

Guia de preparação AZ-305

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.

4 capítulos por domínio	**28** 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-305: 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 100 minutos, no formato do exame. Referência de aprovação: 70%.

Domínio (capítulo)	Peso	Neste guia
1. Projetar soluções de armazenamento de dados	20-25%	18 conceitos · 14 pegadinhas
2. Projetar soluções de continuidade de negócios	15-20%	18 conceitos · 13 pegadinhas
3. Projetar soluções de identidade, governança e monitoramento	25-30%	18 conceitos · 14 pegadinhas
4. Projetar soluções de infraestrutura	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 12 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 · Projetar soluções de armazenamento de dados

A equipe de dados quer identificar e rotular colunas com dados sensíveis no Banco de Dados SQL, com relatórios e integração à auditoria. O que recomendar?

A. Ajuste automático do banco
B. Máscara dinâmica de dados nas colunas
C. Descoberta e classificação de dados
D. Réplica geográfica legível

D2 · Projetar soluções de armazenamento de dados

Um aplicativo com PostgreSQL precisa de busca por similaridade de embeddings, sem adicionar outro banco de dados. O que recomendar?

A. Filas do Armazenamento
B. Azure Files premium
C. Tabelas do Armazenamento com índices
D. Extensão pgvector no servidor flexível

D3 · Projetar soluções de armazenamento de dados

Um data lake terá zonas bruto, refinado e curado, com permissões diferentes por pasta para cada equipe. Qual armazenamento recomendar?

A. Banco de Dados SQL com uma tabela por zona
B. Azure Files premium com uma chave de conta
C. Blobs sem namespace hierárquico com SAS de conta
D. Data Lake Storage com ACLs por pasta

D4 · Projetar soluções de continuidade de negócios

Qual combinação oferece recuperação de desastres regional para um aplicativo web no App Service com Banco de Dados SQL?

A. Backup diário do aplicativo web em outra região
B. Banco SQL com redundância de zona apenas
C. Duas regiões, Front Door e grupo de failover
D. App Service em uma região com dois slots

D5 · Projetar soluções de continuidade de negócios

A conta de armazenamento principal deve ser protegida contra a exclusão acidental do recurso inteiro. O que recomendar?

A. Bloqueio CanNotDelete na conta
B. Exclusão temporária de blobs
C. Camada Cool padrão
D. Redundância LRS

D6 · Projetar soluções de continuidade de negócios

Um SQL Server 2022 local precisa de uma réplica de DR na nuvem, na Instância Gerenciada, com possibilidade de failover. O que recomendar?

A. Link da Instância Gerenciada
B. Backup diário para blobs
C. Exportação BACPAC mensal
D. Site Recovery do servidor

D7 · Projetar soluções de identidade, governança e monitoramento

Assinaturas de sandbox devem permitir experimentos livres, mas sem nenhuma conexão com as redes corporativas. O que recomendar?

A. Assinaturas sandbox no mesmo grupo das de produção
B. Marcas Sandbox nos recursos criados
C. Grupo Sandbox com políticas que negam conexões
D. Revisões de acesso trimestrais

D8 · Projetar soluções de identidade, governança e monitoramento

Em um workspace de testes, um erro de configuração pode gerar ingestão excessiva e uma fatura inesperada. O que recomendar para limitar o custo?

A. Um workspace por VM de teste
B. Mais regras de alerta de log
C. Limite diário de ingestão
D. Retenção interativa maior

D9 · Projetar soluções de identidade, governança e monitoramento

A empresa quer bloquear entradas vindas de países onde não opera, para todos os aplicativos corporativos. O que recomendar?

A. NSG com as faixas de IP desses países
B. Firewall do SQL com lista de países
C. Revisões de acesso mensais
D. Locais nomeados no Acesso Condicional

D10 · Projetar soluções de infraestrutura

O gateway de VPN deve continuar funcionando se uma zona de disponibilidade da região falhar. O que recomendar?

A. Um gateway em cada sub-rede
B. SKU Basic do gateway de VPN
C. Um IP público Basic no gateway
D. SKU com redundância de zona

D11 · Projetar soluções de infraestrutura

VMs VMware devem ser migradas para o Azure sem instalar agentes em cada VM. O que recomendar?

A. Recriar as VMs do zero no Azure
B. Cópia manual dos discos por AzCopy
C. Migração sem agente do Azure Migrate
D. Backup com agente MARS

D12 · Projetar soluções de infraestrutura

Por falhas de rede, o mesmo pedido pode ser enviado duas vezes à fila. Como evitar mensagens duplicadas no próprio agente de mensagens?

A. Event Hubs com mais partições
B. Event Grid com repetição
C. Filas do Armazenamento com retenção longa
D. Detecção de duplicatas do Service Bus

01

CAPÍTULO 1 · 20-25% DA PROVA

Projetar soluções de armazenamento de dados

Aqui preciso casar o tipo de dado e o padrão de acesso com o serviço certo: relacional, documento, chave-valor, grafo, arquivo, bloco ou análise. Para SQL, o eixo é quanto controle preciso: Banco de Dados SQL, Instância Gerenciada ou SQL Server em VM, e depois a camada (General Purpose, Business Critical, Hyperscale, serverless, pool elástico). No Cosmos DB caem API, nível de consistência, chave de partição e modo de capacidade. Erro bastante nas opções de segurança de dados, que parecem iguais: TDE, Always Encrypted, máscara dinâmica, segurança em nível de linha e ledger. No armazenamento, preciso lembrar o que exige namespace hierárquico e qual camada de blob é a mais barata.

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

Tópicos-chave

Banco de Dados SQL, Instância Gerenciada ou SQL Server em VM

Banco de Dados SQL é o PaaS relacional com ACID sem administrar servidores. A Instância Gerenciada é para lift-and-shift em PaaS com recursos de instância: SQL Agent, Database Mail, servidores vinculados, consultas entre bancos e CLR. SQL Server em VM é IaaS, para quando é preciso acesso ao SO, SSRS ou agentes de terceiros.

Modelos de compra vCore x DTU

O vCore oferece General Purpose, Business Critical e Hyperscale, com computação provisionada ou sem servidor, escolha independente de CPU e memória e Benefício Híbrido do Azure. O DTU agrupa recursos e não aceita Benefício Híbrido. Reservas de VM não se aplicam ao Banco de Dados SQL.

Camadas General Purpose, Business Critical e Hyperscale

General Purpose usa armazenamento remoto, com latência maior. Business Critical usa réplicas em grupo de disponibilidade com armazenamento local, menor latência de E/S e uma réplica de leitura incluída. Hyperscale cresce a dezenas de terabytes, com servidores de página e snapshots que deixam backups e restaurações rápidos, e réplicas nomeadas isoladas por equipe.

Escala de leitura no SQL

Em Premium, Business Critical e Hyperscale, conexões com ApplicationIntent=ReadOnly vão para réplicas secundárias, tirando relatórios da réplica de gravação. Para leitores em outro continente, use réplica geográfica legível (replicação geográfica ativa).

Serverless e pool elástico

A camada sem servidor cobra por segundo de vCore usado e, com pausa automática, cobra só armazenamento enquanto pausada; ideal para uso intermitente. Pool elástico compartilha recursos entre muitos bancos com picos em horários diferentes; um banco por cliente em pool equilibra isolamento, restauração individual e custo.

Criptografia no SQL

TDE criptografa em repouso, mas administradores veem os dados; com chave gerenciada pelo cliente no Key Vault, revogar a chave torna o banco inacessível. Always Encrypted criptografa colunas com a chave no cliente, escondendo os dados até do DBA, e exige alterações no cliente; com enclaves seguros permite algumas consultas.

Máscara, RLS, ledger e temporais

Máscara dinâmica mostra só parte do valor nas consultas, sem alterar os dados nem o aplicativo. Segurança em nível de linha filtra linhas por usuário. Tabelas de razão (ledger) geram resumos criptográficos para provar que não houve adulteração, até por administradores. Tabelas temporais mantêm automaticamente o histórico de versões das linhas.

Classificação, auditoria e ajuste automático

Descoberta e classificação rotula colunas sensíveis, e os rótulos aparecem nos logs de auditoria. A auditoria do SQL grava em armazenamento, Log Analytics ou Hubs de Eventos, no nível do servidor ou do banco. O ajuste automático cria e remove índices e força o último plano bom, verificando o impacto.

APIs do Cosmos DB

NoSQL para documentos JSON, com busca vetorial e híbrida. MongoDB para manter drivers e consultas, com arquiteturas RU e vCore (vCore para migrações com consultas complexas). Apache Gremlin para grafos. Table para quem usa Armazenamento de Tabelas e quer distribuição global e SLA de latência. Para Cassandra nativo e híbrido, existe a Instância Gerenciada para Apache Cassandra.

Níveis de consistência do Cosmos DB

Forte, Desatualização limitada, Sessão, Prefixo consistente e Eventual. Sessão é o padrão e garante ler as próprias gravações. Desatualização limitada permite atraso com limite definido em tempo ou versões. Prefixo consistente garante ordem sem limite de atraso; Eventual não garante nem ordem nem as próprias gravações; Forte tem custo e latência maiores.

Particionamento no Cosmos DB

Boa chave de partição tem alta cardinalidade, distribui a carga uniformemente e aparece nos filtros das consultas mais frequentes, como /idUsuario. Cada partição lógica tem limite de 20 GB; chaves de partição hierárquicas, com até três níveis, resolvem clientes grandes em SaaS.

Capacidade e custos no Cosmos DB

Sem servidor cobra só as RUs consumidas, para tráfego baixo e intermitente. Dimensionamento automático varia entre 10% e 100% do máximo para picos sem ajuste manual. Por padrão todas as propriedades são indexadas; excluir caminhos não consultados reduz RU de gravação. TTL apaga itens por prazo usando RU/s restantes.

Recursos do Cosmos DB para integração e segurança

O feed de alterações registra inserções e atualizações em ordem por partição e pode disparar Azure Functions. O RBAC do plano de dados com o Entra ID permite desabilitar a autenticação por chave. Uma região de gravação com regiões de leitura adicionais dá leitura global rápida; os SDKs usam a lista de regiões preferidas.

Armazenamento de Blobs e Data Lake Storage

Camadas Hot, Cool e Archive; Archive é a mais barata, tem período mínimo de 180 dias e exige reidratação antes da leitura. Data Lake Storage é Blob com namespace hierárquico e ACLs POSIX por pasta. SFTP e NFS 3.0 em blobs exigem namespace hierárquico. Escopos de criptografia dão chave própria por contêiner ou blob na mesma conta.

Segurança e escala da conta de armazenamento

Reduza exposição com pontos privados e acesso público bloqueado, acesso anônimo de blob desativado, chave compartilhada desativada, TLS 1.2 e Defender for Storage. Se uma carga ultrapassa os limites de taxa de uma conta, distribua os dados entre contas.

Arquivos e bloco

Azure Files mantém SMB e ACLs NTFS com autenticação do AD DS, do Entra Domain Services ou do Entra Kerberos. Azure NetApp Files entrega NFS de alto desempenho com latência abaixo de milissegundo e snapshots rápidos, como para SAP HANA. Elastic SAN consolida armazenamento em bloco por iSCSI para VMs e AKS.

Discos gerenciados

SSD Premium v2 tem IOPS e taxa de transferência ajustáveis independentemente do tamanho, com custo menor que o Disco Ultra; no SSD Premium v1 o desempenho está ligado ao tamanho. Discos compartilhados, para clusters de failover, funcionam com SSD Premium, SSD Premium v2 e Disco Ultra e exigem software de cluster.

Plataformas de análise e integração

Microsoft Fabric une engenharia, data warehouse (Warehouse com T-SQL e Delta), tempo real e Power BI sobre o OneLake; o espelhamento replica tabelas para o OneLake sem ETL. Databricks oferece Spark, Delta Lake e MLflow. Data Explorer analisa telemetria com KQL. Stream Analytics agrega fluxos em janelas com linguagem parecida com SQL. Data Factory move dados com pipelines e runtime auto-hospedado. Purview cataloga, classifica e mostra linhagem.

Macetes para memorizar

💡 Onde rodar SQL

Banco sozinho = Banco de Dados SQL; precisa da instância (Agent, Mail, servidores vinculados) = Instância Gerenciada; precisa do SO = VM.

💡 Segurança de dados no SQL

TDE = disco; Always Encrypted = cofre até para o DBA; Máscara = tarja; RLS = filtro de linha; Ledger = lacre.

💡 Consistência do Cosmos DB

Do mais forte ao mais fraco: Forte, Limitada, Sessão, Prefixo, Eventual (F-L-S-P-E). Sessão é o padrão.

💡 Chave de partição

Muitos valores, carga uniforme e presente no filtro: se não cumprir os três, a partição esquenta.

💡 Capacidade do Cosmos DB

Pouco e às vezes: sem servidor. Picos variáveis sem ajuste manual: autoscale. Provisionado manual e fixo com carga variável exige ajustes ou paga o pico o tempo todo.

💡 Namespace hierárquico

ACL por pasta, SFTP e NFS 3.0 em blobs: os três exigem namespace hierárquico.

💡 Arquivos

SMB com AD = Azure Files; NFS turbinado = NetApp Files; bloco iSCSI = Elastic SAN.

Tabela de memorização: não confunda

Quando é...	...e quando é

Banco de Dados SQL do Azure Banco relacional PaaS novo, com ACID e junções, sem depender de recursos de instância.	**Instância Gerenciada de SQL** Migração com poucas mudanças de apps que usam SQL Agent, Database Mail, servidores vinculados, consultas entre bancos ou CLR.
Instância Gerenciada de SQL Recursos de instância em PaaS, sem acesso ao SO.	**SQL Server em VM** Precisa do SO: SSRS, agentes de terceiros instalados no servidor ou controle total.
Always Encrypted Esconder colunas sensíveis até dos administradores, com a chave no aplicativo cliente.	**TDE** Criptografia em repouso dos arquivos do banco, com chave da Microsoft ou do cliente no Key Vault.
Máscara dinâmica de dados Mostrar só parte do valor de uma coluna, como os quatro últimos dígitos do cartão.	**Segurança em nível de linha** Filtrar quais linhas cada usuário enxerga.
Consistência Sessão Cada usuário lê as próprias gravações, com menor custo de leitura.	**Desatualização limitada** Leituras em outras regiões aceitam atraso, mas com limite definido em tempo ou versões.
Cosmos DB sem servidor Tráfego baixo e intermitente, pagando só as RUs consumidas.	**Dimensionamento automático** Tráfego variável com picos grandes, sem ajuste manual de RU/s.
Business Critical Menor latência de E/S com réplica somente leitura incluída.	**Hyperscale** Banco de dezenas de terabytes com escala rápida de leitura e backups quase instantâneos.

Números que caem

Item	Valor
Limite de uma partição lógica no Cosmos DB	**20 GB**
Níveis das chaves de partição hierárquicas	**até três**
Faixa do dimensionamento automático no Cosmos DB	**entre 10% e 100% do máximo de RU/s**
Período mínimo da camada Archive	**180 dias, com reidratação antes da leitura**
Conectores do Data Factory	**mais de 90**
Cobrança do SQL sem servidor	**por segundo de vCore usado; pausado cobra só armazenamento**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** TDE para impedir que administradores vejam CPF e cartão.
Como não cair: Com TDE os administradores veem os dados. Esconder até do DBA é Always Encrypted.

⚠ **Alerta de prova:** Always Encrypted para mostrar só os quatro últimos dígitos sem mudar o aplicativo.
Como não cair: Always Encrypted exige alterações no cliente e esconde tudo. Exibição parcial é máscara dinâmica de dados.

⚠ **Alerta de prova:** Máscara dinâmica para classificar colunas, provar integridade ou registrar acessos.
Como não cair: Máscara só esconde valores. Classificar: descoberta e classificação. Provar integridade: ledger. Registrar acessos: auditoria do SQL.

⚠ **Alerta de prova:** Log de atividades da assinatura para saber quem consultou dados do banco.
Como não cair: O log de atividades registra operações de gerenciamento, não consultas. Use auditoria do SQL.

⚠ **Alerta de prova:** Banco de Dados SQL para app que usa SQL Agent e consultas entre bancos.
Como não cair: Recursos de instância apontam para a Instância Gerenciada.

⚠ **Alerta de prova:** Instância Gerenciada quando é preciso instalar agentes no SO ou usar SSRS.
Como não cair: A Instância Gerenciada não permite instalar agentes no SO. Use SQL Server em VM.

⚠ **Alerta de prova:** Modelo DTU ou reserva de VM para usar Benefício Híbrido no SQL.
Como não cair: DTU não aceita Benefício Híbrido e reservas de VM não se aplicam ao Banco de Dados SQL. Use o modelo vCore.

⚠ **Alerta de prova:** Mais RU/s ou TTL curto para resolver o limite de 20 GB por partição lógica.
Como não cair: RU/s não muda o limite e TTL apagaria dados. Use chaves de partição hierárquicas.

⚠ **Alerta de prova:** Chave de partição com poucos valores, como país, status ou data do dia.
Como não cair: Baixa cardinalidade gera partições quentes e data concentra as gravações do dia. Escolha alta cardinalidade, como /idUsuario.

⚠ **Alerta de prova:** Dimensionamento automático com máximo alto para tráfego baixo e intermitente.
Como não cair: O autoscale cobra pelo mínimo do intervalo. Tráfego baixo e intermitente é Cosmos DB sem servidor.

⚠ **Alerta de prova:** Réplica geográfica do SQL ou réplica do PostgreSQL para gravar em várias regiões.
Como não cair: Essas réplicas são somente leitura. Gravação multirregional com documentos é Cosmos DB com gravações em várias regiões.

⚠ **Alerta de prova:** Alta disponibilidade entre zonas no PostgreSQL para tirar relatórios do primário.
Como não cair: O servidor em espera da HA não recebe tráfego. Use réplica de leitura.

⚠ **Alerta de prova:** Blobs sem namespace hierárquico com SAS de conta para permissões por pasta.
Como não cair: Sem namespace hierárquico não há ACLs por pasta. Use Data Lake Storage.

⚠ **Alerta de prova:** Camada Cool para backups de anos que quase nunca são lidos.
Como não cair: Cool é online e custa mais. Leitura rara e espera de horas aceitável: Archive.

Como cai na prova

📝 **Como cai:** Aplicativo existente vai para o Azure com poucas mudanças, citando recursos específicos do mecanismo.
Como resolver: Liste os recursos citados: SQL Agent, Database Mail, servidores vinculados, CLR apontam para Instância Gerenciada; SSRS ou agentes no SO, para VM; MongoDB, Cassandra, MySQL e PostgreSQL ficam no serviço gerenciado do próprio mecanismo. Descarte opções que exigem mudar o modelo de dados.

📝 **Como cai:** Proteção de dados sensíveis em colunas, com um detalhe sobre quem pode ver.
Como resolver: Até o DBA não pode ver: Always Encrypted. Ver só parte: máscara dinâmica. Filtrar linhas: RLS. Revogar acesso ao banco todo: TDE com chave gerenciada pelo cliente. Provar integridade: ledger.

📝 **Como cai:** Cenário do Cosmos DB com consistência, partição ou custo de RU.
Como resolver: Para consistência, procure o detalhe: ler as próprias gravações é Sessão; atraso com limite é Desatualização limitada. Para partição, alta cardinalidade e hierárquica para clientes grandes. Para custo, ajuste a indexação, TTL e o modo de capacidade.

📝 **Como cai:** Escolha de camada ou modelo do Banco de Dados SQL por custo ou desempenho.
Como resolver: Intermitente: serverless. Muitos bancos com picos diferentes: pool elástico. Menor latência e réplica incluída: Business Critical. Dezenas de TB: Hyperscale. Benefício Híbrido: vCore.

📝 **Como cai:** Escolha de armazenamento não relacional por protocolo ou custo.
Como resolver: Identifique o protocolo pedido (SMB, NFS, SFTP, iSCSI) e o padrão de acesso. Chave-valor simples e barato: Tabelas. Retenção longa e leitura rara: Archive. Mídia global: blobs com Front Door.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Uso poucas horas por dia em horários imprevisíveis no SQL	**Camada sem servidor com pausa automática**
Dezenas de bancos SaaS pequenos com picos em horários diferentes	**Pool elástico**
Relatórios na réplica do Business Critical	**ApplicationIntent=ReadOnly na conexão**
Várias equipes de BI com réplicas isoladas do Hyperscale	**Réplicas nomeadas**
Provar criptograficamente que registros não foram adulterados	**Tabelas de razão (ledger)**
Histórico de todas as versões das linhas	**Tabelas temporais do sistema**
Atualizar índice de busca sempre que um documento mudar	**Feed de alterações do Cosmos DB com Azure Functions**
Documentos de sessão expiram e devem ser apagados sozinhos	**TTL no contêiner**
Aplicativos sem as chaves primárias do Cosmos DB	**RBAC do plano de dados com o Entra ID**
Busca vetorial sem adicionar outro banco no PostgreSQL	**Extensão pgvector no servidor flexível**
Parceiros enviam arquivos por SFTP direto para blobs	**Suporte a SFTP no Armazenamento de Blobs**
Servidor de arquivos Windows em PaaS com ACLs NTFS	**Azure Files com autenticação do AD DS**
Tabelas do SQL replicadas para o OneLake sem ETL	**Espelhamento no Microsoft Fabric**
Catálogo, classificação automática e linhagem de dados	**Microsoft Purview**

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

- TDE não esconde dados dos administradores; Always Encrypted esconde.
- Réplicas do SQL e do PostgreSQL são somente leitura; gravar em várias regiões é Cosmos DB.
- Sessão é a consistência padrão do Cosmos DB e garante ler as próprias gravações.
- SFTP, NFS 3.0 e ACLs por pasta em blobs exigem namespace hierárquico.
- Benefício Híbrido no Banco de Dados SQL só no modelo vCore.

Essenciais para a prova (checklist)

- ☐ Sei escolher entre Banco de Dados SQL, Instância Gerenciada e SQL Server em VM.
- ☐ Sei diferenciar General Purpose, Business Critical, Hyperscale, serverless e pool elástico.
- ☐ Sei aplicar TDE, Always Encrypted, máscara dinâmica, RLS, ledger e tabelas temporais ao cenário certo.
- ☐ Sei os cinco níveis de consistência do Cosmos DB e quando usar cada um.
- ☐ Sei escolher uma boa chave de partição e quando usar chaves hierárquicas.
- ☐ Sei escolher entre provisionado, autoscale e sem servidor no Cosmos DB.
- ☐ Sei qual API do Cosmos DB usar para documentos, MongoDB, grafo, tabela e Cassandra.
- ☐ Sei as camadas de blob e o que exige namespace hierárquico.
- ☐ Sei escolher entre Azure Files, NetApp Files, Elastic SAN e discos SSD Premium v2.
- ☐ Sei posicionar Fabric, Databricks, Data Explorer, Stream Analytics, Data Factory e Purview.

Questões de revisão do capítulo

R1.1 · Projetar soluções de armazenamento de dados

Parceiros enviam arquivos por SFTP todos os dias, e a empresa quer receber os arquivos direto no Armazenamento de Blobs, sem manter servidores SFTP. O que recomendar?

A. Azure Data Box para cada parceiro
B. Azure Files com compartilhamento SMB
C. Suporte a SFTP no Armazenamento de Blobs
D. VM Linux com servidor SFTP e AzCopy

R1.2 · Projetar soluções de armazenamento de dados

Sempre que um documento mudar no Cosmos DB, um índice de busca deve ser atualizado, sem consultas periódicas ao banco. O que recomendar?

A. Feed de alterações do Cosmos DB com Azure Functions
B. Backup contínuo com restauração diária
C. Replicação para outra região de leitura
D. Consulta agendada a cada minuto pela aplicação

R1.3 · Projetar soluções de armazenamento de dados

No Banco de Dados SQL Business Critical, relatórios pesados devem ler da réplica secundária para não afetar as transações. Como os relatórios devem se conectar?

A. Com o endereço IP público do servidor
B. Com o ouvinte do grupo de failover primário
C. Com ApplicationIntent=ReadOnly na conexão
D. Com um usuário SQL diferente

R1.4 · Projetar soluções de armazenamento de dados

Registros financeiros devem permitir comprovar, de forma criptográfica, que não foram adulterados, inclusive por administradores. O que recomendar no Banco de Dados SQL?

A. Segurança em nível de linha
B. Tabelas de razão (ledger)
C. Transparent Data Encryption
D. Máscara dinâmica de dados

Respostas comentadas

R1.1. C) Suporte a SFTP no Armazenamento de Blobs

Por quê: O suporte a SFTP exige namespace hierárquico e usuários locais com chave ou senha.

✗ A) Incorreta. É para transferência offline.
✗ B) Incorreta. SMB não é SFTP.
✗ D) Incorreta. Exige manter o servidor.

> **Dica de prova:** SFTP sem servidor: SFTP no Armazenamento de Blobs.

R1.2. A) Feed de alterações do Cosmos DB com Azure Functions

Por quê: O feed de alterações registra inserções e atualizações em ordem por partição e pode ser consumido por Functions ou pelo processador do SDK.

✗ B) Incorreta. Backup não propaga alterações.
✗ C) Incorreta. A replicação não atualiza o índice.
✗ D) Incorreta. Consultas periódicas consomem RU e têm atraso.

> **Dica de prova:** Reagir a alterações no Cosmos DB: feed de alterações.

R1.3. C) Com ApplicationIntent=ReadOnly na conexão

Por quê: A escala de leitura está disponível em Premium, Business Critical e Hyperscale. As consultas somente leitura usam réplicas secundárias.

✗ A) Incorreta. O endereço não define a réplica.
✗ B) Incorreta. Ele aponta para a réplica de gravação.
✗ D) Incorreta. O usuário não define a réplica.

> **Dica de prova:** Relatórios na réplica: ApplicationIntent=ReadOnly.

R1.4. B) Tabelas de razão (ledger)

Por quê: O ledger gera resumos criptográficos que podem ser armazenados fora do banco para verificar a integridade.

✗ A) Incorreta. Filtra linhas por usuário.
✗ C) Incorreta. Criptografa em repouso, sem detectar adulteração.
✗ D) Incorreta. Esconde valores, sem provar integridade.

> **Dica de prova:** Provar que não houve adulteração: ledger.

02

CAPÍTULO 2 · 15-20% DA PROVA

Projetar soluções de continuidade de negócios

Aqui tudo começa com duas perguntas: qual falha preciso suportar (servidor, zona ou região) e quanto posso perder (RPO) e ficar fora (RTO). A prova adora alternativas que protegem contra a falha errada, como redundância de zona quando o cenário é perda de região, ou um conjunto de disponibilidade quando se pede resistência a zona. Também mistura backup e recuperação de desastres: backup protege contra exclusão, corrupção e ransomware; DR mantém o serviço disponível. Preciso dominar as opções de SQL (redundância de zona, grupo de failover, restauração geográfica, LTR), Cosmos DB, redundância de armazenamento e os recursos de proteção do Azure Backup. E sempre conferir o critério de custo: a opção mais barata que atende vence.

Neste capítulo
18 tópicos-chave · 13 pegadinhas · 6 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

RPO e RTO

RPO é quanto dado posso perder e define a frequência mínima de backup ou replicação. RTO é quanto tempo posso ficar parado e define a arquitetura de recuperação. Perder no máximo 1 hora de dados e ficar no máximo 4 horas fora significa RPO de 1 hora e RTO de 4 horas.

HA, DR e backup

Alta disponibilidade trata falhas locais, como servidor ou zona, com recuperação automática. Recuperação de desastres trata eventos maiores, como perda de região. Backup protege contra perda e corrupção de dados, como exclusão acidental e ransomware. A estratégia começa classificando aplicativos por criticidade, RPO e RTO.

SLA composto

Serviços em série multiplicam seus SLAs, então o total é menor que o de cada parte: App Service com 99,95% e SQL com 99,99% dão cerca de 99,94%. Caminhos redundantes, como duas regiões, aumentam o SLA total.

Zonas de disponibilidade para VMs

VMs em três zonas atrás de um Load Balancer Standard com front-end redundante entre zonas continuam atendendo na falha de uma zona. Conjunto de disponibilidade fica em um datacenter e grupo de posicionamento por proximidade aproxima as VMs, aumentando o risco comum.

Redundância do Armazenamento

LRS protege dentro de um datacenter; ZRS entre zonas, sem outra região; GRS copia para a região emparelhada, mas usa LRS na primária; GZRS combina zona e região. RA-GRS e RA-GZRS permitem ler a secundária a qualquer momento pelo ponto de extremidade -secondary. Após o failover da conta, ela vira LRS na nova primária.

Par regional e residência de dados

O GRS replica para a região emparelhada, que pode ficar em outro país. Para Brazil South, o par fica fora do Brasil, então GRS pode violar uma exigência de manter os dados no país; avalie regiões dentro do país ou replicação própria.

Banco de Dados SQL: zona e região

Redundância de zona protege contra falha de zona sem usar outra região, disponível em General Purpose, Business Critical e Hyperscale conforme a região. Grupo de failover replica para outra região com ouvintes de leitura e gravação e somente leitura, que acompanham os papéis após o failover, com política automática ou gerenciada pelo cliente. Combinar os dois resiste a zona e região.

Restauração geográfica e LTR

A restauração geográfica com backup GRS é a DR regional mais barata do SQL, aceitando RPO de cerca de uma hora e RTO de horas. A retenção de longo prazo (LTR) guarda backups completos com políticas semanais, mensais e anuais, por exemplo por dez anos.

Instância Gerenciada de SQL

O grupo de failover da instância replica todos os bancos de usuário para uma instância secundária emparelhada, com failover conjunto e ouvinte estável. O link da Instância Gerenciada usa grupos de disponibilidade distribuídos para ter réplica de DR de um SQL Server 2022 local, com failover para a nuvem e de volta.

Continuidade no Cosmos DB

Com uma região de gravação, habilite o failover gerenciado pelo serviço e defina a prioridade das regiões. Redundância de zona pode ser habilitada ao adicionar a região. O backup contínuo tem camadas de 7 e 30 dias e restaura para uma nova conta. Com gravação em várias regiões, conflitos são resolvidos por padrão com o último gravador vence.

Azure Site Recovery

Replicação contínua com failover sob demanda, planos de recuperação e testes sem impacto, para VMs do Azure entre regiões, VMware, Hyper-V e físicos (com dispositivo de replicação). Também faz DR de zona para zona na mesma região. A consistência de várias VMs gera pontos compartilhados para VMs que trocam dados. Não protege clusters AKS e tem retenção curta para ransomware.

Azure Backup para VMs e bancos

No Windows usa VSS antes do snapshot para consistência de aplicativo; no Linux, scripts de pré e pós-snapshot. A política aprimorada permite vários backups por dia e é exigida por VMs com Inicialização Confiável e discos SSD Premium v2 e Ultra. SQL Server em VM e SAP HANA (Backint) suportam backups de log a cada 15 minutos.

Azure Backup com Cofre de Backup

Protege AKS (extensão no cluster, recursos do Kubernetes e volumes, restauração entre regiões), PostgreSQL servidor flexível (retenção de até dez anos) e blobs. O backup com cofre de blobs leva os dados para fora da conta; o backup operacional usa exclusão temporária e versões dentro da própria conta.

Proteção do backup contra ataques

Exclusão temporária aprimorada, cofre imutável bloqueado e autorização multiusuário com o Resource Guard, que fica em outra assinatura ou locatário e exige aprovação de outra equipe para operações críticas, como reduzir retenção. A redundância do cofre (LRS, ZRS ou GRS) é definida antes de proteger itens.

Roteamento global para failover

Front Door é global de camada 7, com WAF e cache; no roteamento, prioridade define failover e peso distribui entre origens de mesma prioridade. Traffic Manager faz failover global por DNS para tráfego não HTTP. Load Balancer entre regiões oferece IP público global estático para TCP, com failover automático.

Resiliência a zona em PaaS

App Service exige planos Premium v2, v3 ou v4, ou ambientes do App Service, com várias instâncias. AKS usa pools de nós entre zonas e restrições de dispersão de topologia. Service Bus Premium com zonas. Discos ZRS (SSD Premium e SSD Standard) podem ser anexados a outra VM após forçar a desanexação.

Key Vault em falha regional

Em regiões com par, o Key Vault replica o conteúdo para a região emparelhada automaticamente; durante o failover, o cofre fica somente leitura. Para regiões sem par ou requisitos maiores, use cofres em várias regiões.

Práticas de resiliência

Reserva de capacidade sob demanda garante capacidade para as VMs de DR (reserva de VM só dá desconto). Sessão em cache distribuído externo deixa as instâncias sem estado. Ponto de integridade com dependências informa a saúde real ao balanceador. IaC e pipelines prontos reduzem o RTO sem custo fixo. Chaos Studio injeta falhas para validar.

Macetes para memorizar

RPO x RTO

RPO = Ponto (quantos dados para trás); RTO = Tempo (quanto tempo parado).

Escopo da falha

Servidor, Zona, Região: Conjunto não salva zona, Zona não salva região.

Armazenamento

L de Local, Z de Zona, G de Geo, RA de Read Access: GZRS soma zona e geo; RA deixa ler a secundária já.

SQL em DR

Barato = restauração geográfica; rápido e transparente = grupo de failover; anos de guarda = LTR.

Backup x DR

Backup volta no tempo; Site Recovery muda de lugar.

Front Door

Prioridade decide quem assume; peso decide quanto cada um recebe.

Tabela de memorização: não confunda

Quando é...	...e quando é
Grupo de failover do SQL RPO e RTO baixos, failover automático e mesmo ponto de conexão antes e depois.	**Restauração geográfica** Menor custo, aceitando RPO de cerca de uma hora e RTO de horas.
Redundância de zona Sobreviver à falha de uma zona sem depender de outra região.	**Grupo de failover ou réplica em outra região** Sobreviver à perda da região inteira; para os dois cenários, combine ambos.
Azure Backup Pontos de recuperação de semanas atrás contra ransomware, exclusão ou corrupção.	**Azure Site Recovery** RPO de minutos e RTO de horas em desastre regional, com failover. Para os dois requisitos, use juntos.
GRS Cópia na região emparelhada usada só após failover, com LRS na primária.	**RA-GZRS** Proteção contra zona e região, com leitura da secundária a qualquer momento sem esperar o failover.

Azure Front Door Failover global de aplicativo HTTP com WAF e cache na borda.	**Traffic Manager ou Load Balancer entre regiões** Failover global de tráfego não HTTP (TCP); IP global estático pede o Load Balancer entre regiões.
Ouvinte de leitura e gravação Aplicativo transacional que deve sempre apontar para a primária.	**Ouvinte somente leitura** Relatórios na réplica secundária sem mudar a conexão após o failover.
Reserva de capacidade sob demanda Garantir capacidade física para criar as VMs de DR na região secundária.	**Reserva de VM de três anos** Obter desconto por compromisso, sem garantia de capacidade.

Números que caem

Item	Valor
SLA composto App Service 99,95% com SQL 99,99%	**cerca de 99,94%**
Camadas do backup contínuo do Cosmos DB	**7 e 30 dias**
Backups de log do SQL Server em VM e do SAP HANA	**a cada 15 minutos**
Retenção do Azure Backup para PostgreSQL servidor flexível	**até dez anos**
Restauração geográfica do SQL	**RPO de cerca de uma hora e RTO de horas**
Zonas para a camada web resistente a falha de zona	**VMs em três zonas atrás de Load Balancer Standard**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Redundância de zona no banco para proteger contra falha de região.
Como não cair: Zona protege só dentro da região. Falha regional exige grupo de failover, réplica geográfica ou restauração geográfica.

⚠ **Alerta de prova:** Conjunto de disponibilidade para resistir à falha de zona.
Como não cair: O conjunto fica em um datacenter. Para zona, distribua VMs em zonas atrás de um Load Balancer Standard.

⚠ **Alerta de prova:** Slots de implantação ou plano Basic com duas instâncias para resiliência.
Como não cair: Slots ficam nas mesmas instâncias e região; o Basic não tem redundância de zona. Use Premium v2, v3 ou v4 com redundância de zona, ou duas regiões com Front Door.

⚠ **Alerta de prova:** GRS sem acesso de leitura para continuar lendo durante a falha.
Como não cair: No GRS a secundária só é usada após o failover. Leitura imediata pede RA-GRS ou RA-GZRS.

⚠ **Alerta de prova:** Bloqueio CanNotDelete no cofre para impedir exclusão maliciosa de backups.
Como não cair: O bloqueio pode ser removido por quem tem permissão e não impede reduzir retenção. Use cofre imutável bloqueado, exclusão temporária e Resource Guard.

⚠ **Alerta de prova:** Replicação GRS do cofre para impedir exclusões maliciosas.
Como não cair: Redundância copia dados, mas não impede exclusão. Imutabilidade é que protege.

⚠ **Alerta de prova:** Só o Site Recovery para recuperar de ransomware.
Como não cair: A retenção do Site Recovery é curta. Pontos de semanas atrás exigem Azure Backup; combine os dois quando houver também desastre regional.

⚠ **Alerta de prova:** Failover ou consistência forte no Cosmos DB para desfazer exclusões.
Como não cair: Nem failover nem consistência guardam versões anteriores. Voltar no tempo exige backup contínuo com restauração pontual.

⚠ **Alerta de prova:** Replicação geográfica ativa sem grupo de failover para manter o mesmo ponto de conexão.
Como não cair: Sem grupo, é preciso trocar a cadeia de conexão no failover. Os ouvintes do grupo de failover resolvem.

⚠ **Alerta de prova:** Considerar que o SLA composto é igual ao maior ou ao menor SLA isolado.
Como não cair: Dependências em série multiplicam: o total fica abaixo de cada parte.

⚠ **Alerta de prova:** Reserva de VM ou cota maior de vCPUs para garantir capacidade no DR.
Como não cair: Reserva dá desconto e cota não garante capacidade física. Use reserva de capacidade sob demanda.

⚠ **Alerta de prova:** Backup diário da VM para RPO de 15 minutos no SQL Server ou SAP HANA.
Como não cair: Backup diário tem RPO de até 24 horas. Use Azure Backup para SQL em VM ou para SAP HANA com backups de log.

⚠ **Alerta de prova:** Site Recovery para proteger cluster AKS ou exportação de manifestos como backup.
Como não cair: Site Recovery não protege AKS e manifestos não guardam volumes. Use Azure Backup para AKS.

Como cai na prova

📝 **Como cai:** Cenário com RPO e RTO em números para falha regional.
Como resolver: Traduza: RPO de minutos exige replicação contínua (Site Recovery, grupo de failover); RPO de horas aceita backup geográfico. Depois verifique se pede o menor custo e escolha a opção mais barata que ainda atende.

📝 **Como cai:** Requisito de resistência a zona ou região em um serviço PaaS específico.
Como resolver: Identifique o escopo da falha e procure o recurso nativo do serviço: redundância de zona (SQL, Cosmos, App Service Premium, Service Bus Premium, discos ZRS) ou failover regional (grupo de failover, failover gerenciado do Cosmos, GZRS).

📝 **Como cai:** Proteção de backups contra administradores mal-intencionados ou ransomware.
Como resolver: Descarte bloqueios de recurso e redundância. Procure imutabilidade (cofre imutável bloqueado), exclusão temporária e autorização multiusuário com Resource Guard.

📝 **Como cai:** Cálculo de SLA composto.
Como resolver: Converta em decimais e multiplique os SLAs em série. O resultado sempre fica abaixo do menor SLA isolado; redundância em paralelo é o que aumenta o total.

📝 **Como cai:** Arquitetura de DR para aplicativo web completo.
Como resolver: Trate cada camada: roteamento global (Front Door), computação em duas regiões e dados replicados (grupo de failover ou Cosmos DB multirregião). Uma camada sem estratégia regional derruba o conjunto.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
RPO de 15 minutos e RTO de 2 horas para falha regional de VMs	**Azure Site Recovery para região secundária**
DR barato no SQL, RPO de cerca de uma hora	**Restauração geográfica com backup GRS**
Failover regional do SQL com o mesmo ponto de conexão	**Grupo de failover com ouvintes**
SQL Server 2022 local com réplica de DR na nuvem	**Link da Instância Gerenciada**
Backups completos semanais por dez anos no SQL	**Retenção de longo prazo (LTR)**
Cosmos DB com dados apagados dias atrás	**Backup contínuo com restauração pontual**

Região de gravação do Cosmos DB cai e outra assume sem ação manual	**Failover gerenciado pelo serviço**
Gravações mesmo com a perda de uma região, RTO perto de zero	**Ativo-ativo em duas regiões com Front Door e Cosmos DB**
Operação crítica no cofre exige aprovação de outra equipe	**Autorização multiusuário com Resource Guard**
VM com Inicialização Confiável no backup	**Política aprimorada de backup**
Região sem par adequado, DR contra falha de zona	**Site Recovery de zona para zona**
VMs que trocam dados precisam de pontos de recuperação consistentes	**Consistência de várias VMs no Site Recovery**
Cache em duas regiões aceitando gravações	**Replicação geográfica ativa do Redis**
Validar resistência à perda de zona injetando falhas	**Azure Chaos Studio**

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

- Sempre identifique o escopo da falha: zona não é região.
- Backup e DR são complementares; ransomware pede backup, desastre regional pede replicação.
- Restauração geográfica é a DR mais barata; grupo de failover é a mais rápida e transparente.
- Após o failover da conta de armazenamento, ela vira LRS na nova primária.
- O par regional de Brazil South fica fora do Brasil.

Essenciais para a prova (checklist)

- ☐ Sei definir RPO e RTO a partir de um requisito de negócio.
- ☐ Sei diferenciar HA, DR e backup e dar um exemplo de cada.
- ☐ Sei calcular SLA composto de serviços em série.
- ☐ Sei escolher entre LRS, ZRS, GRS, GZRS, RA-GRS e RA-GZRS.
- ☐ Sei quando usar redundância de zona, grupo de failover, restauração geográfica e LTR no SQL.
- ☐ Sei configurar continuidade no Cosmos DB: failover gerenciado, zonas e backup contínuo.
- ☐ Sei quando usar Site Recovery, Azure Backup ou os dois juntos.
- ☐ Sei proteger backups com cofre imutável, exclusão temporária e Resource Guard.
- ☐ Sei escolher entre Front Door, Traffic Manager e Load Balancer entre regiões para failover global.

Questões de revisão do capítulo

R2.1 · Projetar soluções de continuidade de negócios

Um banco do Banco de Dados SQL deve continuar disponível em falha de uma zona, sem usar outra região. O que recomendar?

A. Réplica geográfica somente leitura
B. Redundância de zona no banco
C. Backup com armazenamento LRS
D. Grupo de failover para outra região

R2.2 · Projetar soluções de continuidade de negócios

Com o menor custo, a empresa quer recuperar um Banco de Dados SQL em outra região se a região primária falhar, aceitando RPO de cerca de uma hora e RTO de horas. O que recomendar?

A. Grupo de failover com réplica ativa
B. Redundância de zona no banco
C. Réplica de leitura na mesma região
D. Restauração geográfica com backup GRS

R2.3 · Projetar soluções de continuidade de negócios

Dados de uma conta do Cosmos DB foram excluídos por engano três dias atrás. A empresa quer restaurar a conta para o estado anterior. O que precisava estar configurado?

A. Failover gerenciado pelo serviço
B. Consistência forte na conta
C. Backup periódico com retenção de 8 horas
D. Backup contínuo com restauração pontual

R2.4 · Projetar soluções de continuidade de negócios

Os dados devem permanecer no Brasil, com recuperação geográfica. Por que usar GRS em uma conta em Brazil South pode não atender?

A. O par regional fica fora do Brasil
B. GRS não copia os dados
C. GRS exige uma conta premium
D. Brazil South não oferece redundância

Respostas comentadas

R2.1. B) Redundância de zona no banco

Por quê: A redundância de zona está disponível em várias camadas, como General Purpose, Business Critical e Hyperscale, conforme a região.

✗ A) Incorreta. A réplica geográfica fica em outra região.
✗ C) Incorreta. Backup LRS não mantém o banco disponível.
✗ D) Incorreta. O requisito é não depender de outra região.

> **Dica de prova:** SQL resistente a falha de zona: redundância de zona.

R2.2. D) Restauração geográfica com backup GRS

Por quê: A restauração geográfica é a opção mais barata de DR regional. Grupos de failover atendem RPO e RTO baixos.

✗ A) Incorreta. Atende RPO e RTO menores, com custo maior.
✗ B) Incorreta. Protege contra falha de zona, não de região.
✗ C) Incorreta. Não protege contra falha regional.

> **Dica de prova:** DR regional barato no SQL: restauração geográfica.

R2.3. D) Backup contínuo com restauração pontual

Por quê: O backup contínuo do Cosmos DB tem camadas de 7 e 30 dias e restaura para uma nova conta.

✗ A) Incorreta. Failover não desfaz exclusões.
✗ B) Incorreta. A consistência não guarda versões anteriores.
✗ C) Incorreta. A retenção curta não cobre três dias.

> **Dica de prova:** Voltar no tempo no Cosmos DB: backup contínuo.

R2.4. A) O par regional fica fora do Brasil

Por quê: Pares de regiões podem ficar em outro país. Em exigências de residência, avalie regiões dentro do país ou soluções próprias de replicação.

✗ B) Incorreta. O GRS copia para a região emparelhada.
✗ C) Incorreta. GRS é oferecido em contas Standard.
✗ D) Incorreta. A região oferece LRS, ZRS e GRS.

> **Dica de prova:** Residência de dados e GRS: verifique o par regional.

03

CAPÍTULO 3 · 25-30% DA PROVA

Projetar soluções de identidade, governança e monitoramento

Neste domínio preciso escolher a peça certa entre Microsoft Entra ID, Azure Policy, RBAC, Key Vault, Azure Monitor e Defender for Cloud a partir de um requisito curto. O enunciado quase sempre traz um verbo decisivo: bloquear, impedir, auditar, avisar, rotacionar, recertificar ou configurar automaticamente. Meu erro mais comum é marcar algo que só avisa ou sugere (orçamento, Advisor, política Audit, alerta) quando o cenário pede impedir ou corrigir sozinho. Também confundo onde cada log mora: log de atividades, logs de recurso, logs do Entra e telemetria de aplicativo são coisas diferentes. Por fim, licença pesa: Acesso Condicional e grupos dinâmicos exigem P1; PIM e ID Protection exigem P2 ou Entra ID Governance.

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

Tópicos-chave

Acesso Condicional

Avalia sinais como usuário, aplicativo, dispositivo, local e risco para permitir, bloquear ou exigir controles adicionais, como MFA e dispositivo em conformidade com o Intune. Locais nomeados podem ser definidos por país ou faixa de IP. Também exige termos de uso e força de autenticação. Exige licença P1.

Privileged Identity Management (PIM)

Dá acesso just-in-time a funções do Entra e do Azure por atribuições qualificadas, com aprovação, MFA na ativação, justificativa e auditoria. Resolve o requisito de Proprietário só quando precisar e por tempo limitado. Exige Microsoft Entra ID P2 ou Governance.

ID Protection

Calcula risco de usuário e risco de entrada. Políticas de Acesso Condicional baseadas em risco usam esses sinais para exigir MFA ou troca de senha, como no caso de credencial vazada (risco do usuário). Exige P2.

Revisões de acesso

Recertificação periódica de grupos, aplicativos, pacotes de acesso e funções privilegiadas, com revisores definidos (por exemplo, gestores) e ações automáticas, como remover quem não for aprovado. Para convidados inativos, podem bloquear a entrada por 30 dias e depois excluir a conta.

Gerenciamento de direitos (pacotes de acesso)

Usuários internos e externos solicitam um conjunto de grupos, aplicativos e sites com política de aprovação, expiração automática e revisões. É a resposta para parceiro que pede acesso com aprovação do gestor e prazo de validade.

Fluxos de trabalho de ciclo de vida

Fazem parte do Microsoft Entra ID Governance e são disparados por atributos como data de contratação. Automatizam entrada e saída: gerar o Passe de Acesso Temporário no primeiro dia e remover acessos no desligamento.

Identidade gerenciada (sistema x usuário)

A atribuída pelo sistema segue o ciclo de vida do recurso e é excluída com ele. A atribuída pelo usuário é compartilhada por vários recursos, simplifica permissões e pré-autorização e continua existindo se os recursos forem excluídos. Identidades gerenciadas só existem em recursos do Azure.

Federação de identidade de carga de trabalho

Confia em tokens de provedores externos, como GitHub, Kubernetes e outras nuvens, via OIDC, eliminando segredos e certificados no pipeline. No AKS, o Microsoft Entra Workload ID usa o emissor OIDC do cluster e contas de serviço do Kubernetes para dar identidade própria a cada pod.

Microsoft Entra External ID

Tem dois cenários: colaboração B2B com parceiros no locatário da força de trabalho e identidade de clientes (CIAM) em um locatário externo. Para milhões de consumidores com e-mail, contas sociais e páginas com a marca, use o locatário externo.

Identidade híbrida: PTA, PHS e Cloud Sync

A autenticação de passagem (PTA) valida a senha no AD local, respeita horários de logon e contas desabilitadas, e é recomendado ter vários agentes. A sincronização de hash de senha envia um hash do hash para a nuvem. O Entra Cloud Sync usa agentes leves e atende florestas desconectadas; o Entra Connect Sync fica para cenários mais complexos.

Microsoft Entra Domain Services

Fornece um domínio gerenciado, sincronizado com o Entra ID, com LDAP, Kerberos e ingresso no domínio para aplicativos legados, sem manter controladores de domínio. O Entra ID sozinho não oferece LDAP nem ingresso no domínio tradicional.

Efeitos do Azure Policy

Deny impede a criação fora da regra (SKUs permitidos, marca com valores aprovados via operador in, PaaS sem acesso público). Audit só relata. DeployIfNotExists configura automaticamente, como diagnóstico em escala e backup de VMs por marca. Modify altera os recursos, por exemplo copiando marcas.

Configuração de máquina e Azure Policy para AKS

A configuração de máquina (antiga configuração de convidado) usa uma extensão e definições de política para auditar dentro do SO de VMs e servidores Arc, como a política de senha local. O complemento Azure Policy para AKS usa o Gatekeeper e iniciativas internas, como os padrões de segurança de pods, para bloquear contêineres privilegiados.

Hierarquia de governança

Grupos de gerenciamento organizam assinaturas e herdam políticas; a assinatura é a unidade de escala, cobrança, cotas e governança. Nas zonas de aterrissagem do Cloud Adoption Framework, os grupos são organizados por função: plataforma, zonas de aterrissagem, sandbox e desativados. O grupo Sandbox recebe políticas permissivas, mas isoladas da rede corporativa.

Azure Key Vault

A exclusão temporária vem habilitada por padrão; a proteção contra limpeza, uma vez habilitada, não pode ser desativada. A política de rotação define intervalo e expiração, e o Event Grid avisa sobre chaves perto de expirar. Recomendação: um cofre por aplicativo, ambiente e região, com RBAC, proteção contra limpeza e rede privada.

Níveis de proteção de chaves

Key Vault Standard protege chaves em software; Premium usa HSM multilocatário; Managed HSM é de locatário único, com validação FIPS 140-3 nível 3 e controle total do domínio de segurança.

Configurações de diagnóstico e custos de logs

Enviam logs de recurso, log de atividades e métricas de plataforma para Log Analytics, armazenamento ou Hubs de Eventos, com vários destinos ao mesmo tempo. Para reduzir custo: transformações na regra de coleta de dados, planos de tabela Basic ou Auxiliary, camada de compromisso (a partir de 100 GB por dia) e limite diário, útil em testes, porque em produção pode causar perda de dados importantes.

Defender for Cloud, Sentinel e Application Insights

O CSPM do Defender for Cloud gera recomendações, pontuação segura e análise de caminhos de ataque, e o painel de conformidade regulatória avalia normas como ISO 27001 e PCI DSS. O Sentinel é o SIEM e SOAR, com conectores, regras analíticas e playbooks. O Application Insights usa OpenTelemetry para requisições, dependências e rastreamento distribuído, com testes de disponibilidade e amostragem.

Macetes para memorizar

Política x custo x recomendação

Avisa, Impede, Conserta: orçamento, Advisor e Audit avisam; Deny impede; DeployIfNotExists conserta sozinho.

Licenças do Entra

P1 é a Porta (Acesso Condicional, grupos dinâmicos); P2 é Privilégio e Perigo (PIM e ID Protection).

Identidades gerenciadas

Sistema morre com o recurso; Usuário sobrevive e se compartilha.

Identidade de aplicativos

Dentro do Azure: identidade gerenciada. Pipeline ou pod: federação (Workload ID). Fora e sem federação: entidade de serviço com certificado. Nunca conta de usuário.

Service x Resource Health

Service Health: a Microsoft avisa sobre a nuvem. Resource Health: o MEU recurso caiu.

Custos de logs

Filtra (DCR), Rebaixa (plano de tabela), Compromete (camada de compromisso), Limita (limite diário em teste; em produção pode perder dados).

Key Vault

Soft delete já vem ligado; purge protection, depois de ligada, não desliga.

Tabela de memorização: não confunda

Quando é...	...e quando é
PIM com atribuições qualificadas O privilégio deve ser ativado só quando necessário, com aprovação, MFA e tempo limitado.	**Revisões de acesso** Gestores precisam confirmar periodicamente quem continua em grupos, apps ou funções, com remoção automática de quem não for aprovado.
Acesso Condicional Exigir MFA combinada com dispositivo em conformidade, local, risco ou aplicativo específico.	**Padrões de segurança** Basta exigir MFA, sem verificar o dispositivo nem outras condições.
Identidade gerenciada atribuída pelo sistema Um único recurso precisa de identidade e ela pode morrer junto com ele.	**Identidade gerenciada atribuída pelo usuário** Várias Functions e VMs compartilham a mesma identidade e permissões, e ela deve sobreviver à exclusão dos recursos.
Autenticação de passagem (PTA) Nenhuma forma de hash pode ir para a nuvem e restrições de logon do AD local devem valer.	**Sincronização de hash de senha** A política permite que um hash do hash da senha seja enviado para a nuvem.

Alerta do Service Health Avisos de incidentes, manutenções planejadas, avisos de integridade e de segurança da plataforma.	**Alerta do Resource Health** Saber quando um recurso específico, como uma VM de produção, ficou indisponível, filtrando a causa (plataforma ou usuário).
Especificações de modelo (template specs) Publicar modelos aprovados com versões e acesso por RBAC para as equipes implantarem.	**Pilhas de implantação com negação** Gerenciar recursos implantados como uma unidade, impedir exclusão por terceiros e remover o que sair do modelo.
External ID em locatário externo Milhões de consumidores criando contas com e-mail ou contas sociais, com páginas personalizadas.	**Convites B2B** Parceiros de negócio colaborando no locatário da força de trabalho.

Números que caem

Item	Valor
Camada de compromisso do Log Analytics	**começa em 100 GB por dia**
Managed HSM	**locatário único, validação FIPS 140-3 nível 3**
Revisão de acesso de convidados inativos	**pode bloquear a entrada por 30 dias e depois excluir**
Licença P1	**Acesso Condicional, grupos dinâmicos e identidade híbrida avançada**
Licença P2 ou Entra ID Governance	**ID Protection e PIM**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Orçamento com alerta em 80% ou recomendação do Advisor para limitar tamanhos de VM.
Como não cair: Orçamento avisa e Advisor sugere, mas nenhum impede a criação. Use a política de SKUs de VM permitidos (Deny).

⚠ **Alerta de prova:** Bloqueio ReadOnly ou CanNotDelete para controlar acesso, rotacionar chaves ou validar marcas.
Como não cair: Bloqueios só impedem alterar ou excluir o recurso. Não controlam entrada, não rotacionam, não validam marcas e nem se aplicam a grupos do Entra.

⚠ **Alerta de prova:** NSG com as faixas de IP de países para bloquear entradas nos aplicativos corporativos.
Como não cair: NSG não protege o Entra ID. Bloqueio por país na entrada é com locais nomeados no Acesso Condicional.

⚠ **Alerta de prova:** Identidade gerenciada para um aplicativo que roda fora do Azure.
Como não cair: Identidade gerenciada só existe em recursos do Azure. Sem federação disponível, use entidade de serviço com certificado; com GitHub ou Kubernetes, use federação de identidade de carga de trabalho.

⚠ **Alerta de prova:** Convites B2B para consumidores, para funcionários de empresa adquirida ou para acessar um SaaS.
Como não cair: B2B é para usuários externos de parceiros. Consumidores: External ID em locatário externo. Florestas adquiridas: Cloud Sync. Vários locatários da mesma empresa: organização multilocatário com sincronização. SaaS: aplicativo empresarial com SSO e SCIM.

⚠ **Alerta de prova:** Política com efeito Audit para garantir que todo recurso envie diagnóstico ou tenha backup.
Como não cair: Audit só relata a ausência. Para configurar automaticamente, use DeployIfNotExists.

⚠ **Alerta de prova:** Política Modify que copia marcas para resolver valores aprovados ou relatórios de custo.
Como não cair: Modify altera recursos e não valida valores. Valores aprovados: Deny com operador in. Marcas nos relatórios sem mexer nos recursos: herança de marcas no Cost Management.

⚠ **Alerta de prova:** Retenção interativa de sete anos para logs de auditoria imutáveis.
Como não cair: Retenção não garante imutabilidade e aumenta custo. Use exportação de dados do workspace para armazenamento imutável.

⚠ **Alerta de prova:** Criar mais workspaces ou um workspace por recurso para reduzir custo de ingestão.
Como não cair: Dividir não reduz o preço por GB e fragmenta os dados. Use camada de compromisso, planos de tabela mais baratos e transformações na DCR.

⚠ **Alerta de prova:** Usar o log de atividades para CPU, logs de recurso ou entradas do Entra.
Como não cair: O log de atividades só registra operações de gerenciamento do Azure. CPU é métrica, logs de serviços vêm por diagnóstico e logs do Entra precisam de configuração de diagnóstico própria do Entra.

⚠ **Alerta de prova:** MFA por SMS ou senhas longas como métodos resistentes a phishing.
Como não cair: SMS e senha não resistem a phishing. Os resistentes são chaves de acesso FIDO2, Windows Hello for Business e autenticação por certificado, exigidos via força de autenticação.

⚠ **Alerta de prova:** Padrões de segurança para exigir MFA e dispositivo em conformidade.
Como não cair: Os padrões exigem MFA, mas não verificam o dispositivo. Esse requisito é Acesso Condicional.

⚠ **Alerta de prova:** Bloqueio inteligente de conta para credencial vazada ou senhas com o nome da empresa.
Como não cair: O bloqueio protege contra tentativas. Credencial vazada: Acesso Condicional por risco do usuário. Senha previsível: proteção de senha com lista própria, estendida ao AD local por agentes nos DCs.

⚠ **Alerta de prova:** Azure Blueprints para gerenciar e proteger recursos como unidade.
Como não cair: O Blueprints está em descontinuação e não é recomendado. Use pilhas de implantação com configurações de negação.

Como cai na prova

📝 **Como cai:** Requisito curto terminando em O que recomendar?, com quatro serviços plausíveis.
Como resolver: Grife o verbo (bloquear, avisar, rotacionar, recertificar, configurar automaticamente). Elimine o que só observa quando o verbo é impedir, e o que é manual quando pede automático. Sobram uma ou duas; escolha a que resolve exatamente o escopo citado.

📝 **Como cai:** Escolha DUAS, pedindo as partes de uma mesma solução.
Como resolver: Procure o par complementar: identidade gerenciada + função Usuário de Segredos do Key Vault; PIM + revisões de acesso; logs de recurso + log de atividades; planos de tabela + transformações. Descarte SAS, chave do cofre ou acesso anônimo, que não existem para o Key Vault.

📝 **Como cai:** Aplicativo ou pipeline precisa autenticar sem senha em um recurso do Azure.
Como resolver: Pergunte onde o código roda: em recurso do Azure, identidade gerenciada; em GitHub, Kubernetes ou outra nuvem com OIDC, federação; em pod do AKS, Workload ID; fora sem federação, entidade de serviço com certificado. No SQL, combine com autenticação do Entra.

📝 **Como cai:** Cenário de custo ou retenção de logs no Azure Monitor.
Como resolver: Volume alto e estável: camada de compromisso. Dados que não deveriam entrar: transformação na DCR. Pouca consulta: plano Basic ou Auxiliar. Teste com risco de surpresa: limite diário. Anos e imutável: exportação para armazenamento imutável.

📝 **Como cai:** Governança em escala com muitas assinaturas, ambientes e equipes.
Como resolver: Políticas comuns vão no grupo de gerenciamento e herdam; separação de cobrança e cotas exige assinaturas diferentes; inventário é Resource Graph; nomes e marcas seguem convenção definida antes das implantações.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Correlacionar eventos de várias fontes, detectar ameaças e automatizar respostas	**Microsoft Sentinel (SIEM e SOAR)**
Função só quando precisar, com aprovação e tempo limitado	**PIM com atribuições qualificadas**
A cada trimestre gestores confirmam quem continua	**Revisões de acesso recorrentes**
Parceiros solicitam acesso com aprovação e expiração automática	**Pacotes de acesso no gerenciamento de direitos**
LDAP, Kerberos e ingresso no domínio sem manter controladores	**Microsoft Entra Domain Services**
Pipeline do GitHub Actions sem segredos no repositório	**Federação de identidade de carga de trabalho com OIDC**
Nenhum hash de senha na nuvem e restrições de logon locais	**Autenticação de passagem (PTA)**
Consultar em segundos recursos de dezenas de assinaturas por tipo, região e marca	**Azure Resource Graph com KQL**
Provedor de serviços gerencia recursos de vários clientes do próprio locatário	**Azure Lighthouse com delegação**
Remover colunas com dados pessoais antes da ingestão	**Transformação na regra de coleta de dados**
Logs volumosos consultados raramente, só em investigações	**Plano de tabela Auxiliar**
Ingestão alta e estável no Log Analytics	**Camada de compromisso do workspace**
App interno acessado de fora sem abrir portas de entrada	**Proxy de Aplicativo do Microsoft Entra**
Convidados reclamam de MFA duplicada	**Confiança na MFA nas configurações de acesso entre locatários**

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

- Avisar não é impedir: orçamento, Advisor, alertas e Audit nunca bloqueiam a criação de recursos.
- Bloqueios de recurso não controlam identidade, não validam marcas e não rotacionam nada.
- B2B é só para parceiros externos; consumidores vão para External ID em locatário externo.
- Log de atividades registra operações de gerenciamento; não tem CPU, logs de serviços nem entradas do Entra.
- Proteção contra limpeza no Key Vault é irreversível depois de habilitada.

Essenciais para a prova (checklist)

☐ Sei escolher entre PIM, revisões de acesso, gerenciamento de direitos e fluxos de trabalho de ciclo de vida.

☐ Sei quais recursos exigem P1 e quais exigem P2.

☐ Sei quando usar identidade gerenciada do sistema, do usuário, Workload ID, federação ou entidade de serviço com certificado.

☐ Sei diferenciar PTA, sincronização de hash, Cloud Sync e Entra Domain Services.

☐ Sei o que fazem os efeitos Deny, Audit, Modify e DeployIfNotExists.

☐ Sei organizar grupos de gerenciamento e assinaturas no modelo de zonas de aterrissagem.

☐ Sei configurar Key Vault com rotação, proteção contra limpeza, ponto privado e escolher entre Standard, Premium e Managed HSM.

☐ Sei para onde vão os dados de uma configuração de diagnóstico e como reduzir o custo do Log Analytics.

☐ Sei diferenciar Service Health, Resource Health, Application Insights, Container insights e alertas de métrica multirrecurso.

☐ Sei quando usar Defender for Cloud e Sentinel, e as ferramentas do Cost Management como herança de marcas, regras de alocação de custo e recomendações de reserva.

Questões de revisão do capítulo

R3.1 · Projetar soluções de identidade, governança e monitoramento

Uma loja virtual precisa permitir que milhões de consumidores criem contas com e-mail ou com contas sociais, com páginas de entrada personalizadas com a marca. Qual solução de identidade recomendar?

A. Microsoft Entra External ID em um locatário externo
B. Usuários membros criados no locatário corporativo
C. Active Directory Domain Services em VMs do Azure
D. Convites B2B para cada consumidor da loja

R3.2 · Projetar soluções de identidade, governança e monitoramento

A segurança quer auditar configurações dentro do sistema operacional das VMs, como a política de senha local do Windows, e ver a conformidade no Azure Policy. O que recomendar?

A. Revisões de acesso dos administradores
B. Bloqueio ReadOnly nas máquinas virtuais
C. Política de marcas nos grupos de recursos
D. Configuração de máquina com o Azure Policy

R3.3 · Projetar soluções de identidade, governança e monitoramento

A equipe quer ser avisada sempre que uma VM de produção ficar indisponível por um problema da plataforma Azure. O que recomendar?

A. Relatório de custos diário
B. Alerta de métrica de rede das VMs
C. Recomendações do Azure Advisor
D. Alerta do Resource Health nas VMs

R3.4 · Projetar soluções de identidade, governança e monitoramento

Um aplicativo que roda fora do Azure, sem suporte a federação de identidade, precisa chamar APIs do Azure. Qual credencial recomendar?

A. Chave de assinatura do Azure
B. Conta de usuário com MFA desativada
C. Identidade gerenciada do aplicativo
D. Entidade de serviço com certificado

Respostas comentadas

R3.1. A) Microsoft Entra External ID em um locatário externo

Por quê: O Microsoft Entra External ID tem dois cenários: colaboração B2B com parceiros no locatário da força de trabalho e identidades de clientes (CIAM) em um locatário externo.

✗ B) Incorreta. Misturar consumidores com funcionários dificulta segurança e escala.
✗ C) Incorreta. AD DS não oferece inscrição de consumidores nem login social.
✗ D) Incorreta. B2B é para parceiros de negócio, não para consumidores em massa.

> **Dica de prova:** Identidade de consumidores: External ID com locatário externo.

R3.2. D) Configuração de máquina com o Azure Policy

Por quê: A configuração de máquina (antiga configuração de convidado) usa uma extensão e definições de política para avaliar o SO de VMs e servidores Arc.

✗ A) Incorreta. Revisam acesso, não configurações.
✗ B) Incorreta. Impede alterações no recurso, sem avaliar o SO.
✗ C) Incorreta. Marcas não avaliam o SO.

> **Dica de prova:** Auditar dentro do SO: configuração de máquina.

R3.3. D) Alerta do Resource Health nas VMs

Por quê: Alertas do Resource Health podem cobrir assinaturas ou grupos de recursos e filtrar pela causa, como plataforma ou usuário.

✗ A) Incorreta. Não trata disponibilidade.
✗ B) Incorreta. Tráfego baixo não indica a causa.
✗ C) Incorreta. Não geram alertas de indisponibilidade.

> **Dica de prova:** Recurso indisponível pela plataforma: alerta do Resource Health.

R3.4. D) Entidade de serviço com certificado

Por quê: Quando identidades gerenciadas e federação não são possíveis, use certificados com rotação e armazenamento seguro.

✗ A) Incorreta. Não existe chave de assinatura para APIs do Azure.
✗ B) Incorreta. Contas de usuário não devem ser usadas por aplicativos.
✗ C) Incorreta. Identidades gerenciadas só existem em recursos do Azure.

> **Dica de prova:** App fora do Azure sem federação: entidade de serviço com certificado.

04

CAPÍTULO 4 · 30-35% DA PROVA

Projetar soluções de infraestrutura

Este é o domínio de maior peso, e cobre computação, padrões de aplicativo, mensageria, rede, APIs e migração. Na prova eu recebo um requisito e quatro serviços que parecem servir; o detalhe que decide está no adjetivo: regional ou global, HTTP ou não, com ou sem API do Kubernetes, entrada ou saída, ordem garantida ou não. Erro bastante em mensageria (Service Bus, Filas do Armazenamento, Event Grid, Event Hubs) e em balanceamento (Load Balancer, Application Gateway, Front Door, Traffic Manager). Em rede, a pegadinha recorrente é Private Link sem DNS e emparelhamento que não é transitivo. Em migração, preciso lembrar que Site Recovery replica VMs e não leva para PaaS.

Neste capítulo

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

Tópicos-chave

Escolha de computação

VMs dão controle total do SO e permitem instalar agentes. App Service é o padrão para web e APIs sem gerenciar SO, com escala e slots. Functions atende processamento por evento pagando pelo uso. Container Apps serve microsserviços com escala até zero, revisões e Dapr, sem API do Kubernetes. AKS é para quem precisa da API do Kubernetes, CRDs e operadores.

Planos do Azure Functions

O Flex Consumption oferece instâncias sempre prontas, integração com VNet e escala rápida; o Premium também evita a inicialização a frio. O plano de consumo clássico pode ter inicialização a frio e não tem integração com VNet. Flex Consumption, Premium e Dedicado têm integração com VNet para saída.

Durable Functions x Logic Apps

Durable Functions faz fluxos com estado em código, com orquestrações, temporizadores, espera por eventos externos (aprovações) e o padrão fan-out/fan-in. Logic Apps integra sistemas com conectores prontos e pouco código; o Standard roda no runtime do Functions, em locatário único, com integração com VNet.

Azure Service Bus

Agente de mensagens corporativo com filas, tópicos e assinaturas filtradas (SQL ou correlação), sessões para ordem, transações, mensagens mortas e detecção de duplicatas pelo MessageId. O Premium usa recursos dedicados, aceita mensagens de até 100 MB e oferece Link Privado e zonas.

Event Grid, Event Hubs e Filas do Armazenamento

Event Grid distribui eventos discretos de serviços do Azure, como criação de recursos e blobs, com repetição exponencial e dead-lettering em blobs. Event Hubs é streaming de alto volume com partições, grupos de consumidores, endpoint Kafka e Captura para o data lake. Filas do Armazenamento são a fila simples e barata, sem ordem, sessões ou transações.

Padrões de arquitetura de nuvem

Claim-Check guarda o conteúdo grande em blob e manda só a referência. Circuit Breaker interrompe chamadas após falhas seguidas; Retry com espera exponencial trata falhas transitórias. CQRS separa leitura e gravação; Backends for Frontends dá um back-end por tipo de cliente; Strangler Fig moderniza aos poucos com fachada; Cache-Aside carrega o cache sob demanda; consumidores concorrentes e nivelamento de carga com fila aumentam vazão e suavizam picos.

Balanceamento de carga

Load Balancer atua na camada 4; o interno com portas HA é o padrão para NVAs em alta disponibilidade. Application Gateway é camada 7 regional, com WAF, terminação TLS e roteamento por caminho. Front Door é camada 7 global, com WAF, cache e filtro geográfico. Traffic Manager roteia por DNS e atende tráfego não HTTP. Para AKS, o Application Gateway for Containers usa a API Gateway ou Ingress do Kubernetes.

Azure Firewall e Firewall Manager

SKUs Basic, Standard e Premium; só o Premium tem inspeção de TLS e IDPS completo, baseado em assinaturas (o Basic é voltado a pequenas empresas). O Firewall Manager gerencia políticas com herança pai e filho e configura hubs virtuais protegidos no Virtual WAN, com intenção de roteamento. Combine Application Gateway com WAF e Azure Firewall quando houver HTTP e outros tráfegos para inspecionar.

Topologia hub-spoke e Virtual WAN

O hub concentra serviços compartilhados, como firewall e gateways, e UDRs forçam o tráfego dos spokes pelo firewall. O emparelhamento global liga VNets de regiões diferentes pela rede da Microsoft, sem gateways, cobra pela transferência de dados e não é transitivo. O Virtual WAN é a alternativa gerenciada para muitas filiais, com VPN site a site, ponto a site, ExpressRoute, trânsito entre hubs e parceiros de SD-WAN.

Regras de administrador de segurança

Definidas centralmente para todas as VNets, podem permitir, negar ou sempre permitir e têm precedência sobre os NSGs criados pelas equipes. NSGs comuns podem ser alterados pelas equipes; UDRs e DNS não filtram tráfego.

Conectividade híbrida

ExpressRoute com emparelhamento privado leva ao espaço privado; o emparelhamento da Microsoft usa endereços públicos dos serviços. VPN site a site é o backup de menor custo do ExpressRoute; máxima resiliência pede circuitos em locais de emparelhamento diferentes. Global Reach liga datacenters pelos circuitos. Gateways de VPN VpnGw1AZ a VpnGw5AZ resistem a falha de zona.

Private Link e DNS

Ponto de extremidade privado dá IP privado ao PaaS, mas o nome precisa resolver: o DNS local encaminha as zonas privatelink para o Azure, por exemplo com o DNS Private Resolver (ponto de entrada); para o Azure resolver nomes locais, ponto de saída com regras de encaminhamento. Em escala, zonas privadas centralizadas no hub e registros criados por política DeployIfNotExists.

Serviço de Link Privado e AMPLS

O serviço de Link Privado, atrás de um Load Balancer, publica um serviço próprio para consumidores de outras empresas por ponto privado, mesmo com endereços sobrepostos e sem emparelhamento. O Azure Monitor Private Link Scope (AMPLS) usa um ponto privado para vários recursos de monitoramento e exige atenção ao DNS.

Azure DDoS Protection

Network Protection protege a VNet inteira, com ajuste adaptativo, alertas, acesso a especialistas em resposta e proteção de custo. IP Protection é para poucos IPs públicos, com menor custo. Ambos tratam ataques volumétricos; ataques de camada 7 ficam com o WAF.

Azure API Management

Centraliza chaves de assinatura, políticas de limite de taxa (rate-limit-by-key, quota-by-key), cache, transformação, versionamento e portal do desenvolvedor. A política validate-jwt exige token válido do Entra. O gateway auto-hospedado roda em Docker ou Kubernetes perto de APIs locais. Várias regiões exigem o nível Premium; o Developer não tem SLA.

Ferramentas de migração

Azure Migrate é o hub: descoberta, avaliação, dependências, migração sem agente de VMware via vCenter, aplicativos web do IIS para App Service e avaliação de SQL. DMS online migra SQL Server para a Instância Gerenciada com pouca parada (BACPAC é offline). SSMA converte Oracle. Storage Mover migra NFS e SMB. Azure VMware Solution mantém vCenter e vSAN, com HCX. Rehospedar é a estratégia mais rápida.

Azure Arc

Servidores e clusters Kubernetes fora do Azure recebem ID de recurso, marcas, Azure Policy, extensões (como o Azure Monitor Agent) e Update Manager. Kubernetes habilitado pelo Arc aceita GitOps com Flux v2. Gerencia onde os recursos estão, sem migrar.

Rede e escala no AKS

Azure CNI Overlay faz só os nós usarem IPs da VNet. Cluster privado tira o IP público do servidor de API. Nós virtuais escalam para o ACI em segundos. KEDA escala pods por fontes como a fila do Service Bus, até zero; o autoescalador de cluster adiciona nós. Pools Spot usam taints para cargas tolerantes; o pool do sistema usa VMs regulares.

Macetes para memorizar

💡 Mensageria

Bus = negócio (ordem, transação); Grid = aviso (algo aconteceu); Hubs = rio (fluxo contínuo); Fila do Armazenamento = caixa simples.

💡 Balanceadores

Matriz 2x2: regional L4 = Load Balancer; regional L7 = Application Gateway; global L7 = Front Door; global por DNS/não HTTP = Traffic Manager. Global TCP com IP estático = Load Balancer entre regiões.

💡 Contêineres

Precisa falar com o Kubernetes? AKS. Só quer rodar contêineres Linux escalando a zero? Container Apps. Um contêiner isolado? ACI.

💡 Private Link

Ponto privado sem DNS é meio caminho: sempre pense em zona privatelink e encaminhamento.

💡 Rede do App Service

Ponto privado = porta de entrada; integração com VNet = porta de saída; Conexões Híbridas = túnel para uma porta local sem VPN.

💡 Escala no AKS

KEDA escala Pods; autoescalador de cluster escala Nós; nós virtuais pegam carona no ACI.

💡 Migração

Migrate descobre e avalia; Site Recovery replica VM; DMS leva banco; SSMA converte Oracle; Storage Mover leva compartilhamentos.

Tabela de memorização: não confunda

Quando é...	...e quando é
Azure Service Bus Precisa de ordem por cliente (sessões), transações, tópicos, mensagens mortas, duplicatas detectadas ou mensagens grandes no Premium.	**Filas do Armazenamento** Fila simples e barata para milhões de mensagens, sem ordem, sessões nem transações.

Event Grid Reagir a eventos discretos de serviços do Azure, como criação de recurso ou de blob, entregando a funções, webhooks e filas.	**Event Hubs** Ingerir milhões de eventos de telemetria por segundo com vários consumidores, Kafka ou Captura para o lago.
Azure Container Apps Microsserviços Linux com escala até zero, revisões e Dapr, sem operar Kubernetes.	**Azure Kubernetes Service** Controle total do cluster: API do Kubernetes, CRDs, operadores, políticas de rede próprias ou contêineres Windows.
Application Gateway Aplicativo regional com servidores privados na VNet, WAF, TLS e roteamento por caminho.	**Azure Front Door** Distribuição global com WAF na borda, cache, filtro geográfico e, no Premium, Link Privado para a origem.
DDoS IP Protection Proteger poucos IPs públicos com o menor custo.	**DDoS Network Protection** Muitos recursos críticos na VNet, com suporte de resposta, alertas e proteção de custo.
Ponto de extremidade privado do aplicativo Controlar a ENTRADA do aplicativo, recebendo um IP privado.	**Integração com VNet** Permitir a SAÍDA do aplicativo ou da função para recursos privados, como um SQL com ponto privado.
VPN site a site como backup Caminho alternativo de menor custo se o circuito falhar.	**Circuitos ExpressRoute em locais diferentes** Máxima resiliência, inclusive contra falha de um local de emparelhamento inteiro.

Números que caem

Item	Valor
Tamanho máximo de mensagem no Service Bus Premium	**até 100 MB**
SKUs de gateway de VPN com redundância de zona	**VpnGw1AZ a VpnGw5AZ**
SKUs do Azure Firewall	**Basic, Standard e Premium (só o Premium com inspeção de TLS e IDPS completo)**
GatewaySubnet	**só existe uma por VNet**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Uma fila do Service Bus para entregar cada pedido a três sistemas.
Como não cair: Uma fila entrega cada mensagem a um só consumidor. Para vários sistemas com filtros, use tópico com assinaturas filtradas.

⚠ **Alerta de prova:** Event Hubs ou Service Bus para disparar uma função quando um recurso é criado.
Como não cair: Eventos do Resource Manager e de blobs chegam pelo Event Grid com tópico de sistema.

⚠ **Alerta de prova:** Front Door Premium para um aplicativo regional que precisa de WAF.
Como não cair: Sem necessidade de distribuição global, a resposta é Application Gateway com WAF, que é regional.

⚠ **Alerta de prova:** Front Door ou Application Gateway para publicar APIs com chaves, limites e portal.
Como não cair: Eles roteiam tráfego, sem gestão de assinaturas de API. Use API Management.

⚠ **Alerta de prova:** Container Apps para imagens Windows ou para quem precisa de CRDs.
Como não cair: Container Apps executa só Linux e não expõe a API do Kubernetes. Use AKS (com pool de nós Windows, se for o caso).

⚠ **Alerta de prova:** Autoescalador de cluster sozinho para escalar pods pelo tamanho da fila.
Como não cair: Ele adiciona nós, sem olhar a fila. Escalar pods por evento, até zero, é KEDA.

⚠ **Alerta de prova:** Emparelhamento da Microsoft no ExpressRoute para acessar PaaS por IP privado.
Como não cair: Esse emparelhamento usa endereços públicos. Use ponto de extremidade privado e encaminhe o DNS das zonas privatelink (DNS Private Resolver). Pontos de extremidade de serviço não atendem redes locais.

⚠ **Alerta de prova:** Segundo circuito ExpressRoute no mesmo local de emparelhamento.
Como não cair: Custa mais e o local continua como ponto único. Menor custo: VPN site a site de backup; máxima resiliência: locais diferentes.

⚠ **Alerta de prova:** NSG restritivo ou WAF contra ataques volumétricos.
Como não cair: NSG não mitiga e WAF atua na camada 7. Volumétrico é DDoS Protection.

⚠ **Alerta de prova:** Azure Firewall Standard para inspeção de TLS e IDPS.
Como não cair: Inspeção de TLS e IDPS completo só no Firewall Premium.

⚠ **Alerta de prova:** Emparelhamento direto entre spokes quando todo tráfego deve ser inspecionado.
Como não cair: O emparelhamento direto contorna o firewall do hub. Use Azure Firewall no hub com UDRs.

⚠ **Alerta de prova:** Site Recovery para levar SQL Server à Instância Gerenciada ou sites IIS ao App Service.
Como não cair: Site Recovery replica VMs, não migra para PaaS. Use DMS online (ou link da Instância Gerenciada) e Azure Migrate para aplicativos web.

⚠ **Alerta de prova:** Restringir o App Service pelo IP do escritório para aceitar só o Front Door.
Como não cair: Os usuários chegam pelo Front Door. Use a marca de serviço AzureFrontDoor.Backend com o cabeçalho X-Azure-FDID, ou Front Door Premium com Link Privado.

⚠ **Alerta de prova:** Repetição contínua sem espera para lidar com serviço instável.
Como não cair: Repetir sem intervalo sobrecarrega o serviço. Falha transitória: Retry com espera exponencial; falhas seguidas: Circuit Breaker.

Como cai na prova

📝 **Como cai:** Requisito de computação com detalhe de controle do SO, contêiner ou cobrança por uso.
Como resolver: Pergunte: precisa de agente no SO ou acesso administrativo? VM. Web sem SO? App Service. Evento curto e paga pelo uso? Functions Flex Consumption. Microsserviço sem Kubernetes? Container Apps. API do Kubernetes ou Windows orquestrado? AKS.

📝 **Como cai:** Cenário de mensagens com palavras como ordem, filtro, volume, evento ou barato.
Como resolver: Ordem, transação, duplicata ou vários destinos filtrados: Service Bus (tópico). Evento do Azure: Event Grid. Telemetria massiva ou Kafka: Event Hubs. Simples e barato: Filas do Armazenamento.

📝 **Como cai:** Escolha de balanceador ou proteção na borda.
Como resolver: Defina escopo (regional ou global) e camada (HTTP ou não). Acrescente proteção: WAF para camada 7, DDoS para volumétrico, Firewall Premium para TLS e IDPS.

📝 **Como cai:** Acesso privado a PaaS a partir do datacenter ou de outra VNet.
Como resolver: Ponto de extremidade privado mais DNS (zonas privatelink e DNS Private Resolver). Descarte firewall com IP público, emparelhamento da Microsoft e ponto de extremidade de serviço para redes locais.

📝 **Como cai:** Migração com prazo, tempo de parada ou mudança de mecanismo.
Como resolver: Prazo curto sem mudar código: rehospedar com Azure Migrate. SQL com pouca parada: migração online pelo DMS. Oracle: SSMA. Antes de tudo, descoberta e avaliação no Azure Migrate.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Integrar Outlook, SharePoint e Salesforce com poucos ou nenhum código	**Azure Logic Apps**
Fluxo em código que espera dias por aprovação e mantém estado	**Durable Functions**
Processar mil arquivos em paralelo e consolidar ao final	**Fan-out/fan-in do Durable Functions**
Anexos maiores que o limite da fila	**Padrão Claim-Check com o conteúdo em blob**
Ordem por cliente, mensagens mortas e duplicatas	**Service Bus com sessões**
Produtores Kafka existentes sem mudar código	**Event Hubs com endpoint Kafka**
Dispositivos com identidade individual que recebem comandos	**Azure IoT Hub (IoT Edge se precisar processar offline)**
Milhares de tarefas paralelas em pools criados e removidos automaticamente	**Azure Batch (VMs HPC com InfiniBand para MPI)**
TCP de NVAs em alta disponibilidade em todas as portas	**Load Balancer interno com portas HA**
NVAs de SD-WAN trocando rotas por BGP	**Azure Route Server**
Expor serviço próprio a outra empresa por IP privado, sem emparelhamento	**Serviço de Link Privado com Load Balancer**
App Service acessa porta TCP de banco local sem VPN	**Conexões Híbridas do App Service**
Isolamento de locatário único, dentro da VNet, só IP privado	**Ambiente do App Service v3**
Mover VMware rápido mantendo vCenter e vSAN	**Azure VMware Solution**

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

- Emparelhamento de VNets não é transitivo e contorna o firewall se for direto entre spokes.
- Fila entrega a um consumidor; tópico entrega a vários assinantes filtrados.
- Container Apps é só Linux e não expõe a API do Kubernetes.
- Ponto de extremidade privado sempre vem acompanhado de solução de DNS.
- Site Recovery replica VMs; para PaaS use DMS, link da Instância Gerenciada ou Azure Migrate para aplicativos web.

Essenciais para a prova (checklist)

- ☐ Sei escolher entre VM, App Service, Functions, Container Apps, AKS, ACI e Batch pelo requisito.
- ☐ Sei a diferença entre os planos Consumo clássico, Flex Consumption e Premium do Functions.

- ☐ Sei escolher entre Service Bus, Filas do Armazenamento, Event Grid e Event Hubs.
- ☐ Sei reconhecer os padrões Claim-Check, Circuit Breaker, Retry, CQRS, BFF, Strangler Fig, Cache-Aside e nivelamento de carga.
- ☐ Sei escolher entre Load Balancer, Application Gateway, Front Door e Traffic Manager.
- ☐ Sei desenhar hub-spoke com Azure Firewall e UDR e quando usar Virtual WAN.
- ☐ Sei configurar ponto de extremidade privado com DNS Private Resolver e zonas centralizadas.
- ☐ Sei escolher entre VPN de backup, circuitos em locais diferentes e Global Reach no ExpressRoute.
- ☐ Sei quais recursos do API Management atendem limite de taxa, validação de token, gateway local e várias regiões.
- ☐ Sei qual ferramenta de migração usar para VMware, SQL Server, Oracle, sites IIS e compartilhamentos.

Questões de revisão do capítulo

R4.1 · Projetar soluções de infraestrutura

Mensagens com anexos de 500 MB precisam passar por uma fila sem exceder os limites de tamanho do serviço. Qual padrão recomendar?

A. Padrão Claim-Check com o anexo em blob
B. Padrão Sharding das mensagens grandes na fila
C. Padrão Strangler Fig da fila
D. Padrão Cache-Aside do anexo

R4.2 · Projetar soluções de infraestrutura

Servidores de desenvolvimento ficam com CPU baixa quase o tempo todo, com picos ocasionais. Qual família de VM reduz o custo?

A. Série M, de memória
B. Série N, com GPU
C. Série L, de armazenamento
D. Série B, expansível

R4.3 · Projetar soluções de infraestrutura

A empresa quer proteger apenas dois IPs públicos contra ataques volumétricos, com o menor custo. O que recomendar?

A. DDoS Network Protection na VNet
B. DDoS IP Protection nesses IPs
C. NSG com regras de entrada
D. WAF no Front Door

R4.4 · Projetar soluções de infraestrutura

Várias instâncias de um serviço devem processar mensagens da mesma fila em paralelo, para aumentar a vazão. Qual padrão recomendar?

A. Padrão Strangler Fig com fachada
B. Padrão de consumidores concorrentes
C. Padrão Sharding por cliente
D. Padrão Claim-Check com blobs

Respostas comentadas

R4.1. A) Padrão Claim-Check com o anexo em blob

Por quê: No Claim-Check, o conteúdo grande fica em um armazenamento, e a mensagem carrega uma referência.

✗ B) Incorreta. Particiona dados, sem resolver o tamanho.
✗ C) Incorreta. Moderniza sistemas.
✗ D) Incorreta. Trata leituras em cache.

> **Dica de prova:** Mensagem grande: Claim-Check.

R4.2. D) Série B, expansível

Por quê: A série B é indicada para cargas com uso médio baixo, como desenvolvimento, testes e servidores pequenos.

✗ A) Incorreta. É para grandes bancos em memória.
✗ B) Incorreta. É para gráficos e IA.
✗ C) Incorreta. É para alto desempenho de disco.

> **Dica de prova:** CPU baixa com picos: série B.

R4.3. B) DDoS IP Protection nesses IPs

Por quê: O DDoS IP Protection é indicado para poucos IPs. O Network Protection adiciona suporte de resposta e proteção de custo.

✗ A) Incorreta. Atende muitos recursos com custo fixo maior.
✗ C) Incorreta. Não mitiga ataques volumétricos.
✗ D) Incorreta. Trata ataques de camada 7.

> **Dica de prova:** Poucos IPs: DDoS IP Protection.

R4.4. B) Padrão de consumidores concorrentes

Por quê: Consumidores concorrentes escalam o processamento e aumentam a resiliência, exigindo mensagens idempotentes.

✗ A) Incorreta. Moderniza sistemas aos poucos.

✗ C) Incorreta. Particiona dados.

✗ D) Incorreta. Trata mensagens grandes.

> **Dica de prova:** Vários leitores na mesma fila: consumidores concorrentes.

DIA DA PROVA

Estratégia de prova

A AZ-305 é uma prova de arquiteto: quase todo enunciado descreve um requisito de negócio curto e pergunta o que recomendar, com quatro serviços reais e plausíveis. A diferença entre certa e errada está em um detalhe do requisito: escopo (zona, região, global), protocolo (HTTP ou não), verbo (impedir ou avisar), custo (menor custo, menor esforço de gestão) ou restrição (sem senha, sem acesso público, sem mudar código). As alternativas erradas costumam ser serviços que resolvem um problema vizinho, como avisar em vez de bloquear, replicar em vez de fazer backup ou atuar na camada errada. Também aparecem itens de múltipla resposta que pedem as duas peças complementares de uma mesma solução.

Como responder

✓ Administre o tempo: são cerca de 50 itens em 100 minutos, cerca de 2 minutos cada; a Microsoft varia entre 40 e 60, então recalcule ao ver o total.

✓ Priorize a revisão pelos pesos: infraestrutura (30-35%) e identidade, governança e monitoramento (25-30%) somam mais da metade; dados (20-25%) e continuidade (15-20%) completam.

✓ Leia primeiro a última frase (o que recomendar) e depois grife no enunciado as restrições: menor custo, menor esforço, sem segredos, sem acesso público, sem mudar código.

✓ Elimine alternativas de outra categoria de serviço (Batch, Bastion, Advisor, log de atividades costumam ser distratores fora de contexto) antes de comparar as plausíveis.

✓ Nos itens Escolha DUAS, procure duas peças que se complementam na mesma solução, não duas soluções alternativas.

✓ Em cenários de resiliência, decida primeiro o escopo da falha (servidor, zona, região) e o RPO e RTO; só depois escolha o serviço.

✓ Quando duas opções atendem, a pergunta normalmente decide por custo ou esforço: escolha a mais barata ou mais gerenciada que ainda cumpre todos os requisitos.

✓ A nota mínima é 700 numa escala de 1 a 1000, com itens de múltipla escolha e de múltipla resposta; nos de múltipla resposta, confira quantas alternativas o enunciado pede.

Erros que derrubam candidatos

✗ Escolher algo que avisa ou recomenda (orçamento, Advisor, Audit, alertas) quando o requisito é impedir ou configurar automaticamente.

✗ Proteger contra a falha errada: redundância de zona para desastre regional ou conjunto de disponibilidade para falha de zona.

✗ Confundir serviços de mensageria e de balanceamento por não checar ordem, volume, protocolo e escopo regional ou global.

✗ Esquecer o DNS ao usar pontos de extremidade privados ou supor que emparelhamento de VNets é transitivo.

✗ Confundir TDE, Always Encrypted e máscara dinâmica, ou Banco de Dados SQL com Instância Gerenciada.

✗ Usar B2B, contas de usuário ou segredos em código onde cabem External ID, identidades gerenciadas ou federação.

✗ Ignorar o critério de menor custo e escolher a solução mais robusta quando uma mais barata já atende.

Na semana da prova

- ☐ Refaça as provas práticas e, em cada erro, anote qual detalhe do enunciado deveria ter levado à resposta certa.
- ☐ Revise as tabelas de comparação de cada capítulo: mensageria, balanceadores, opções de SQL, consistência do Cosmos DB e redundância de armazenamento.
- ☐ Repasse os gatilhos e macetes em voz alta até responder cada um sem pensar.
- ☐ Revise licenças do Entra (P1 x P2), efeitos do Azure Policy e as opções de redução de custo do Log Analytics.
- ☐ Na véspera, revise só as listas de lembrar e os checklists de cada domínio, conferindo se sabe responder cada item do checklist.

REVISÃO FINAL

Folha de cola

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

1. Projetar soluções de armazenamento de dados

‣ Uso poucas horas por dia em horários imprevisíveis no SQL → **Camada sem servidor com pausa automática**

‣ Dezenas de bancos SaaS pequenos com picos em horários diferentes → **Pool elástico**

‣ Relatórios na réplica do Business Critical → **ApplicationIntent=ReadOnly na conexão**

‣ Várias equipes de BI com réplicas isoladas do Hyperscale → **Réplicas nomeadas**

‣ Provar criptograficamente que registros não foram adulterados → **Tabelas de razão (ledger)**

⚠ Com TDE os administradores veem os dados. Esconder até do DBA é Always Encrypted.

⚠ Always Encrypted exige alterações no cliente e esconde tudo. Exibição parcial é máscara dinâmica de dados.

⚠ Máscara só esconde valores. Classificar: descoberta e classificação. Provar integridade: ledger. Registrar acessos: auditoria do SQL.

2. Projetar soluções de continuidade de negócios

‣ RPO de 15 minutos e RTO de 2 horas para falha regional de VMs → **Azure Site Recovery para região secundária**

‣ DR barato no SQL, RPO de cerca de uma hora → **Restauração geográfica com backup GRS**

‣ Failover regional do SQL com o mesmo ponto de conexão → **Grupo de failover com ouvintes**

‣ SQL Server 2022 local com réplica de DR na nuvem → **Link da Instância Gerenciada**

‣ Backups completos semanais por dez anos no SQL → **Retenção de longo prazo (LTR)**

⚠ Zona protege só dentro da região. Falha regional exige grupo de failover, réplica geográfica ou restauração geográfica.

⚠ O conjunto fica em um datacenter. Para zona, distribua VMs em zonas atrás de um Load Balancer Standard.

⚠ Slots ficam nas mesmas instâncias e região; o Basic não tem redundância de zona. Use Premium v2, v3 ou v4 com redundância de zona, ou duas regiões com Front Door.

3. Projetar soluções de identidade, governança e monitoramento

‣ Correlacionar eventos de várias fontes, detectar ameaças e automatizar respostas → **Microsoft Sentinel (SIEM e SOAR)**

‣ Função só quando precisar, com aprovação e tempo limitado → **PIM com atribuições qualificadas**

‣ A cada trimestre gestores confirmam quem continua → **Revisões de acesso recorrentes**

‣ Parceiros solicitam acesso com aprovação e expiração automática → **Pacotes de acesso no gerenciamento de direitos**

‣ LDAP, Kerberos e ingresso no domínio sem manter controladores → **Microsoft Entra Domain Services**

⚠ Orçamento avisa e Advisor sugere, mas nenhum impede a criação. Use a política de SKUs de VM permitidos (Deny).

⚠ Bloqueios só impedem alterar ou excluir o recurso. Não controlam entrada, não rotacionam, não validam marcas e nem se aplicam a grupos do Entra.

⚠ NSG não protege o Entra ID. Bloqueio por país na entrada é com locais nomeados no Acesso Condicional.

4. Projetar soluções de infraestrutura

‣ Integrar Outlook, SharePoint e Salesforce com poucos ou nenhum código → **Azure Logic Apps**

‣ Fluxo em código que espera dias por aprovação e mantém estado → **Durable Functions**

‣ Processar mil arquivos em paralelo e consolidar ao final → **Fan-out/fan-in do Durable Functions**

‣ Anexos maiores que o limite da fila → **Padrão Claim-Check com o conteúdo em blob**

‣ Ordem por cliente, mensagens mortas e duplicatas → **Service Bus com sessões**

⚠ Uma fila entrega cada mensagem a um só consumidor. Para vários sistemas com filtros, use tópico com assinaturas filtradas.

⚠ Eventos do Resource Manager e de blobs chegam pelo Event Grid com tópico de sistema.

⚠ Sem necessidade de distribuição global, a resposta é Application Gateway com WAF, que é regional.

GABARITO

Respostas do diagnóstico

D1. C) Descoberta e classificação de dados → revise o capítulo 1

Por quê: Os rótulos aparecem nos logs de auditoria, mostrando quem acessou dados sensíveis.

✗ A) Incorreta. Trata desempenho.
✗ B) Incorreta. Esconde valores, sem classificar.
✗ D) Incorreta. Não classifica dados.

> **Dica de prova:** Rotular colunas sensíveis: descoberta e classificação.

D2. D) Extensão pgvector no servidor flexível → revise o capítulo 1

Por quê: O pgvector está disponível no PostgreSQL servidor flexível. O Azure AI Search e o Cosmos DB também oferecem busca vetorial.

✗ A) Incorreta. Não fazem busca.
✗ B) Incorreta. Não é banco de dados.
✗ C) Incorreta. Não fazem busca vetorial.

> **Dica de prova:** Vetores no PostgreSQL: pgvector.

D3. D) Data Lake Storage com ACLs por pasta → revise o capítulo 1

Por quê: O Data Lake Storage combina o Armazenamento de Blobs com namespace hierárquico, ACLs POSIX e integração com Fabric, Databricks e Synapse.

✗ A) Incorreta. Um banco não é armazenamento de arquivos do lago.
✗ B) Incorreta. A chave dá acesso total ao compartilhamento.
✗ C) Incorreta. Sem namespace, não há ACLs por pasta.

> **Dica de prova:** Lago com permissões por pasta: Data Lake Storage.

D4. C) Duas regiões, Front Door e grupo de failover → revise o capítulo 2

Por quê: Cada camada precisa da própria estratégia regional: roteamento global, computação duplicada e dados replicados.

✗ A) Incorreta. Tem RTO alto.
✗ B) Incorreta. Não cobre falha de região.
✗ D) Incorreta. Slots ficam na mesma região.

> **Dica de prova:** DR web + SQL: duas regiões + Front Door + grupo de failover.

D5. A) Bloqueio CanNotDelete na conta → revise o capítulo 2

Por quê: Contas excluídas podem ser recuperadas em alguns casos, mas o bloqueio evita o problema.

✗ B) Incorreta. Não protege a conta.

✗ C) Incorreta. Não protege contra exclusão.

✗ D) Incorreta. Não protege contra exclusão.

> **Dica de prova:** Evitar excluir a conta: bloqueio CanNotDelete.

D6. A) Link da Instância Gerenciada → revise o capítulo 2

Por quê: O link usa grupos de disponibilidade distribuídos e permite failover para a nuvem e de volta.

✗ B) Incorreta. Tem RPO alto.

✗ C) Incorreta. Tem RPO muito alto.

✗ D) Incorreta. Replica a VM, não para a Instância Gerenciada.

> **Dica de prova:** DR do SQL Server local na nuvem: link da Instância Gerenciada.

D7. C) Grupo Sandbox com políticas que negam conexões → revise o capítulo 3

Por quê: Nas zonas de aterrissagem, o grupo Sandbox recebe políticas mais permissivas, mas isoladas da conectividade corporativa.

✗ A) Incorreta. Misturar ambientes compartilha políticas e conectividade.

✗ B) Incorreta. Marcas não bloqueiam conexões.

✗ D) Incorreta. Revisões não impedem conexões de rede.

> **Dica de prova:** Sandbox isolado: grupo de gerenciamento próprio com políticas.

D8. C) Limite diário de ingestão → revise o capítulo 3

Por quê: O limite diário é útil em ambientes de teste. Em produção, pode causar perda de dados importantes e deve ser usado com cuidado.

✗ A) Incorreta. Não reduz o volume total.

✗ B) Incorreta. Não limitam a ingestão.

✗ D) Incorreta. Aumenta o custo de retenção.

> **Dica de prova:** Evitar surpresa de ingestão: limite diário.

D9. D) Locais nomeados no Acesso Condicional → revise o capítulo 3

Por quê: Locais nomeados podem ser definidos por país ou faixa de IP e usados para bloquear ou exigir controles adicionais.

✗ A) Incorreta. NSGs não protegem o Entra ID.

✗ B) Incorreta. Protege só o banco.

✗ C) Incorreta. Não bloqueiam entradas.

> **Dica de prova:** Bloquear países na entrada: locais nomeados.

D10. D) SKU com redundância de zona → revise o capítulo 4

Por quê: Os SKUs VpnGw1AZ a VpnGw5AZ usam IPs públicos Standard redundantes entre zonas.

✗ A) Incorreta. Só existe uma GatewaySubnet por VNet.

✗ B) Incorreta. Não oferece redundância de zona.

✗ C) Incorreta. O IP Basic foi desativado.

> **Dica de prova:** VPN resistente a zona: SKU AZ.

D11. C) Migração sem agente do Azure Migrate → revise o capítulo 4

Por quê: A migração sem agente usa o dispositivo do Azure Migrate conectado ao vCenter e permite testes antes da virada.

✗ A) Incorreta. Exige reinstalar tudo.

✗ B) Incorreta. É manual e sujeita a erros.

✗ D) Incorreta. Não migra VMs.

> **Dica de prova:** VMware para Azure sem agentes: Azure Migrate.

D12. D) Detecção de duplicatas do Service Bus → revise o capítulo 4

Por quê: A detecção de duplicatas usa o MessageId. Consumidores idempotentes continuam sendo boa prática.

✗ A) Incorreta. Não detecta duplicatas.

✗ B) Incorreta. Pode entregar eventos repetidos.

✗ C) Incorreta. Não detectam duplicatas.

> **Dica de prova:** Evitar duplicatas na fila: detecção de duplicatas.

Agora, treine no formato real

Faça as 6 provas completas do curso AZ-305: 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.