco de Dados SQL e Serviço de Aplicativos como PaaS, e Microsoft 365 e Dynamics 365 como SaaS.

☐ Sei dizer o que é do cliente e o que é do provedor em local, IaaS, PaaS e SaaS.

☐ Sei diferenciar nuvem pública, privada, híbrida, multinuvem e soberana a partir de um cenário.

☐ Sei diferenciar scale up, scale down, scale out e scale in.

☐ Sei diferenciar escalabilidade de elasticidade e alta disponibilidade de recuperação de desastres.

☐ Sei classificar um gasto como CapEx ou OpEx e explicar por que a nuvem favorece OpEx.

☐ Sei converter 99%, 99,9% e 99,99% em indisponibilidade aproximada por mês.

☐ Sei associar previsibilidade, gerenciabilidade, governança, confiabilidade e agilidade às suas palavras-chave.

☐ Sei por que serverless combina com eventos e demanda irregular e como ele é cobrado.

Questões de revisão do capítulo

R2.1 · Descrever conceitos de nuvem

Qual é uma vantagem da nuvem privada em relação à nuvem pública?

A. Manutenção do hardware feita pelo provedor
B. Controle maior sobre o hardware e a segurança
C. Nenhum investimento inicial em infraestrutura
D. Escala praticamente ilimitada sob demanda

R2.2 · Descrever conceitos de nuvem

Uma empresa quer levar servidores locais para a nuvem rapidamente, sem alterar as aplicações e mantendo controle do sistema operacional. Qual modelo de serviço é mais adequado?

A. IaaS, com máquinas virtuais
B. SaaS, com software pronto
C. PaaS, com serviço de aplicativos
D. Serverless, com funções

R2.3 · Descrever conceitos de nuvem

Qual das opções é um exemplo de despesa operacional (OpEx)?

A. Construir uma sala refrigerada para servidores
B. Adquirir equipamentos de rede com depreciação
C. Comprar racks de servidores para o datacenter
D. Pagar todo mês pelo consumo de VMs no Azure

R2.4 · Descrever conceitos de nuvem

Uma equipe cria ambientes de teste temporários com VMs e os apaga no fim de cada sprint. Qual vantagem da nuvem está sendo aproveitada?

A. Manter hardware próprio disponível para uso exclusivo da equipe
B. Evitar qualquer custo, pois ambientes de teste são sempre gratuitos
C. Comprar licenças perpétuas antes de cada novo ambiente de teste
D. Provisionar e liberar recursos rapidamente, pagando pelo uso

Respostas comentadas

R2.1. B) Controle maior sobre o hardware e a segurança

Por quê: A nuvem privada oferece mais controle e isolamento, ao custo de investimentos, manutenção e escala limitada à capacidade adquirida.

✗ A) Incorreta. Na nuvem privada local, a manutenção é da própria empresa.
✗ C) Incorreta. A nuvem privada costuma exigir investimento inicial.
✗ D) Incorreta. A escala da nuvem privada é limitada pelo hardware disponível.

> **Dica de prova:** Nuvem privada: mais controle, mais custo e menos escala.

R2.2. A) IaaS, com máquinas virtuais

Por quê: Migrações lift-and-shift são um caso típico de IaaS, porque mantêm a aplicação e o sistema operacional como estão.

✗ B) Incorreta. SaaS substitui a aplicação por um software pronto.
✗ C) Incorreta. PaaS costuma exigir adaptar a aplicação.
✗ D) Incorreta. Funções exigem reescrever a aplicação.

> **Dica de prova:** Migrar sem mudar a aplicação: IaaS.

R2.3. D) Pagar todo mês pelo consumo de VMs no Azure

Por quê: OpEx é o gasto com serviços ou produtos conforme o uso, lançado no período. CapEx é o investimento antecipado em infraestrutura física.

✗ A) Incorreta. Construir instalações é despesa de capital.
✗ B) Incorreta. Equipamentos depreciados são despesa de capital.
✗ C) Incorreta. Comprar servidores é despesa de capital.

> **Dica de prova:** Paga no mês pelo que usou: OpEx.

R2.4. D) Provisionar e liberar recursos rapidamente, pagando pelo uso

Por quê: A agilidade da nuvem permite experimentar e descartar ambientes rapidamente, com custo proporcional ao uso.

✗ A) Incorreta. A nuvem evita manter hardware próprio.
✗ B) Incorreta. Recursos de teste também geram custo enquanto existem.
✗ C) Incorreta. Licenças perpétuas não combinam com ambientes temporários.

> **Dica de prova:** Ambiente temporário: criar, usar, apagar e pagar pelo uso.

03

CAPÍTULO 3 · 30-35% DA PROVA

Descrever o gerenciamento e a governança do Azure

Aqui eu preciso saber qual ferramenta resolve cada problema de custo, governança, gerenciamento e monitoramento: Azure Policy, bloqueios, tags, Purview, Service Trust Portal, Resource Manager, ARM/Bicep, Arc, Advisor, Service Health, Azure Monitor e Cost Management. Vale 30-35% e o estilo é quase sempre ferramenta x ferramenta: o enunciado descreve um objetivo e as alternativas trazem serviços vizinhos que fazem outra coisa. Onde mais erro é no comportamento fino: o que um Deny faz com recursos que já existem, o que ReadOnly bloqueia, se tags são herdadas, o que um orçamento faz ao estourar. Também confundo Advisor (recomendações) com Service Health (incidentes) e calculadora (antes) com Cost Management (depois).

Neste capítulo

18 tópicos-chave · 14 pegadinhas · 8 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Azure Policy: definição, atribuição e iniciativa

A definição descreve a condição e o efeito; a atribuição aplica a definição ou iniciativa a um escopo; a iniciativa agrupa várias políticas para um mesmo objetivo, como tags obrigatórias e regiões permitidas. Na atribuição é possível excluir escopos filhos, e isenções registram exceções com justificativa e prazo. O painel de conformidade mostra o percentual de recursos conformes, e as iniciativas internas de conformidade regulatória mapeiam controles de normas como a ISO 27001.

Efeitos do Azure Policy

Audit só registra a não conformidade; Deny bloqueia criações e alterações fora do padrão; Modify altera propriedades, como adicionar tags; DeployIfNotExists implanta o que falta, como configurar backup; AuditIfNotExists só registra que o recurso relacionado não existe; Disabled desativa a política. Recursos já existentes fora da regra são marcados como não conformes, nunca excluídos, movidos ou desligados. As políticas valem para todos, inclusive Proprietários.

Bloqueios de recurso

CanNotDelete impede a exclusão, mas permite alterações; ReadOnly impede alterações no plano de controle, inclusive iniciar, parar e reiniciar uma VM. Valem até para administradores, podem ser aplicados a assinaturas, grupos de recursos ou recursos e são herdados pelos escopos abaixo. Criar ou remover bloqueios exige Microsoft.Authorization/locks, presente em Proprietário e Administrador de Acesso do Usuário, não em Colaborador.

Tags (marcas)

Pares nome e valor para organizar recursos, ratear custos por projeto ou centro de custo e identificar recursos para automação, como desligar VMs. Não são herdadas do grupo de recursos por padrão; para padronizar, usa-se Azure Policy (exigir com Deny ou adicionar com Modify). Tags não controlam acesso, não impedem exclusão, não criptografam, não geram alertas e não têm custo.

Microsoft Purview

Reúne governança de dados e soluções de risco e conformidade para dados no Azure, ambientes locais e outras nuvens. O Mapa de Dados cataloga, classifica e mostra a linhagem; rótulos de confidencialidade classificam documentos e aplicam proteção como criptografia; a prevenção contra perda de dados (DLP) evita compartilhar informações confidenciais por engano. O Compliance Manager dá pontuação de conformidade e ações recomendadas por regulamento, como a LGPD.

Portal de Confiança do Serviço

O Service Trust Portal reúne relatórios de auditoria independentes, certificados ISO e documentos sobre como a Microsoft protege os dados na nuvem. É onde o auditor encontra a documentação de conformidade da própria Microsoft. Não gera alertas operacionais nem métricas.

Azure Resource Manager

É a camada de implantação e gerenciamento: toda operação de criar, atualizar e excluir recursos passa por ele, com RBAC, tags, bloqueios e modelos. Em modelos, identifica as dependências e cria os recursos na ordem certa, em paralelo quando independentes. A operação what-if mostra o que será criado, alterado ou excluído antes de implantar; a região de um grupo de recursos só guarda os metadados, e os recursos podem estar em outras regiões.

Infraestrutura como código: modelos ARM e Bicep

Modelos ARM são arquivos JSON declarativos; o Bicep é uma linguagem mais simples que gera modelos ARM, e as implantações continuam passando pelo Resource Manager. A implantação é idempotente: reaplicar o modelo mantém iguais os recursos já conformes. Arquivos de parâmetros por ambiente reaproveitam o mesmo modelo, módulos Bicep reaproveitam definições entre equipes, exportar o modelo de um grupo de recursos transforma o que existe em código, e guardar no Git permite versionar e revisar mudanças.

Ferramentas de gerenciamento

O portal do Azure roda no navegador, de qualquer rede, permite criar, configurar e excluir recursos e montar painéis personalizados. O Cloud Shell roda no navegador, já autenticado, com Bash ou PowerShell e as ferramentas instaladas, sem licença por usuário. Azure CLI usa comandos az (az vm create); Azure PowerShell usa cmdlets Verbo-AzSubstantivo (New-AzVM); o aplicativo móvel permite ver alertas e reiniciar VMs pelo celular.

Azure Arc

Estende o Azure Resource Manager, o gerenciamento e a governança do Azure para servidores, Kubernetes e SQL Server fora do Azure: datacenter local, borda e outras nuvens. Permite vê-los no portal e aplicar as mesmas políticas sem migrá-los. Quem migra é o Azure Migrate.

Azure Advisor

Analisa configuração e uso dos recursos e dá recomendações personalizadas em cinco categorias: confiabilidade, segurança, desempenho, custo e excelência operacional, com base no Well-Architected Framework. Exemplo típico: VM com uso muito baixo de CPU por semanas, recomendação de redimensionar ou desligar. O Advisor Score mede o quanto os recursos seguem essas boas práticas; o Advisor não aplica regras nem informa incidentes.

Azure Service Health

Combina três visões, da mais ampla à mais específica: Azure Status (página pública, sem login, status global), Service Health (incidentes, manutenções planejadas e avisos de integridade, como descontinuações, para os serviços e regiões que você usa) e Resource Health (saúde de uma VM ou banco específico). Permite configurar alertas para ser avisado de eventos que afetem seus serviços. Não mostra métricas de CPU nem recomendações de economia.

Azure Monitor: métricas, logs e ferramentas

Métricas são números no tempo, vistos em gráficos no Metrics Explorer; logs são registros detalhados, consultados com KQL no Log Analytics, cujo custo depende do volume ingerido e retido. Logs de recurso não são coletados por padrão e exigem configurações de diagnóstico; dados de dentro do SO convidado exigem o Agente do Azure Monitor e uma regra de coleta; o log de atividades registra quem fez o quê no plano de controle. Workbooks são relatórios interativos, e VM insights e Container insights dão visões prontas.

Alertas do Azure Monitor

Há alertas de métrica (como CPU acima de 90% por 10 minutos), de pesquisa de logs (consultas KQL avaliadas em intervalos) e de log de atividades (como exclusão de uma VM). Alertas de métrica podem usar limites estáticos ou dinâmicos, que aprendem o padrão histórico, inclusive sazonal. O grupo de ações define o que acontece quando o alerta dispara: SMS, e-mail, webhooks, runbooks e funções.

Application Insights

Recurso do Azure Monitor para monitoramento de desempenho de aplicações (APM): tempo de resposta, falhas e dependências de uma aplicação em produção. Os testes de disponibilidade acessam a aplicação a partir de vários pontos do mundo e alertam em caso de falha.

Fatores de custo

Influenciam o custo: tipo e tamanho do recurso, consumo, região (energia, impostos e mão de obra variam), largura de banda (em geral entrada gratuita e saída cobrada), modelo de compra, tipo de assinatura (créditos, cotas, contratos) e itens do Azure Marketplace, cuja licença pode vir na fatura do Azure além dos recursos usados. Na armazenagem, camada e redundância mudam o preço do mesmo volume. Grupos de recursos e grupos de gerenciamento não cobram; VM parada e desalocada deixa de cobrar computação, mas discos (e, conforme o caso, IPs públicos) continuam, inclusive se esquecidos após excluir a VM.

Modelos de compra e descontos

Pagamento conforme o uso tem o maior preço por hora e nenhum compromisso. Reservas do Azure dão desconto para cargas estáveis com compromisso de um ou três anos, vinculadas a tipo de recurso e região; o plano de economia para computação troca um gasto fixo por hora por desconto aplicado automaticamente, com flexibilidade de tamanho e região. VMs Spot usam capacidade ociosa, com menor preço, para cargas interrompíveis; o Benefício Híbrido reaproveita licenças de Windows Server e SQL Server com Software Assurance; os preços de Dev/Teste atendem assinantes do Visual Studio fora de produção.

Calculadora de preços e Microsoft Cost Management

A calculadora de preços estima custos antes da implantação; o Cost Management acompanha e analisa os gastos reais, com tendência, previsão até o fim do período e filtros por escopo, serviço e tag. Orçamentos disparam alertas ao atingir limites, mas por padrão não desligam nada nem bloqueiam a assinatura; ações automáticas só com grupos de ações. Exportações agendadas (diárias, semanais ou mensais) enviam os dados de custo para uma conta de armazenamento.

Macetes para memorizar

Quem controla o quê

RBAC = quem pode; Policy = como o recurso deve ser; Bloqueio = não mexa nele; Tag = etiqueta para organizar e ratear.

Efeitos do Policy

Audit aponta, Deny barra, Modify ajusta (tags), DeployIfNotExists implanta o que falta.

Saúde

Status = mundo (público); Service Health = meus serviços e regiões; Resource Health = meu recurso.

Custo antes x depois

Calculadora antes, Cost Management depois; orçamento avisa, não desliga.

Descontos

Estável e longo = reserva; gasto por hora flexível = plano de economia; interrompível = Spot; licença própria = Benefício Híbrido; não produção = Dev/Teste.

Linha de comando

az minúsculo = Azure CLI; Verbo-AzSubstantivo (New-AzVM) = Azure PowerShell.

Categorias do Advisor

Cinco: confiabilidade, segurança, desempenho, custo e excelência operacional.

Largura de banda

Dado entra de graça, sai pagando.

Tabela de memorização: não confunda

Quando é...	...e quando é
Azure Policy Definir como os recursos devem ser: regiões permitidas, SKUs permitidos, tags obrigatórias.	**RBAC** Definir quem pode fazer o quê; mesmo com permissão no RBAC, um Deny do Policy ainda nega.
Azure Policy Avaliar propriedades e conformidade dos recursos em escala.	**Bloqueio de recurso** Impedir exclusão (CanNotDelete) ou alteração (ReadOnly) acidental de um recurso, grupo ou assinatura.
CanNotDelete O recurso pode ser alterado, mas não excluído, como um banco de produção.	**ReadOnly** Nada pode ser alterado até a janela de mudança, nem reiniciar uma VM; só leitura.
Calculadora de preços Estimar o custo mensal antes de migrar ou implantar.	**Cost Management** Acompanhar gasto real, tendência, previsão do mês, orçamentos com alertas e exportações.
Azure Advisor Recomendações de boas práticas (custo, segurança, confiabilidade, desempenho, excelência operacional).	**Azure Service Health** Incidentes, manutenções planejadas e avisos de descontinuação que afetam seus serviços e regiões.

Reservas do Azure Mesmas VMs rodando de forma estável por um ou três anos.	**VMs Spot** Processamento em lote ou testes que toleram interrupção, buscando o menor preço.
Métricas Números no tempo para gráficos rápidos (Metrics Explorer) e alertas de métrica.	**Logs** Registros detalhados consultados com KQL no Log Analytics e alertas de pesquisa de logs.

Números que caem

Item	Valor
Compromisso das reservas e do plano de economia	**um ou três anos**
Frequência das exportações agendadas de custo	**diárias, semanais ou mensais**
Categorias de recomendação do Azure Advisor	**cinco**
Tipos de bloqueio de recurso	**dois: CanNotDelete e ReadOnly**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Criar tag de exceção ou bloqueio para tirar um grupo de recursos do alcance de uma política.
Como não cair: Use exclusão na atribuição da política (ou isenção com justificativa e prazo).

⚠ **Alerta de prova:** Achar que uma política Deny exclui, move ou desliga recursos que já existiam fora do padrão.
Como não cair: Recursos existentes só são marcados como não conformes; o Deny barra novas criações e alterações.

⚠ **Alerta de prova:** Achar que o Proprietário da assinatura escapa de um Deny do Azure Policy.
Como não cair: RBAC e Policy são verificações separadas e as duas precisam passar; a política vale para todos.

⚠ **Alerta de prova:** Achar que CanNotDelete impede alterações ou que ReadOnly permite reiniciar a VM.
Como não cair: CanNotDelete só impede excluir; ReadOnly nega até iniciar, parar e reiniciar.

⚠ **Alerta de prova:** Achar que um bloqueio no grupo de recursos não vale para os recursos dentro dele.
Como não cair: Bloqueios são herdados pelos escopos abaixo.

⚠ **Alerta de prova:** Achar que o Colaborador pode criar e remover bloqueios.
Como não cair: Exige Microsoft.Authorization/locks: Proprietário ou Administrador de Acesso do Usuário.

⚠ **Alerta de prova:** Achar que recursos herdam automaticamente as tags do grupo de recursos.
Como não cair: Não herdam por padrão; só com política configurada (Modify).

⚠ **Alerta de prova:** Achar que estourar o orçamento bloqueia a assinatura ou desliga VMs.
Como não cair: O orçamento só envia alertas; ações automáticas exigem grupo de ações configurado.

⚠ **Alerta de prova:** Usar a calculadora de preços para ver a fatura real ou a tendência do mês.
Como não cair: A calculadora só estima; gasto real e previsão estão no Cost Management.

⚠ **Alerta de prova:** Procurar incidentes no Advisor, ou CPU da VM no Service Health.
Como não cair: Incidentes e manutenções = Service Health; recomendações = Advisor; métricas = Azure Monitor.

⚠ **Alerta de prova:** Escolher Azure Migrate para governar servidores locais sem migrá-los.
Como não cair: Governar fora do Azure sem migrar é Azure Arc; Migrate é para migrar.

⚠ **Alerta de prova:** Escolher AuditIfNotExists para configurar automaticamente o backup que falta.
Como não cair: AuditIfNotExists só registra; quem implanta o que falta é DeployIfNotExists.

⚠ **Alerta de prova:** Achar que VM parada e desalocada zera a cobrança, ou que excluir a VM elimina todo o custo dela.
Como não cair: Desalocada, a computação para de cobrar, mas os discos gerenciados (e, conforme o caso, IPs públicos) continuam; após excluir a VM, discos e IPs esquecidos seguem gerando custo.

⚠ **Alerta de prova:** Achar que a entrada de dados é cobrada e a saída é gratuita.
Como não cair: Em geral é o inverso: entrada gratuita, saída para a internet cobrada.

Como cai na prova

📝 **Como cai:** Objetivo de governança com Policy, bloqueio, tag e RBAC nas alternativas.
Como resolver: Pergunte o verbo: impor regra de configuração = Policy; impedir excluir/alterar = bloqueio; ratear ou automatizar = tag; dar permissão a pessoa = RBAC.

📝 **Como cai:** O que acontece quando... (Deny em recursos existentes, ReadOnly e reiniciar, tag no grupo, orçamento estourado, bloqueio no grupo).
Como resolver: Lembre do comportamento padrão: não conforme sem exclusão; operação negada; sem herança de tag; só alertas; bloqueio herdado.

📝 **Como cai:** Problema de monitoramento pede a ferramenta certa.
Como resolver: Incidente do Azure = Service Health; boas práticas = Advisor; métrica em gráfico = Metrics Explorer; logs com KQL = Log Analytics; quem fez o quê = log de atividades; aplicação = Application Insights; dados do SO convidado = Agente do Azure Monitor.

📝 **Como cai:** Cenário de custo pede ferramenta ou modelo de compra.
Como resolver: Estimar = calculadora; real, previsão, orçamento, exportação = Cost Management; carga estável = reserva; interrompível = Spot; licenças existentes = Benefício Híbrido; depois explique a diferença pelos fatores de custo (região, saída de dados, camada, redundância).

📝 **Como cai:** Infraestrutura como código e ferramentas de gerenciamento.
Como resolver: Repetível e versionado = ARM/Bicep; mesmo modelo com valores diferentes = parâmetros; reuso = módulos; prévia = what-if; JSON = ARM; sintaxe mais simples = Bicep; sem instalar nada = Cloud Shell.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Regiões permitidas, tamanhos de VM permitidos, tag obrigatória em todas as assinaturas	**Azure Policy (atribuído em grupo de gerenciamento)**
Agrupar várias políticas e atribuir juntas	**Iniciativa de política**
Ver nível de conformidade com uma norma como ISO 27001	**Iniciativas de conformidade regulatória do Azure Policy**
Relatórios de auditoria independentes e certificados ISO da Microsoft	**Portal de Confiança do Serviço**
Pontuação de conformidade e ações para regulamento como a LGPD	**Compliance Manager do Purview**
Classificar documento como Confidencial com criptografia; impedir vazamento de números de cartão	**Rótulos de confidencialidade; DLP do Purview**
Mapa, classificação e linhagem dos dados da organização	**Microsoft Purview**
Servidores, Kubernetes ou SQL Server locais ou em outra nuvem com as mesmas políticas, sem migrar	**Azure Arc**

VM ociosa, recomendação para reduzir custo	**Azure Advisor**
Incidente, manutenção planejada ou descontinuação que afeta meus recursos	**Azure Service Health (alertas e avisos de integridade)**
Ser avisado quando alguém excluir uma VM	**Alerta sobre o log de atividades**
Tempo de resposta, falhas e dependências da aplicação web; site responde de vários lugares	**Application Insights (testes de disponibilidade)**
Ver o que será criado, alterado ou excluído antes de implantar	**Operação what-if**
Licenças Windows Server/SQL Server com Software Assurance; gasto fixo por hora com flexibilidade	**Benefício Híbrido do Azure; plano de economia para computação**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Deny não apaga nada que já existe: só marca como não conforme e barra o novo.
- ReadOnly impede até reiniciar a VM; CanNotDelete só impede excluir; bloqueios são herdados e valem até para Proprietários.
- Tags não são herdadas por padrão e não controlam acesso.
- Orçamento só alerta; calculadora só estima; Cost Management mostra o real.
- Arc governa sem migrar; Migrate migra.

Essenciais para a prova (checklist)

☐ Sei diferenciar definição, atribuição, iniciativa, exclusão e isenção no Azure Policy.

☐ Sei o efeito de Audit, Deny, Modify, DeployIfNotExists, AuditIfNotExists e Disabled.

☐ Sei a diferença entre CanNotDelete e ReadOnly e quem pode gerenciar bloqueios.

☐ Sei quando usar Purview (Mapa de Dados, rótulos, DLP, Compliance Manager) e o Portal de Confiança do Serviço.

☐ Sei o papel do Resource Manager, a relação entre Bicep e ARM e o que é idempotência e what-if.

☐ Sei identificar Azure CLI e Azure PowerShell pelo formato do comando e o que o Cloud Shell oferece.

☐ Sei separar Advisor, Service Health (Status, Service Health, Resource Health) e Azure Monitor.

☐ Sei escolher entre alertas de métrica, de pesquisa de logs e de log de atividades e para que serve o grupo de ações.

☐ Sei listar os fatores de custo e o que continua cobrando com a VM desalocada.

☐ Sei escolher entre pagamento por uso, reserva, plano de economia, Spot, Benefício Híbrido e Dev/Teste.

Questões de revisão do capítulo

R3.1 · Descrever o gerenciamento e a governança do Azure

Um auditor precisa acessar relatórios de auditoria independentes, certificados ISO e documentos de conformidade dos serviços de nuvem da Microsoft. Onde ele encontra esse material?

A. No Portal de Confiança do Serviço
B. No painel do Cost Management
C. No Azure Advisor da assinatura
D. Na Integridade de Recursos da VM

R3.2 · Descrever o gerenciamento e a governança do Azure

Um grupo de recursos tem a tag Projeto=Alpha. O que acontece com os recursos criados dentro dele?

A. São movidos para uma assinatura com o mesmo nome da tag
B. Herdam a tag automaticamente, sem nenhuma configuração adicional
C. Não herdam a tag automaticamente, salvo uma política configurada
D. Ficam bloqueados até receberem a mesma tag do grupo de recursos

R3.3 · Descrever o gerenciamento e a governança do Azure

A equipe quer um alerta que aprenda o padrão histórico de uma métrica e ajuste o limite sozinho, sem definir um valor fixo. Qual opção atende?

A. Limites dinâmicos no alerta de métrica da VM
B. Orçamento com alerta no Cost Management
C. Marca de alerta aplicada ao recurso
D. Bloqueio CanNotDelete na métrica da VM

R3.4 · Descrever o gerenciamento e a governança do Azure

Uma VM tem um bloqueio ReadOnly. O que acontece quando um administrador tenta reiniciá-la pelo portal?

A. A VM reinicia, pois o bloqueio só impede excluir
B. A VM reinicia, e o bloqueio é removido junto
C. A operação é negada enquanto houver o bloqueio
D. A operação é adiada para a próxima manutenção

Respostas comentadas

R3.1. A) No Portal de Confiança do Serviço

Por quê: O Portal de Confiança do Serviço (Service Trust Portal) reúne relatórios de auditoria, certificações e documentos sobre como a Microsoft protege os dados na nuvem.

✗ B) Incorreta. O Cost Management trata de custos.
✗ C) Incorreta. O Advisor dá recomendações sobre os recursos do cliente.
✗ D) Incorreta. A Integridade de Recursos mostra o estado de recursos específicos.

> **Dica de prova:** Relatórios de auditoria e certificados da Microsoft: Service Trust Portal.

R3.2. C) Não herdam a tag automaticamente, salvo uma política configurada

Por quê: Para padronizar tags, é comum usar políticas que herdam ou exigem tags. Por padrão, recursos não herdam as tags do grupo.

✗ A) Incorreta. Tags não movem recursos.
✗ B) Incorreta. A herança não é automática.
✗ D) Incorreta. Recursos não ficam bloqueados por falta de tag.

> **Dica de prova:** Tags não são herdadas por padrão.

R3.3. A) Limites dinâmicos no alerta de métrica da VM

Por quê: Alertas de métrica podem usar limites estáticos ou dinâmicos. Os dinâmicos aprendem o comportamento da métrica, inclusive padrões sazonais.

✗ B) Incorreta. Orçamentos tratam de custo.
✗ C) Incorreta. Marcas não disparam alertas.
✗ D) Incorreta. Bloqueios não geram alertas.

> **Dica de prova:** Limite que se ajusta sozinho: limites dinâmicos.

R3.4. C) A operação é negada enquanto houver o bloqueio

Por quê: O bloqueio ReadOnly permite só leituras no plano de controle. Operações como iniciar, parar e reiniciar uma VM são bloqueadas até o bloqueio ser removido.

✗ A) Incorreta. Quem só impede exclusões é o CanNotDelete.
✗ B) Incorreta. O bloqueio não é removido automaticamente.
✗ D) Incorreta. A operação é negada, não adiada.

> **Dica de prova:** ReadOnly: nem reiniciar a VM.

DIA DA PROVA

Estratégia de prova

O AZ-900 cobra reconhecimento: dado um objetivo de negócio curto, qual conceito, serviço ou ferramenta do Azure o atende. As alternativas erradas costumam ser serviços reais do Azure que resolvem outro problema, então quem sabe a função de cada um em uma frase elimina três opções rapidamente. Há itens de múltipla escolha e de múltipla resposta (escolha duas), e os de múltipla resposta misturam afirmações verdadeiras com inversões sutis, como trocar o papel de dois serviços. A prova também testa comportamento padrão (o que acontece quando), escopo e herança, além de pares que se parecem: VPN x ExpressRoute, GRS x RA-GRS, Advisor x Service Health, calculadora x Cost Management. Não é preciso configurar nada, mas é preciso saber exatamente o limite de cada serviço.

Como responder

✓ Gerencie o tempo: a Microsoft não divulga o número exato de itens (fica entre 40 e 60); conte com cerca de 50 em 45 minutos, menos de um minuto por item; marque os duvidosos e volte no fim.

✓ Pontuação de 1 a 1000 com mínimo de 700: mire em acertar com folga o domínio de arquitetura e serviços (35-40%), que é o mais pesado.

✓ Leia o enunciado procurando a palavra-chave decisiva (sem internet, sem IP público, sem migrar, automaticamente, antes de implantar, só apontar) antes de olhar as alternativas.

✓ Elimine primeiro as alternativas que são serviços reais de outra área: se a pergunta é de governança, descarte DNS, Bastion e Files; se é de rede, descarte Advisor e Policy.

✓ Em múltipla resposta, avalie cada afirmação isoladamente como verdadeira ou falsa e desconfie de frases com papéis invertidos ou com 'sempre', 'nunca', '100%' e 'só'.

✓ Quando o enunciado pede menor custo, menor esforço ou privilégio mínimo, escolha a opção mais simples que atende, não a mais poderosa (ACI antes de AKS, Leitor antes de Colaborador, LRS se a falha é só de disco).

✓ Em perguntas de responsabilidade compartilhada, ancore-se nas regras fixas: físico é sempre do provedor; dados, dispositivos, contas e identidades são sempre do cliente.

✓ Em perguntas de escopo, desenhe mentalmente a hierarquia (grupo de gerenciamento > assinatura > grupo de recursos > recurso): RBAC, Policy e bloqueios descem; tags não.

Erros que derrubam candidatos

✗ Escolher o serviço mais avançado em vez do que o requisito pede, como AKS para um contêiner simples ou ExpressRoute para um notebook.

✗ Confundir pares de vocabulário: scale in x scale down, escalabilidade x elasticidade, híbrida x multinuvem, autenticação x autorização.

✗ Achar que Archive lê na hora, que GRS lê a secundária antes do failover ou que ZRS protege contra falha regional.

✗ Atribuir a uma ferramenta de governança o papel de outra: tag protegendo contra exclusão, bloqueio substituindo permissão, orçamento desligando VMs.

✗ Trocar Advisor por Service Health, calculadora por Cost Management ou Arc por Migrate.

✗ Esquecer comportamentos padrão: RBAC nega por padrão, tags não são herdadas, Deny não apaga recursos existentes, ReadOnly impede reiniciar VM.

✗ Achar que em SaaS ou PaaS o cliente deixa de ser responsável pelos dados e pelas identidades.

Na semana da prova

- ☐ Revise as comparações e as pegadinhas dos três capítulos até explicar cada par sem consultar.
- ☐ Refaça os simulados completos com cronômetro de 45 minutos e anote cada erro como 'confundi X com Y'.
- ☐ Monte uma folha de uma página com redundância (LRS/ZRS/GRS/GZRS/RA), camadas de blob (30/90/180 dias), tabela do SLA e efeitos do Policy, e releia todo dia.
- ☐ Repasse os gatilhos de rede e identidade, que concentram muitos serviços parecidos.
- ☐ Na véspera, revise só os itens de 'lembrar' de cada capítulo e descanse; no dia, leia cada enunciado até o fim antes de marcar.

REVISÃO FINAL

Folha de cola

Leia na véspera e na manhã da prova: os gatilhos e as pegadinhas mais importantes de cada domínio.

1. Descrever a arquitetura e os serviços do Azure

‣ RDP/SSH pelo portal sem expor VMs com IP público → **Azure Bastion**

‣ Conexão privada com o datacenter, sem passar pela internet → **Azure ExpressRoute (via provedor de conectividade)**

‣ Filial com túnel IPsec criptografado pela internet → **Gateway de VPN site a site**

‣ Funcionário em home office conectando o notebook à rede virtual → **VPN ponto a site**

‣ Redes virtuais em regiões diferentes pelo backbone da Microsoft → **Emparelhamento global de redes virtuais**

⚠ Sub-redes da mesma rede virtual já se comunicam; emparelhamento é entre redes virtuais, e para restringir usa-se NSG.

⚠ Archive é offline e exige reidratação que pode levar horas; leitura imediata pede Cool ou Cold.

⚠ Exclusão antecipada vale para Cool (30), Cold (90) e Archive (180 dias).

2. Descrever conceitos de nuvem

‣ Parte dos dados precisa ficar no datacenter por exigência legal; o resto vai para a nuvem → **Nuvem híbrida**

‣ Datacenter próprio + Azure para absorver picos sazonais quando a capacidade local acaba → **Nuvem híbrida (cloud bursting)**

‣ Azure e outro provedor público ao mesmo tempo → **Multinuvem (gerenciada com Azure Arc)**

‣ Infraestrutura dedicada só a uma empresa, mesmo no datacenter do provedor → **Nuvem privada**

‣ Não quer mais comprar, instalar nem manter hardware → **Nuvem pública**

⚠ Nuvem soberana é instância isolada para governos e requisitos nacionais; local por regra + nuvem para o resto é nuvem híbrida.

⚠ Dois provedores públicos é multinuvem; híbrida é local ou privada + pública.

⚠ PaaS costuma exigir adaptar a aplicação e funções exigem reescrever; migrar sem mudar e com controle do SO é IaaS.

3. Descrever o gerenciamento e a governança do Azure

‣ Regiões permitidas, tamanhos de VM permitidos, tag obrigatória em todas as assinaturas → **Azure Policy (atribuído em grupo de gerenciamento)**

‣ Agrupar várias políticas e atribuir juntas → **Iniciativa de política**

‣ Ver nível de conformidade com uma norma como ISO 27001 → **Iniciativas de conformidade regulatória do Azure Policy**

‣ Relatórios de auditoria independentes e certificados ISO da Microsoft → **Portal de Confiança do Serviço**

‣ Pontuação de conformidade e ações para regulamento como a LGPD → **Compliance Manager do Purview**

⚠ Use exclusão na atribuição da política (ou isenção com justificativa e prazo).

⚠ Recursos existentes só são marcados como não conformes; o Deny barra novas criações e alterações.

⚠ RBAC e Policy são verificações separadas e as duas precisam passar; a política vale para todos.

GABARITO

Respostas do diagnóstico

D1. C) Camada fria (Cold) → revise o capítulo 1

Por quê: As camadas online são Hot, Cool e Cold. A Archive é offline. Para dados raros com leitura imediata e retenção de 90 dias ou mais, a Cold é a opção online mais barata.

✗ A) Incorreta. A camada Archive é offline e exige reidratação, que pode levar horas.

✗ B) Incorreta. A camada Hot tem armazenamento mais caro, indicado para acesso frequente.

✗ D) Incorreta. O desempenho premium serve para baixa latência, com custo maior.

> **Dica de prova:** Raro, mas precisa ler na hora: Cool ou Cold, nunca Archive.

D2. B) Azure Virtual Desktop → revise o capítulo 1

Por quê: O Azure Virtual Desktop centraliza desktops na nuvem, com suporte a várias sessões e acesso de vários dispositivos.

✗ A) Incorreta. O Container Instances executa contêineres.

✗ C) Incorreta. O App Service hospeda aplicações web.

✗ D) Incorreta. O Functions executa código orientado a eventos.

> **Dica de prova:** Desktop Windows na nuvem: Azure Virtual Desktop.

D3. D) Redefinição de senha por autoatendimento → revise o capítulo 1

Por quê: O Microsoft Entra ID oferece recursos de identidade como SSO, MFA, acesso condicional e redefinição de senha por autoatendimento.

✗ A) Incorreta. Grupos de gerenciamento organizam assinaturas.

✗ B) Incorreta. Bloqueios protegem recursos.

✗ C) Incorreta. O emparelhamento conecta redes.

> **Dica de prova:** Menos chamados de senha: redefinição por autoatendimento.

D4. C) Previsibilidade de desempenho → revise o capítulo 2

Por quê: A previsibilidade de desempenho na nuvem vem de recursos como escala automática, balanceamento e alta disponibilidade.

✗ A) Incorreta. CapEx é despesa de capital, não benefício de desempenho.

✗ B) Incorreta. Nuvem privada é um modelo de implantação.

✗ D) Incorreta. Soberania trata de leis e localização dos dados.

> **Dica de prova:** Desempenho estável nos picos: previsibilidade.

D5. C) Modelo baseado em consumo → revise o capítulo 2

Por quê: A computação em nuvem usa um modelo baseado em consumo: a empresa paga pelo que usa e evita despesas antecipadas com infraestrutura.

✗ A) Incorreta. Comprar servidores é despesa de capital, o oposto do objetivo.
✗ B) Incorreta. Um contrato longo de hardware dedicado é um compromisso fixo.
✗ D) Incorreta. Licenças perpétuas envolvem pagamento antecipado, não cobrança por uso.

> **Dica de prova:** Pagar só pelo que usa: modelo baseado em consumo.

D6. D) Elasticidade → revise o capítulo 2

Por quê: Escalabilidade é a capacidade de aumentar ou reduzir recursos. Elasticidade é fazer isso automaticamente, acompanhando a demanda.

✗ A) Incorreta. Governança trata de políticas e controles.
✗ B) Incorreta. Previsibilidade trata de desempenho e custo previsíveis.
✗ C) Incorreta. Portabilidade não é o benefício descrito.

> **Dica de prova:** Ajuste automático à demanda: elasticidade.

D7. C) Plano de economia do Azure para computação → revise o capítulo 3

Por quê: O plano de economia para computação troca um compromisso de gasto por hora por descontos, aplicados automaticamente em vários serviços de computação.

✗ A) Incorreta. A reserva é vinculada a um tipo de recurso e região.
✗ B) Incorreta. As VMs Spot usam capacidade ociosa, sem compromisso.
✗ D) Incorreta. Um orçamento não gera desconto.

> **Dica de prova:** Compromisso de gasto por hora, com flexibilidade: plano de economia.

D8. C) Bloqueio de recurso do tipo CanNotDelete → revise o capítulo 3

Por quê: Bloqueios de recursos podem ser CanNotDelete, que impede a exclusão, ou ReadOnly, que impede alterações. Eles valem até para administradores.

✗ A) Incorreta. Alertas de custo não protegem recursos.
✗ B) Incorreta. Tags só identificam recursos.
✗ D) Incorreta. O Advisor faz recomendações, mas não impede exclusões.

> **Dica de prova:** Evitar exclusão acidental: bloqueio CanNotDelete.

D9. D) Excluir o grupo de recursos inteiro → revise o capítulo 3

Por quê: Grupos de recursos organizam recursos com o mesmo ciclo de vida, o que facilita implantar, gerenciar e excluir tudo junto.

✗ A) Incorreta. Mover recursos não os remove.
✗ B) Incorreta. Tags não excluem recursos.
✗ C) Incorreta. Excluir a assinatura afetaria outros projetos.

> **Dica de prova:** Mesmo ciclo de vida: mesmo grupo de recursos.

Agora, treine no formato real

Faça as 6 provas completas do curso AZ-900: 300 questões inéditas, tempo do exame, explicação de cada alternativa e link da documentação para revisar.

Ver as 6 provas completas e o cupom do mês →

Até o dia da prova, uma revisão por dia no seu feed

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o "não confunda" de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

Material independente de preparação, sem afiliação ou endosso de Microsoft. As questões são inéditas e não reproduzem a prova real.