Strecht Simulados · Guia de preparação



Guia de preparação AZ-104

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.

5
capítulos por domínio

32
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-104: 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. Gerenciar identidades e governança do Azure	20-25%	18 conceitos · 14 pegadinhas
2. Implantar e gerenciar recursos de computação	20-25%	18 conceitos · 14 pegadinhas
3. Implementar e gerenciar armazenamento	15-20%	18 conceitos · 14 pegadinhas
4. Implementar e gerenciar redes virtuais	15-20%	18 conceitos · 14 pegadinhas
5. Monitorar e manter recursos do Azure	10-15%	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 · Gerenciar identidades e governança do Azure

Um usuário diz que consegue excluir uma VM, e o administrador quer ver todas as atribuições de função que dão acesso a ele nesse recurso, inclusive as herdadas. Onde verificar?

A. Log de atividades do recurso
B. Recurso Verificar acesso, no IAM
C. Conformidade do Azure Policy
D. Recomendações do Azure Advisor para o recurso

D2 · Gerenciar identidades e governança do Azure

Todos os recursos precisam da marca CentroCusto. Se ela estiver ausente, deve ser copiada do grupo de recursos na criação ou atualização. Qual abordagem atende?

A. Política com efeito Modify que herda a marca do grupo
B. Bloqueio Excluir aplicado no grupo de recursos
C. Função personalizada com permissão de gravar marcas
D. Política com efeito Audit que lista os recursos sem marca

D3 · Gerenciar identidades e governança do Azure

Ao criar um grupo de recursos, é preciso escolher uma região. O que essa região define?

A. A região para onde vão os backups
B. A moeda usada no faturamento
C. Onde ficam os metadados do grupo
D. A região obrigatória de todos os recursos

D4 · Implantar e gerenciar recursos de computação

Um contêiner de limpeza deve rodar todos os dias às 2h no Azure Container Apps e terminar ao concluir. O que usar?

A. Slot de implantação diário
B. Revisão com escala até zero
C. Job com gatilho agendado
D. Grupo do ACI com política Always

D5 · Implantar e gerenciar recursos de computação

O administrador precisa executar um comando do PowerShell em uma VM Windows sem abrir RDP e sem instalar nada. O que usar?

A. Recomendações do Azure Advisor
B. Extensão de antimalware da VM
C. Diagnóstico de inicialização da VM
D. Recurso Executar comando da VM

D6 · Implantar e gerenciar recursos de computação

Uma VM precisa passar para outra VNet na mesma região. Como fazer?

A. Mover a VM para outro grupo de recursos
B. Emparelhar as VNets e mover a NIC
C. Recriar a VM na nova VNet com os discos
D. Trocar a sub-rede da NIC para a outra VNet

D7 · Implementar e gerenciar armazenamento

Blobs de um contêiner devem ser copiados de forma assíncrona para uma conta da empresa em outra região, onde outra equipe vai ler e processar os dados. O que usar?

A. Replicação de objetos entre as contas
B. Exclusão temporária na conta de origem
C. Política de ciclo de vida na origem
D. Redundância GRS na conta de origem

D8 · Implementar e gerenciar armazenamento

Um aplicativo precisa de compartilhamentos do Azure Files em SSD, com baixa latência e alto IOPS. Qual tipo de conta criar?

A. Conta Standard de uso geral v2 com GZRS
B. Conta premium do tipo BlockBlobStorage
C. Conta premium do tipo FileStorage
D. Conta Standard de uso geral v2 com camada Hot

D9 · Implementar e gerenciar armazenamento

Aplicativos usam a chave primária de uma conta de armazenamento. Como rotacionar a chave sem interromper os aplicativos?

A. Criar uma nova conta e copiar os dados para ela
B. Mudar a redundância da conta e regenerar a primária
C. Usar a chave secundária e regenerar a primária
D. Regenerar as duas chaves ao mesmo tempo no portal

D10 · Implementar e gerenciar redes virtuais

Em um hub-spoke, o tráfego do spoke1 para o spoke2 passa por uma NVA no hub, com rotas definidas, mas é descartado ao entrar no spoke2. O que habilitar nos emparelhamentos?

A. Usar gateway remoto nos spokes
B. Permitir tráfego encaminhado
C. Ponto de extremidade de serviço
D. Registro automático de DNS

D11 · Implementar e gerenciar redes virtuais

Um NSG tem a regra 100, que nega a porta 3389 de qualquer origem, e a regra 200, que permite a porta 3389 do IP do administrador. O que acontece com o RDP do administrador?

A. É liberado, pois a origem é mais específica
B. É negado, pois a regra 100 é avaliada antes da 200
C. É liberado, pois regras de permissão prevalecem
D. Depende da ordem em que as regras foram criadas

D12 · Implementar e gerenciar redes virtuais

Um aplicativo antigo guarda a sessão na memória do servidor, e cada cliente deve voltar à mesma VM atrás do Load Balancer. O que configurar?

A. Persistência de sessão por IP do cliente
B. Investigação de integridade TCP na porta
C. Regra de NAT de entrada para cada VM
D. Tempo limite de ociosidade maior na regra

01

CAPÍTULO 1 · 20-25% DA PROVA

Gerenciar identidades e governança do Azure

Aqui eu preciso separar com clareza três mecanismos: funções do Microsoft Entra (gerenciam usuários e grupos), Azure RBAC (o que alguém pode fazer nos recursos) e Azure Policy (quais propriedades os recursos podem ter), além de bloqueios, marcas, grupos de gerenciamento e Cost Management. A prova adora cenários de menor privilégio, mensagens de erro como RequestDisallowedByPolicy e questões de Escolha DUAS sobre escopos, bloqueios e marcas. Também cai administração do Entra: exclusão e restauração de usuários, grupos dinâmicos, unidades administrativas, B2B, licenças e SSPR. Onde mais erro: achar que Proprietário gerencia usuários do Entra, que marcas são herdadas sozinhas e que NotActions é uma negação.

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

Tópicos-chave

Funções do Entra x Azure RBAC

Funções do Microsoft Entra, como Administrador de Usuários e Administrador Global, controlam objetos do diretório; funções do Azure RBAC, como Proprietário e Colaborador, controlam recursos. São sistemas separados: um Administrador Global sem acesso às assinaturas precisa ativar o gerenciamento de acesso para recursos (elevar acesso), de forma temporária e removida depois do uso.

RBAC aditivo

O Azure RBAC soma as permissões de todas as atribuições: Leitor na assinatura mais Colaborador em RG1 permite gerenciar RG1. Atribuições não têm prioridade numérica nem conflito, e o escopo amplo não restringe o específico. Só atribuições de negação removem acesso, e são criadas pelo Azure em casos específicos, como Blueprints e aplicativos gerenciados.

Escopos e herança do RBAC

Funções podem ser atribuídas em grupo de gerenciamento, assinatura, grupo de recursos ou recurso, e se propagam para tudo abaixo, inclusive assinaturas já existentes. Menor privilégio é a função interna mais específica no menor escopo: um fornecedor que só reinicia vm-erp01 recebe a função no escopo da própria VM. Verificar acesso, no IAM, lista as funções de alguém com o escopo de origem de cada uma.

Entidades de segurança

Recebem funções do RBAC: usuários, grupos, entidades de serviço e identidades gerenciadas. Unidades administrativas, marcas e grupos de recursos não são identidades. Atribuir a função a um grupo de segurança reduz o número de atribuições e respeita o limite por assinatura quando a equipe muda muito.

Quem concede acesso e quem gerencia bloqueios

Atribuir funções exige Microsoft.Authorization/roleAssignments/write, presente em Proprietário, Administrador de Acesso do Usuário e Administrador de Controle de Acesso Baseado em Função; Colaborador não atribui funções. Criar ou excluir bloqueios exige Microsoft.Authorization/locks/*, presente em Proprietário e Administrador de Acesso do Usuário.

Funções personalizadas

Usadas quando nenhuma função interna atende, como ver e reiniciar VMs (virtualMachines/read e virtualMachines/restart/action). Definem Actions, NotActions e AssignableScopes, que aceita grupos de gerenciamento, assinaturas e grupos de recursos. NotActions só subtrai ações do conjunto concedido; se outra atribuição conceder a ação, o usuário a terá.

Funções de plano de dados

Leitor e Colaborador atuam no plano de controle; para ler o conteúdo, são necessárias funções de dados, como Leitor de Dados de Blob de Armazenamento. No Key Vault com modelo RBAC, Usuário de Segredos do Key Vault lê o valor dos segredos, enquanto Leitor do Key Vault lê só metadados e Colaborador do Key Vault gerencia o cofre sem ver o conteúdo. Identidade gerenciada mais função de dados evita guardar segredos.

Ciclo de vida de usuários no Entra

Usuário excluído fica em Usuários excluídos por 30 dias e pode ser restaurado com as associações a grupos; recriar geraria outro ID. Para impedir a entrada sem excluir, bloqueia-se a entrada (conta desabilitada) e revogam-se as sessões; remover a licença não impede a entrada. Muitos usuários pelo portal: criação em massa com modelo CSV; licença exige o local de uso preenchido.

Grupos, dinâmicos e licenciamento

Grupos dinâmicos usam regras sobre atributos, como departamento igual a Vendas, exigem Entra ID P1 ou superior e só a regra define os membros, sem inclusão manual. Proprietários de grupo gerenciam membros sem função administrativa no diretório. O licenciamento baseado em grupo adiciona ou remove licenças conforme a entrada e saída do grupo.

Unidades administrativas

Restringem o escopo de funções do Entra a um conjunto de usuários, grupos ou dispositivos, como o administrador da filial de Recife que só redefine senhas dos usuários de lá. Não importam usuários, não atribuem licenças e não restringem convites.

Colaboração B2B (External ID)

O parceiro é convidado como usuário convidado e entra com a conta da própria organização; para acessar recursos, precisa receber uma função do Azure RBAC como qualquer usuário. Convidados podem entrar em grupos, têm permissões padrão restritas no diretório e não exigem P2. As configurações de colaboração externa definem quem pode convidar (por exemplo, só administradores e Emissor de Convites) e restrições de domínio.

Licenças do Entra, SSPR e sincronização

P1 adiciona Acesso Condicional, grupos dinâmicos e write-back de senha; P2 adiciona ID Protection e PIM; padrões de segurança e convites B2B são gratuitos. A SSPR define escopo (Nenhum, Selecionado, Todos), métodos e quantos são exigidos, e para usuários híbridos exige write-back de senha no Entra Connect Sync ou Cloud Sync. A sincronização de hash de senha mantém a entrada funcionando mesmo com o AD local indisponível; autenticação de passagem e AD FS dependem do local.

Efeitos do Azure Policy

Deny recusa a criação (erro RequestDisallowedByPolicy, válido até para proprietários); Audit só registra; Modify altera propriedades como marcas na criação ou atualização; Append adiciona campos ao recurso; DeployIfNotExists implanta o recurso relacionado que falta com a identidade gerenciada da atribuição; AuditIfNotExists só registra a ausência. Políticas internas comuns: Locais permitidos, Tipos de recursos não permitidos, Exigir uma marca e Herdar uma marca do grupo de recursos.

Atribuição, avaliação e correção de políticas

O enforcementMode DoNotEnforce mostra a conformidade sem aplicar o efeito; isenções (Waiver ou Mitigated) podem ter data de expiração e valer para um escopo específico. A avaliação ocorre após a atribuição, na criação ou alteração, a cada 24 horas e sob demanda com az policy state trigger-scan. Recursos existentes são corrigidos com Modify ou DeployIfNotExists mais tarefa de correção, cuja identidade gerenciada precisa de permissão de gravação; iniciativas agrupam políticas, e a definição salva no grupo de gerenciamento pode ser atribuída nas assinaturas abaixo.

Bloqueios de recurso

CanNotDelete permite ler e alterar (parar, iniciar, redimensionar) mas não excluir; ReadOnly permite só ler. Valem para todos, inclusive proprietários, são aplicados em assinatura, grupo de recursos ou recurso (não em grupo de gerenciamento) e herdados pelos filhos; o erro é ScopeLocked. Atuam no plano de controle: ReadOnly numa conta de armazenamento bloqueia a listagem de chaves, que é um POST.

Marcas de recursos

Metadados nome-valor, até 50 pares por recurso, criados por portal, CLI, PowerShell, modelos ou API. Não são herdadas do grupo nem da assinatura sem política (Modify) e não controlam permissões. Servem para organizar e agrupar custos na análise de custos.

Hierarquia: grupos de gerenciamento, assinaturas e grupos de recursos

Todo diretório tem um grupo de gerenciamento raiz, com até seis níveis abaixo; cada grupo ou assinatura tem um único pai, e mover a assinatura troca a herança para a do novo pai. A região do grupo de recursos guarda só os metadados; excluir o grupo exclui os recursos; mover recursos muda o ID mas não a região, e entre assinaturas exige o mesmo locatário. Transferir a assinatura para outro diretório remove as atribuições de função, e atribuições, funções personalizadas e identidades gerenciadas precisam ser recriadas no novo diretório; MissingSubscriptionRegistration pede registrar o provedor, e limite de vCPUs pede aumento de cota da família na região.

Cost Management e economia

A análise de custos agrupa por serviço, grupo, região ou marca; orçamentos (em grupo de recursos, assinatura ou grupo de gerenciamento) alertam sobre custo real ou previsto e só agem por grupo de ações com runbook, função ou Logic App; alertas de anomalia avisam desvios sem valor fixo; exportações agendadas geram CSV ou Parquet. A calculadora de preços estima antes de implantar, o Advisor (categoria Custo) aponta VMs subutilizadas, e para VMs 24x7 com licenças combinam-se reserva e Benefício Híbrido do Azure.

Macetes para memorizar

Entra x RBAC

Entra cuida de gente; RBAC cuida de coisa.

Três mecanismos de governança

RBAC soma quem pode, Policy barra o que não pode existir, Lock trava até para o dono.

Bloqueios

CanNotDelete: mexe mas não apaga. ReadOnly: só olha (nem lista chave).

Efeitos de política

Deny nega, Audit anota, Modify mexe, DINE implanta o que falta.

Códigos de erro

Policy = RequestDisallowedByPolicy; Lock = ScopeLocked; RBAC = AuthorizationFailed; provedor = MissingSubscriptionRegistration.

Licenças do Entra

P1 = Acesso Condicional, grupos dinâmicos e write-back de senha; P2 = PIM e ID Protection; convite B2B e padrões de segurança = grátis.

NotActions

NotActions tira do pacote, não proíbe.

Tabela de memorização: não confunda

Quando é...	...e quando é
Função do Microsoft Entra Criar usuários, redefinir senhas, gerenciar objetos do diretório.	**Função do Azure RBAC** Gerenciar ou ler recursos do Azure em um escopo.
Azure Policy Restringir propriedades dos recursos (região, SKU, tipo, marca), valendo até para proprietários.	**Azure RBAC** Definir o que cada identidade pode fazer nos recursos.
Bloqueio CanNotDelete Evitar exclusão acidental, mantendo alterações de configuração.	**Bloqueio ReadOnly** Congelar o recurso, bloqueando também alterações e operações POST como listar chaves.
Efeito Deny Recusar recurso sem a marca obrigatória.	**Efeito Modify** Adicionar ou herdar a marca automaticamente na criação ou atualização.
DeployIfNotExists Implantar a extensão ou recurso relacionado que falta.	**AuditIfNotExists** Apenas registrar que o recurso relacionado não existe.
Unidade administrativa Delegar gestão do Entra a um subconjunto de usuários, grupos ou dispositivos.	**Grupo de gerenciamento** Organizar assinaturas e herdar políticas e funções do Azure.
Sincronização de hash de senha Mesma senha com entrada funcionando mesmo com o AD local fora do ar.	**Autenticação de passagem** Validar a senha nos agentes locais, dependendo da infraestrutura local.

Números que caem

Item	Valor
Prazo para restaurar usuário excluído no Entra	**30 dias**
Marcas por recurso	**Até 50 pares nome-valor**
Níveis de grupos de gerenciamento abaixo da raiz	**Até seis**
Avaliação periódica do Azure Policy	**A cada 24 horas (ou sob demanda com trigger-scan)**
Licença mínima para grupos dinâmicos e Acesso Condicional	**Microsoft Entra ID P1**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Dar Colaborador, Proprietário ou Administrador de Acesso do Usuário para quem precisa criar usuários e redefinir senhas.
Como não cair: Gerenciar usuários é função do Entra, como Administrador de Usuários; funções do RBAC tratam recursos.

⚠ **Alerta de prova:** Achar que Leitor na assinatura prevalece sobre Colaborador no grupo, ou que as duas entram em conflito.
Como não cair: RBAC é aditivo: as permissões se somam e o escopo amplo não restringe o específico.

⚠ **Alerta de prova:** Ler NotActions como negação que vence outras atribuições.
Como não cair: NotActions apenas subtrai do conjunto daquela função; outra atribuição pode conceder a ação.

⚠ **Alerta de prova:** Esperar que um recurso criado em RG-Alfa receba a marca Projeto=Alfa do grupo.
Como não cair: Marcas não são herdadas por padrão; use política Herdar uma marca com efeito Modify.

⚠ **Alerta de prova:** Testar uma política nova com bloqueio, isenção ou trocando o efeito para Append.
Como não cair: Atribua com o modo de imposição desabilitado (DoNotEnforce): mostra a conformidade sem bloquear e sem mudar a definição.

⚠ **Alerta de prova:** Mudar o efeito para Audit ou dar Leitor à identidade da política para corrigir recursos existentes.
Como não cair: Correção exige Modify ou DeployIfNotExists mais tarefa de correção, com identidade que tenha permissão de gravação.

⚠ **Alerta de prova:** Contar com o orçamento para bloquear criação ou parar recursos ao atingir o valor.
Como não cair: Orçamento só alerta; para agir, ligue um grupo de ações a runbook, função ou Logic App.

⚠ **Alerta de prova:** Dar Leitor ou Colaborador da Conta de Armazenamento para o aplicativo ler blobs.
Como não cair: Leitor e Colaborador são plano de controle; use identidade gerenciada com Leitor de Dados de Blob de Armazenamento.

⚠ **Alerta de prova:** Converter o convidado B2B em membro ou dar Administrador Global para ele gerenciar um grupo de recursos.
Como não cair: Tipo de usuário e funções do Entra não dão acesso a recursos; atribua uma função do Azure no RG.

⚠ **Alerta de prova:** Remover a licença ou mover de grupo para impedir a entrada de quem está saindo.
Como não cair: Bloqueie a entrada da conta e revogue as sessões; excluir perderia a conta exigida pela auditoria.

⚠ **Alerta de prova:** Criar a VM em outro grupo de recursos quando o limite de vCPUs da família foi atingido.
Como não cair: A cota vale para a assinatura na região; peça aumento ou use outra família ou região.

⚠ **Alerta de prova:** Aplicar bloqueio em grupo de gerenciamento ou no locatário.
Como não cair: Bloqueios só em assinatura, grupo de recursos e recurso.

⚠ **Alerta de prova:** Achar que mover a VM para um grupo criado em outra região muda a região da VM.
Como não cair: A região do grupo guarda metadados; a VM continua onde estava, só o ID muda. Trocar região é outro processo.

⚠ **Alerta de prova:** Supor que, ao transferir a assinatura para outro diretório, as atribuições ficam ou viram convites.
Como não cair: As atribuições de função são removidas, e elas, as funções personalizadas e as identidades gerenciadas precisam ser recriadas no novo diretório.

Como cai na prova

📝 **Como cai:** Uma operação falha com uma mensagem de erro e quatro causas possíveis.
Como resolver: Mapeie o código: RequestDisallowedByPolicy é política, ScopeLocked é bloqueio, AuthorizationFailed é RBAC, MissingSubscriptionRegistration é provedor, limite de vCPUs é cota.

📝 **Como cai:** Pedido de menor privilégio para uma tarefa (operar VMs, ler blobs, ler segredos, reiniciar uma VM).
Como resolver: Escolha a função mais específica (de dados quando for conteúdo) e o menor escopo; descarte Proprietário e Administrador de Acesso do Usuário quando não se deve conceder acesso a outros.

📝 **Como cai:** Requisito sobre marcas: exigir, herdar, relatar ou somar custos.
Como resolver: Recusar sem marca: Deny. Copiar do grupo: Modify (mais tarefa de correção para existentes). Só relatar: Audit. Custos por centro de custo: análise de custos agrupada pela marca.

📝 **Como cai:** Escolha DUAS sobre bloqueios, grupos de gerenciamento, marcas ou B2B.
Como resolver: Julgue cada alternativa isoladamente contra os fatos fixos: bloqueio em assinatura, RG e recurso; até seis níveis e um pai; até 50 marcas sem herança; convidado entra com a própria conta e recebe RBAC.

📝 **Como cai:** Requisito de custo: estimar, acompanhar, alertar, agir ou reduzir.
Como resolver: Estimar: calculadora. Ver por marca: análise de custos. Avisar em valor: orçamento. Desvio sem valor: anomalia. Arquivo diário: exportação. Agir: grupo de ações com runbook. Reduzir 24x7: reserva + Benefício Híbrido; VMs ociosas: Advisor.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Erro RequestDisallowedByPolicy	**Atribuição do Azure Policy com efeito Deny**
Erro ScopeLocked ou AuthorizationFailed	**ScopeLocked = bloqueio; AuthorizationFailed = falta de RBAC**
Erro MissingSubscriptionRegistration	**Registrar o provedor de recursos na assinatura**
Ver o impacto de uma política sem bloquear nem mudar a definição	**enforcementMode DoNotEnforce**
Liberar só um grupo da política, por três meses	**Isenção de política com data de expiração**
Marca ausente deve ser copiada do grupo de recursos	**Política com efeito Modify (herdar marca) + tarefa de correção para os existentes**
Se a extensão não existir, implantar	**DeployIfNotExists**
Mesma política em várias assinaturas, inclusive futuras	**Atribuição em grupo de gerenciamento**
Nenhuma função interna atende exatamente	**Função personalizada com Actions específicas**
Administrador de filial redefine senha só dos usuários dela	**Unidade administrativa com a função no escopo**
Usuários entram e saem do grupo pelo atributo departamento	**Grupo de segurança com associação dinâmica (P1)**
Mesma senha e entrada funcionando com o AD local indisponível	**Sincronização de hash de senha**
Avisar quando o custo diário fugir do padrão, sem valor fixo	**Alerta de anomalia do Cost Management**
Estimar custo antes de implantar	**Calculadora de preços do Azure**

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

- Funções do Entra e do Azure RBAC são sistemas separados.
- RBAC é aditivo; NotActions subtrai, não nega.
- Azure Policy e bloqueios valem até para proprietários.
- Marcas não são herdadas sem política Modify.
- Orçamento só alerta; quem age é o grupo de ações.

Essenciais para a prova (checklist)

☐ Sei dizer se uma tarefa pede função do Entra ou função do Azure RBAC.

☐ Sei calcular o acesso efetivo somando atribuições em escopos diferentes.

☐ Sei escrever uma função personalizada com Actions, NotActions e AssignableScopes válidos.

☐ Sei escolher o efeito de política certo (Deny, Audit, Modify, Append, DeployIfNotExists, AuditIfNotExists).

☐ Sei testar, isentar, avaliar sob demanda e corrigir recursos com o Azure Policy.

☐ Sei o que CanNotDelete e ReadOnly permitem e em quais escopos se aplicam.

☐ Sei restaurar, bloquear e criar usuários em massa, e configurar grupos dinâmicos, licenças e unidades administrativas.

☐ Sei convidar usuários B2B, controlar quem convida e dar acesso a recursos para convidados.

☐ Sei quais recursos exigem Entra ID P1 ou P2 e como configurar SSPR com write-back.

☐ Sei qual ferramenta de custo usar para estimar, analisar, alertar, exportar e agir.

Questões de revisão do capítulo

R1.1 · Gerenciar identidades e governança do Azure

Um usuário foi excluído do Microsoft Entra ID por engano há dez dias. Como recuperá-lo com as associações a grupos?

A. Reativar o usuário pelo log de auditoria do Entra
B. Restaurar um backup do diretório no Azure Backup
C. Recriar o usuário com o mesmo nome e e-mail
D. Restaurar o usuário em Usuários excluídos

R1.2 · Gerenciar identidades e governança do Azure

Nenhum IP público pode ser criado em uma assinatura de dados sensíveis. O que aplicar?

A. Marca obrigatória nos IPs públicos
B. Função Leitor para a equipe de rede
C. Bloqueio CanNotDelete nos IPs existentes
D. Política Tipos de recursos não permitidos

R1.3 · Gerenciar identidades e governança do Azure

Um aplicativo em uma VM precisa ler blobs de uma conta de armazenamento, sem guardar chaves ou senhas. O que configurar?

A. Função Colaborador da Conta de Armazenamento para a VM
B. Identidade gerenciada com Leitor de Dados de Blob de Armazenamento
C. Chave da conta de armazenamento guardada em uma variável de ambiente
D. Identidade gerenciada com a função Leitor na conta de armazenamento

R1.4 · Gerenciar identidades e governança do Azure

Um consultor externo aceitou o convite B2B e agora precisa gerenciar os recursos do grupo RG-Projeto. O que falta fazer?

A. Atribuir uma função do Azure a ele no RG-Projeto
B. Criar uma assinatura separada para o convidado
C. Converter o convidado em usuário membro do locatário
D. Atribuir a ele a função Administrador Global

Respostas comentadas

R1.1. D) Restaurar o usuário em Usuários excluídos

Por quê: A exclusão de usuários é temporária por 30 dias. Após esse prazo, ou com exclusão permanente, não é possível restaurar.

✗ A) Incorreta. O log de auditoria registra eventos, sem restaurar objetos.
✗ B) Incorreta. O Azure Backup não faz backup de usuários do Entra.
✗ C) Incorreta. Um novo usuário teria outro ID e perderia as associações.

> **Dica de prova:** Usuário excluído: restaurar em até 30 dias.

R1.2. D) Política Tipos de recursos não permitidos

Por quê: Tipos de recursos não permitidos e Tipos de recursos permitidos são políticas internas usadas para limitar serviços em um escopo.

✗ A) Incorreta. Uma marca não impede a criação.
✗ B) Incorreta. Isso bloquearia todo o trabalho da equipe.
✗ C) Incorreta. O bloqueio não impede a criação de novos IPs.

Dica de prova: Proibir um tipo de recurso: Tipos de recursos não permitidos.

R1.3. B) Identidade gerenciada com Leitor de Dados de Blob de Armazenamento

Por quê: Funções de dados, como Leitor de Dados de Blob de Armazenamento, dão acesso ao conteúdo. Funções como Leitor e Colaborador atuam na gestão do recurso.

✗ A) Incorreta. Ela gerencia a conta e depende de chaves para acessar dados.
✗ C) Incorreta. Isso guarda um segredo na VM, o que foi vetado.
✗ D) Incorreta. Leitor atua no plano de controle e não lê o conteúdo dos blobs.

Dica de prova: Ler dados sem segredo: identidade gerenciada + função de dados.

R1.4. A) Atribuir uma função do Azure a ele no RG-Projeto

Por quê: Convidados são entidades de segurança do diretório e recebem funções do Azure RBAC como qualquer usuário.

✗ B) Incorreta. Uma nova assinatura não dá acesso ao RG-Projeto.
✗ C) Incorreta. O tipo de usuário não concede acesso a recursos.
✗ D) Incorreta. Funções do Entra não dão acesso a recursos.

Dica de prova: Convidado com acesso a recursos: atribuição de função RBAC.

02

CAPÍTULO 2 · 20-25% DA PROVA

Implantar e gerenciar recursos de computação

Aqui eu preciso dominar modelos ARM e Bicep (seções, modos de implantação, dependências, escopos, what-if), máquinas virtuais (disponibilidade, discos, tamanhos, operações do dia a dia), conjuntos de dimensionamento, App Service (planos, níveis, slots, configurações de rede) e contêineres (ACR, ACI e Container Apps). A prova costuma dar um requisito operacional e quatro recursos parecidos: conjunto de disponibilidade x zonas, Executar comando x extensão, ACI x Container Apps, escala vertical x horizontal. Muitas questões testam o que não pode ser alterado depois da criação (conjunto de disponibilidade, VNet da VM, região). Onde mais erro: achar que o modo Complete é inofensivo, que integração com VNet protege a entrada do App Service e confundir as políticas de reinício e de atualização.

Neste capítulo

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

Tópicos-chave

Seções de modelos ARM e Bicep

Parâmetros recebem valores informados por quem implanta, variáveis simplificam expressões internas, saídas devolvem valores ao final e funções definidas pelo usuário calculam expressões. Para usar a região do grupo, o padrão de location é [resourceGroup().location] (em Bicep, sem colchetes). Um arquivo de parâmetros por ambiente (JSON ou .bicepparam) mantém um só modelo para dev e produção, e segredos podem vir do Key Vault por referência.

Modos de implantação Incremental e Complete

Incremental, o padrão, mantém no grupo os recursos que não estão no modelo. Complete exclui do grupo os recursos não definidos no modelo, por isso exige cuidado. Nenhum dos modos define ordem, escopo ou valores.

Dependências e referências

Em ARM, dependsOn define a ordem de criação, como a NIC aguardando a VNet; no Bicep, referências simbólicas criam dependências implícitas. A palavra-chave existing referencia um recurso já criado, por exemplo a VNet de outra equipe, sem recriá-lo; módulos Bicep (palavra-chave module, em arquivo local, registro privado ou especificação de modelo) reutilizam definições.

Escopo e ferramentas do Bicep

targetScope pode ser resourceGroup (padrão), subscription, managementGroup ou tenant; criar grupos de recursos exige subscription. az bicep decompile converte JSON em Bicep e az bicep build faz o inverso; o what-if lista criações, alterações e exclusões antes de implantar. Exportar o modelo do grupo no portal gera um ponto de partida que precisa de ajustes, e o histórico de implantações do grupo mostra operações e erros.

Conjuntos de disponibilidade e zonas

Conjuntos de disponibilidade distribuem VMs em domínios de falha (energia e rede) e domínios de atualização dentro do mesmo datacenter; na manutenção planejada, um domínio de atualização é reiniciado por vez. Zonas de disponibilidade protegem contra a perda de um datacenter. O conjunto de disponibilidade é definido na criação: incluir VM existente exige recriá-la com os discos.

SLA de VM

99,9% para uma instância única com SSD Premium ou Ultra em todos os discos; 99,95% com conjunto de disponibilidade; 99,99% com zonas de disponibilidade. Um conjunto com uma só VM não dá SLA de conjunto, e HDD Standard não atende o 99,9%.

Posicionamento, isolamento e Spot

Grupo de posicionamento por proximidade reduz a latência entre VMs e pode ser combinado com conjunto de disponibilidade. Host Dedicado dá servidor físico exclusivo e controle de manutenção. VMs Spot usam capacidade ociosa para cargas interrompíveis; a política de remoção Desalocar mantém os discos (cobrados) e Excluir remove tudo; preço máximo -1 significa pagar até o preço regular.

Tipos de disco gerenciado

Disco Ultra atende as cargas mais exigentes, com IOPS muito alto ajustável sem trocar o disco, e não é usado como disco de SO; SSD Premium v2 também ajusta IOPS e taxa de forma independente, com limite menor. SSD Standard é para cargas leves e HDD Standard para backup e acesso pouco frequente. O disco efêmero do SO serve cargas sem estado, sem custo de armazenamento, e perde dados ao desalocar ou reimagear.

Operações com discos e tamanhos

Trocar o tipo de disco (por exemplo HDD Standard para SSD Premium) exige, na maioria dos casos, desalocar a VM. Disco de dados novo precisa ser inicializado, particionado e formatado no sistema operacional. Se o tamanho desejado não aparece ao redimensionar, desaloque a VM para ver os tamanhos disponíveis na região.

Famílias de tamanhos de VM

D é uso geral; E e M são otimizadas para memória; F para computação; L para armazenamento; N tem GPU; B é expansível, acumulando créditos para picos em cargas leves.

Operações e manutenção de VMs

Reimplantar move a VM para outro nó (perde o disco temporário e IPs dinâmicos podem mudar); trocar de VNet exige recriar a VM com os discos; trocar de região usa o Azure Resource Mover. Executar comando roda um script pontual pelo agente da VM, e a Extensão de Script Personalizado roda scripts pós-implantação em várias VMs. Diagnóstico de inicialização mostra captura de tela e logs do boot e habilita o console serial; Trusted Launch é o padrão para VMs de 2ª geração com inicialização segura e vTPM.

Automação de VMs

Azure Update Manager aplica patches em VMs do Azure e servidores habilitados pelo Arc, com agendamento por configuração de manutenção. Desligamento automático desaloca a VM em um horário, sem scripts. Azure Compute Gallery guarda definições e versões de imagens com réplicas regionais.

Conjuntos de Dimensionamento de Máquinas Virtuais

Escalam horizontalmente por métrica, agenda ou escala preditiva e podem abranger as zonas 1, 2 e 3. A orquestração Flexível, recomendada para novas cargas, mistura tamanhos e VMs Spot com regulares; a Uniforme usa instâncias idênticas. A política de atualização é Automática, Contínua (Rolling) ou Manual (instâncias antigas ficam com a versão antiga até o administrador agir); a política de redução é Default, NewestVM ou OldestVM, e a proteção de instância impede remover instâncias escolhidas.

Planos do App Service

O plano define instâncias e nível de preço, é Windows ou Linux, e os aplicativos precisam de plano do mesmo sistema e região; aplicativos no mesmo plano dividem as instâncias. Free não aceita domínio personalizado nem slots; Basic tem escala manual e Always On; Standard e Premium têm escala automática e slots. Scale up muda o nível (mais recursos por instância) e scale out muda o número de instâncias.

Slots de implantação

Slots são aplicativos ativos com nome próprio; a troca (swap) aquece as instâncias antes de redirecionar o tráfego e pode ser desfeita trocando de volta. Configurações e cadeias de conexão marcadas como configuração de slot (sticky) não acompanham a troca. A troca automática faz o swap após cada implantação no slot de preparo.

Configurações e rede do App Service

Restrições de acesso filtram a entrada por regras ordenadas de IP; integração com VNet trata só a saída; ponto de extremidade privado dá entrada por IP privado e permite desligar o acesso público. Referências do Key Vault (@Microsoft.KeyVault(...)) leem segredos sem mudar o código, e domínio personalizado exige CNAME (subdomínio) ou A (raiz) mais TXT asuid. Always On evita o descarregamento, a verificação de integridade remove instâncias que falham, o Centro de Implantação liga GitHub Actions, o fluxo de logs (az webapp log tail) mostra logs em tempo real e o backup personalizado vai para um contêiner de armazenamento.

Azure Container Registry

Camadas Basic, Standard e Premium; só a Premium tem replicação geográfica e pontos de extremidade privados. AcrPull baixa, AcrPush envia e AcrDelete exclui imagens; identidade gerenciada com AcrPull evita o usuário administrador. ACR Tasks com az acr build compila imagens na nuvem, sem Docker local.

Container Instances e Container Apps

ACI é a forma mais simples de rodar um contêiner; o grupo de contêineres compartilha IP, portas, volumes e ciclo de vida, como um pod. Políticas de reinício: Always (padrão), OnFailure e Never; só o volume do Azure Files persiste dados (emptyDir some com o grupo). Container Apps é sem servidor, com escala por KEDA até zero, revisões com divisão de tráfego, ambiente com VNet e logs comuns, entrada externa ou limitada ao ambiente e jobs manuais, agendados (cron) ou por eventos.

Macetes para memorizar

Seções do modelo

Parameter vem de fora, variable nasce dentro, output sai no fim.

Modo Complete

Complete completa a faxina: o que não está no modelo vai para o lixo.

SLA de VM

Sozinha premium 99,9; conjunto 99,95; zonas 99,99: cada degrau de proteção soma um pedaço de nove.

Níveis do App Service

Free não tem domínio; Basic acorda (Always On) e escala à mão; Standard escala sozinho e ganha slots.

Reinício no ACI

Always repete sempre, OnFailure só se cair, Never nunca mais.

Escala

Up = maior (mais recurso por instância); Out = mais (mais instâncias).

Funções do ACR

Pull puxa, Push empurra, Delete apaga; replicação geográfica só no Premium.

Tabela de memorização: não confunda

Quando é...	...e quando é
Conjunto de disponibilidade Proteger contra falha de rack e manutenção dentro do mesmo datacenter (SLA 99,95%).	**Zonas de disponibilidade** Continuar atendendo se um datacenter inteiro cair (SLA 99,99%).
Modo Incremental Implantar mantendo recursos do grupo que não estão no modelo (padrão).	**Modo Complete** Fazer o grupo ficar igual ao modelo, excluindo o que não está nele.
Executar comando Rodar um comando pontual de diagnóstico ou correção sem RDP e sem instalar nada.	**Extensão de Script Personalizado** Rodar scripts armazenados após a implantação, como instalar um agente em várias VMs.
Azure Container Instances Contêiner simples sob demanda, sem orquestrador, pagando pelo tempo de execução.	**Azure Container Apps** Aplicativo com escala por HTTP até zero, revisões e divisão de tráfego, sem gerenciar Kubernetes.
Escala vertical (scale up) Falta memória ou CPU em cada instância, mesmo com poucos usuários.	**Escala horizontal (scale out)** A carga cresce e precisa de mais instâncias para dividir o tráfego.
Restrições de acesso Filtrar a entrada do aplicativo por IPs.	**Integração com rede virtual** Deixar o aplicativo alcançar recursos privados na saída.

Orquestração Flexível Misturar tamanhos e combinar Spot com VMs regulares; recomendada para novas cargas.	**Orquestração Uniforme** Instâncias idênticas a partir de um mesmo modelo.

Números que caem

Item	Valor
SLA de VM única com SSD Premium ou Ultra em todos os discos	**99,9%**
SLA com conjunto de disponibilidade	**99,95%**
SLA com zonas de disponibilidade	**99,99%**
Domínios de atualização reiniciados por vez na manutenção planejada	**1**
Preço máximo -1 em VM Spot	**Pagar até o preço de VM regular**
Menor nível do App Service com escala automática por regras	**Standard**
Menor nível do App Service com Always On	**Basic**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Colocar as VMs no mesmo conjunto de disponibilidade ou num grupo de posicionamento para sobreviver à falha de um datacenter.
Como não cair: Conjunto fica num só datacenter e grupo de posicionamento aproxima as VMs; use zonas de disponibilidade.

⚠ **Alerta de prova:** Editar a VM para escolher o conjunto de disponibilidade ou trocar a sub-rede da NIC para outra VNet.
Como não cair: As duas coisas são definidas na criação: recrie a VM usando os discos existentes.

⚠ **Alerta de prova:** Mover a VM para outro grupo de recursos para mudar de região.
Como não cair: Mover entre grupos não muda a região; use o Azure Resource Mover.

⚠ **Alerta de prova:** Aumentar o número de instâncias quando falta memória em cada instância.
Como não cair: Mais instâncias dividem a carga mas cada uma segue com a mesma memória; faça scale up para um plano maior.

⚠ **Alerta de prova:** Usar integração com VNet ou NSG na sub-rede de integração para filtrar quem acessa o aplicativo.
Como não cair: Integração com VNet é só saída; entrada se filtra com restrições de acesso ou se torna privada com ponto de extremidade privado.

⚠ **Alerta de prova:** Guardar a cadeia de conexão no web.config ou usar troca com visualização para ela não ir à produção.
Como não cair: Marque-a como configuração de slot (sticky); arquivos acompanham o conteúdo trocado.

⚠ **Alerta de prova:** Escolher OnFailure para um contêiner que nunca deve reiniciar.
Como não cair: OnFailure reinicia em caso de erro; para nunca reiniciar, a política é Never.

⚠ **Alerta de prova:** Usar ACI ou AKS para escalar até zero por requisições HTTP sem gerenciar cluster.
Como não cair: ACI não escala por HTTP e AKS exige operar o cluster; a resposta é Container Apps.

⚠ **Alerta de prova:** Escolher SSD Premium v2 para 160.000 IOPS com latência abaixo de milissegundo.
Como não cair: O limite por disco do Premium v2 é menor; o tipo para as cargas mais exigentes é o Disco Ultra.

⚠ **Alerta de prova:** Usar Disco Ultra ou SSD Premium v2 como SO rápido de um conjunto sem estado.
Como não cair: Ultra não é disco de SO e Premium v2 tem custo de armazenamento; use disco efêmero do SO.

⚠ **Alerta de prova:** Responder 5 VMs indisponíveis num conjunto com 10 VMs, 2 domínios de falha e 5 de atualização.
Como não cair: Um domínio de atualização por vez: 10 VMs em 5 domínios dá 2 VMs por vez.

⚠ **Alerta de prova:** Usar az bicep build para converter modelos JSON em Bicep.
Como não cair: build gera JSON a partir do Bicep; JSON para Bicep é az bicep decompile.

⚠ **Alerta de prova:** Definir preço máximo -1 achando que isso mantém os discos da VM Spot.
Como não cair: O preço só define quando ocorre remoção por preço; manter discos é a política de remoção Desalocar.

⚠ **Alerta de prova:** Atribuir a política de atualização Manual quando se quer remover primeiro as VMs mais antigas.
Como não cair: Política de atualização trata versões; remoção na redução é a política OldestVM.

Como cai na prova

📝 **Como cai:** Requisito de disponibilidade com números ou falha descrita (rack, datacenter, manutenção).
Como resolver: Falha de datacenter: zonas. Rack ou manutenção no mesmo datacenter: conjunto de disponibilidade. Para contas de manutenção, divida as VMs pelos domínios de atualização e conte só um domínio por vez.

📝 **Como cai:** Algo que precisa mudar numa VM existente (conjunto, VNet, região, host, tipo de disco, tamanho).
Como resolver: Lembre o que é imutável: conjunto e VNet exigem recriar com os discos; região usa Resource Mover; host usa reimplantar; tipo de disco e tamanho ausente pedem desalocar.

📝 **Como cai:** Trecho de modelo ARM ou Bicep com um problema (ordem, escopo, valor por ambiente, recurso existente).
Como resolver: Ordem: dependsOn. Valor por implantação: parameters e arquivo de parâmetros. Criar grupos: targetScope subscription. Recurso de outra equipe: existing. Reuso: module. Prever: what-if.

📝 **Como cai:** Problema no App Service (memória, lentidão inicial, instância com falha, domínio, segredo, filtro de IP).
Como resolver: Associe ao recurso: scale up, Always On, verificação de integridade, nível pago com CNAME ou A mais TXT asuid, referência do Key Vault, restrições de acesso; confira se o nível do plano oferece o recurso.

📝 **Como cai:** Escolha entre ACI, Container Apps, AKS e VM com Docker.
Como resolver: Simples e sob demanda: ACI. Escala até zero, revisões, tráfego dividido ou jobs agendados: Container Apps. Orquestração completa e operar cluster: AKS. Descarte VM com Docker quando o requisito é não gerenciar servidor.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Adicionar VMs com CPU acima de um limite e remover abaixo de outro	**Conjunto de dimensionamento com escala automática**
Continuar atendendo se um datacenter inteiro cair	**Zonas de disponibilidade (VMSS com zonas 1, 2 e 3)**
Latência de rede mínima entre camadas	**Grupo de posicionamento por proximidade**
Servidores físicos sem VMs de outros clientes	**Host Dedicado do Azure**

Carga interrompível, menor custo de computação	**VMs Spot**
Falhas que parecem do host físico, sem perder discos	**Reimplantar a VM**
Inicialização segura e vTPM contra rootkits	**Inicialização confiável (Trusted Launch)**
Ver o que será criado, alterado ou excluído antes de implantar	**Operação what-if**
Imagem versionada replicada para várias regiões	**Azure Compute Gallery**
Publicar, validar e colocar em produção sem indisponibilidade	**Slots de implantação com troca**
Primeira requisição lenta após período sem uso	**Always On**
20% do tráfego para a nova versão do contêiner	**Revisões do Container Apps com divisão de tráfego**
Contêiner de aplicativo e auxiliar compartilhando rede, armazenamento e ciclo de vida	**Mesmo grupo de contêineres no ACI**
Gerar imagem a partir de Dockerfile sem Docker no agente	**ACR Tasks com az acr build**

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

- Modo Complete exclui do grupo o que não está no modelo; Incremental é o padrão.
- Conjunto de disponibilidade e VNet da VM são definidos na criação; mudar exige recriar com os discos.
- Zonas protegem contra perda de datacenter; conjunto de disponibilidade não.
- Integração com VNet do App Service é só saída; entrada é restrição de acesso ou ponto de extremidade privado.
- ACI: política de reinício padrão Always; só volume do Azure Files persiste dados.

Essenciais para a prova (checklist)

☐ Sei a função de parameters, variables, outputs, dependsOn, existing, module e targetScope.

☐ Sei a diferença entre implantação Incremental e Complete e quando usar what-if, export e decompile.

☐ Sei escolher entre conjunto de disponibilidade, zonas, grupo de posicionamento e Host Dedicado.

☐ Sei os SLAs de VM e o que cada um exige.

☐ Sei escolher o tipo de disco e o que exige desalocar a VM.

☐ Sei quando reimplantar, redimensionar, recriar ou usar Resource Mover numa VM.

☐ Sei configurar VMSS: escala automática, zonas, orquestração, política de atualização e de redução.

☐ Sei o que cada nível do App Service oferece e como slots, configurações sticky e troca automática funcionam.

☐ Sei configurar rede, segredos, domínio, integridade e logs de um aplicativo no App Service.

- [ ] Sei escolher entre ACR (camada e função), ACI e Container Apps para cada cenário.

Questões de revisão do capítulo

R2.1 · Implantar e gerenciar recursos de computação

Ao criar um aplicativo web Linux, o plano do App Service existente não aparece na lista. Qual é a causa provável?

A. O plano existente está no nível Free
B. A região não aceita aplicativos Linux
C. O aplicativo precisa de um slot antes
D. O plano é Windows, e o app exige Linux

R2.2 · Implantar e gerenciar recursos de computação

Uma implantação de modelo ARM falhou no grupo de recursos. Onde ver as operações executadas e a mensagem de erro detalhada?

A. Histórico de implantações do grupo
B. Recomendações do Azure Advisor
C. Métricas de plataforma do grupo
D. Painel do Azure Service Health

R2.3 · Implantar e gerenciar recursos de computação

Um aplicativo no App Service deve aceitar requisições só dos IPs do escritório. O que configurar?

A. Integração com rede virtual no aplicativo
B. Certificado TLS no domínio do aplicativo
C. NSG na sub-rede de integração do aplicativo
D. Restrições de acesso com regras de IP

R2.4 · Implantar e gerenciar recursos de computação

Um aplicativo no App Service deve ler a senha do banco no Azure Key Vault, sem alterar o código que lê as configurações. O que usar?

A. Senha gravada no arquivo web.config
B. Cadeia de conexão em texto no código
C. Variável definida só no slot de preparo do app
D. Referência do Key Vault nas configurações

Respostas comentadas

R2.1. D) O plano é Windows, e o app exige Linux

Por quê: Planos do App Service são Windows ou Linux. Aplicativos precisam de um plano do mesmo sistema e da mesma região.

✗ A) Incorreta. O nível não esconde o plano por sistema.
✗ B) Incorreta. O Linux está disponível nas regiões comuns.
✗ C) Incorreta. Slots são criados depois do aplicativo.

> **Dica de prova:** App Linux precisa de plano Linux.

R2.2. A) Histórico de implantações do grupo

Por quê: Em Implantações, é possível ver parâmetros, operações por recurso, erros e o modelo usado, além de reimplantar.

✗ B) Incorreta. O Advisor não detalha implantações.
✗ C) Incorreta. Grupos de recursos não têm métricas de implantação.
✗ D) Incorreta. Ele mostra incidentes da plataforma.

> **Dica de prova:** Erro de implantação: histórico de implantações.

R2.3. D) Restrições de acesso com regras de IP

Por quê: As restrições de acesso formam uma lista ordenada de regras de permissão e negação para o tráfego de entrada do aplicativo.

✗ A) Incorreta. Ela conecta a saída do aplicativo a uma VNet.
✗ B) Incorreta. O TLS criptografa, sem filtrar origens.
✗ C) Incorreta. A integração com VNet trata só o tráfego de saída.

> **Dica de prova:** Filtrar entrada no App Service: restrições de acesso.

R2.4. D) Referência do Key Vault nas configurações

Por quê: Referências do Key Vault usam a sintaxe @Microsoft.KeyVault(...) nas configurações do aplicativo. A identidade do aplicativo precisa de acesso ao segredo.

✗ A) Incorreta. Isso guarda o segredo junto com o código.
✗ B) Incorreta. Segredos no código são uma má prática.
✗ C) Incorreta. A produção continuaria sem o segredo.

> **Dica de prova:** Segredo do Key Vault sem mudar código: referência nas configurações.

03

CAPÍTULO 3 · 15-20% DA PROVA

Implementar e gerenciar armazenamento

Aqui eu preciso escolher o tipo de conta, a redundância e a camada de acesso certos, proteger dados contra exclusão, sobrescrita e corrupção, controlar acesso com chaves, SAS, Entra e firewall, e operar o Azure Files com File Sync. A prova cobra muito a diferença entre recursos que parecem iguais: exclusão temporária, controle de versão, restauração pontual, imutabilidade e replicação de objetos resolvem acidentes diferentes. Também cai bastante qual ferramenta de transferência usar (AzCopy, Storage Explorer, Data Box, Import/Export) e os prazos mínimos das camadas. Onde mais erro: achar que GRS ou bloqueio de recurso protege contra exclusão de dados, e esquecer que só o prefixo RA permite ler a secundária sem failover.

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

Tópicos-chave

Tipos de conta de armazenamento

Standard de uso geral v2 é a recomendada para a maioria dos cenários: aceita blobs, arquivos, filas e tabelas, todas as redundâncias e camadas de acesso, com Azure Files em HDD. As premium são BlockBlobStorage (muitas transações pequenas, IoT, telemetria, IA), FileStorage (Azure Files em SSD e NFS) e blobs de página.

Nome da conta

De 3 a 24 caracteres, só letras minúsculas e números, único em todo o Azure, pois forma o ponto de extremidade, como contosodados2026.blob.core.windows.net. Sublinhado, ponto, hífen e maiúsculas não são aceitos.

Redundância

LRS protege dentro de um datacenter; ZRS copia de forma síncrona entre zonas e aguenta a falha de um datacenter sem sair da região; GRS e GZRS adicionam cópia assíncrona em região secundária (o GRS usa LRS na primária). O prefixo RA permite ler a secundária a qualquer momento pelo ponto de extremidade secundário; LRS para ZRS se faz por conversão solicitada no portal.

Failover da conta e hora da última sincronização

Em desastre, o cliente inicia o failover da conta; depois dele a conta vira LRS na nova primária e a redundância geográfica precisa ser reconfigurada. Como a replicação é assíncrona, gravações posteriores à hora da última sincronização podem ser perdidas, então ela é consultada antes do failover.

Camadas de acesso de blobs

Online: Hot (maior custo de armazenamento), Cool (mínimo de 30 dias) e Cold (mínimo de 90 dias). Archive é offline, com mínimo de 180 dias. Sair antes do mínimo gera cobrança de exclusão antecipada proporcional aos dias restantes, sem reembolso.

Reidratação do Archive

Um blob em Archive não pode ser lido diretamente, nem com SAS; é preciso reidratá-lo mudando a camada ou copiando para uma camada online. Na prioridade padrão leva até 15 horas; a prioridade alta custa mais e é para emergências.

Gerenciamento do ciclo de vida

Regras filtradas por prefixo ou marca de índice mudam camadas (Hot, Cool, Cold, Archive) e excluem blobs, versões e snapshots, sem scripts, e rodam uma vez por dia. As condições usam data de modificação, de criação ou do último acesso; esta exige o rastreamento de hora do último acesso habilitado.

Proteção de dados de blobs

Exclusão temporária de blobs guarda blobs, versões e snapshots excluídos por 1 a 365 dias; exclusão temporária de contêineres guarda o contêiner inteiro também por 1 a 365 dias; controle de versão mantém versões anteriores de blobs sobrescritos. A restauração pontual devolve contêineres de blobs de blocos a um momento anterior e exige controle de versão, feed de alterações e exclusão temporária, com período menor que a retenção da exclusão temporária.

Feed de alterações e inventário

O feed de alterações grava um registro ordenado e durável de criações, alterações e exclusões no contêiner $blobchangefeed. O inventário de blobs gera relatórios diários ou semanais em CSV ou Parquet com o estado atual dos blobs e propriedades como camada e tamanho.

Replicação de objetos

Copia blobs de blocos de forma assíncrona para outra conta independente, com camada e redundância próprias, escolhendo contêineres e filtros. Exige controle de versão nas duas contas e feed de alterações na origem; contas com namespace hierárquico não aceitam replicação de objetos.

Armazenamento imutável

Retenção baseada em tempo mantém os dados sem alteração ou exclusão pelo período definido; com a política bloqueada, nem administradores reduzem o prazo (WORM regulatório). Retenção legal é uma marca em contêineres ou versões que mantém os dados imutáveis sem prazo, até ser removida.

Assinaturas de acesso compartilhado (SAS)

SAS de conta e de serviço são assinadas com a chave da conta; a de delegação de usuário é assinada com credenciais do Entra e é a recomendada para blobs. Parâmetros sip (IPs permitidos) e spr (protocolo) restringem o uso, além de permissões, início e expiração. Uma política de acesso armazenada (até cinco por contêiner) permite revogar as SAS de serviço ligadas a ela sem trocar chaves.

Chaves de acesso e chave compartilhada

A conta tem duas chaves: para rotacionar sem parada, passe os aplicativos para a secundária e regenere a primária; o recomendado é guardá-las no Key Vault ou, melhor, usar autenticação do Entra. Desativar Permitir acesso por chave da conta de armazenamento bloqueia chaves e SAS de conta ou serviço, mas a SAS de delegação de usuário continua funcionando.

Segurança de rede e acesso anônimo da conta

O firewall da conta em Redes selecionadas aceita regras de IP público e regras de rede virtual, que exigem ponto de extremidade de serviço na sub-rede. A versão mínima do TLS (MinimumTlsVersion) recusa TLS 1.0 e 1.1; contas novas já usam 1.2. O acesso anônimo de blob vem desabilitado em contas novas: primeiro se habilita na conta, depois se define o nível do contêiner como Blob ou Contêiner.

Criptografia em repouso

Toda conta é criptografada automaticamente com AES de 256 bits, com chaves gerenciadas pela Microsoft por padrão, e a criptografia não pode ser desabilitada. Chaves gerenciadas pelo cliente ficam no Key Vault ou HSM gerenciado, acessadas pela conta por identidade gerenciada, quando a empresa precisa controlar e rotacionar a chave.

Azure Files

SMB usa a porta 445; se ela estiver bloqueada, as saídas são VPN ponto a site, site a site, ExpressRoute ou servidor local com File Sync. NFS 4.1 exige conta FileStorage premium e rede privada ou ponto de extremidade de serviço. Standard pago conforme o uso tem as camadas Otimizada para transações, Hot e Cool; para passar de 5 TiB até 100 TiB em conta antiga, habilite compartilhamentos de arquivos grandes, que não pode ser desfeito.

Proteção e identidade no Azure Files

Instantâneos de compartilhamento são somente leitura e incrementais, aparecem em Versões anteriores no Windows e são automatizados pelo Azure Backup; a exclusão temporária de compartilhamentos vem habilitada por padrão em contas novas, de 1 a 365 dias. Com autenticação baseada em identidade (como AD DS local), permissões de compartilhamento usam funções RBAC, como Storage File Data SMB Share Contributor (leitura e gravação) e SMB Share Reader (só leitura), e permissões de arquivo e pasta usam ACLs NTFS.

Azure File Sync e ferramentas de transferência

O Serviço de Sincronização de Armazenamento contém grupos de sincronização com um ponto de extremidade de nuvem (compartilhamento do Azure Files) e vários de servidor; a camada de nuvem tem políticas de espaço livre do volume e de data de acesso. AzCopy faz copy (inclusive servidor a servidor entre contas), sync com --delete-destination=true e login --identity; Storage Explorer é a interface gráfica que usa AzCopy; Data Box é dispositivo da Microsoft para dezenas a centenas de TB offline; Import/Export usa discos próprios preparados com a WAImportExport.

Macetes para memorizar

Prazos mínimos das camadas

Cool 30, Cold 90, Archive 180: cada degrau mais frio prende o dado por mais tempo.

Leitura da secundária

RA = Read Access: sem RA, a secundária só abre depois do failover.

Qual proteção usar

Apagou blob: exclusão temporária. Sobrescreveu: versão. Estragou tudo há horas: restauração pontual. Sumiu o contêiner: exclusão temporária de contêineres.

Nome da conta

3 a 24, só minúsculas e números: nada de _ . - nem maiúscula.

Bloqueio x dado

Bloqueio protege o recurso, não o conteúdo do blob.

Tipos de SAS

Delegação de usuário: o Entra assina. Serviço e conta: a chave assina.

Imutabilidade

Legal = sem data; Tempo = com data no calendário.

Tabela de memorização: não confunda

Quando é...	...e quando é

ZRS Sobreviver à falha de um datacenter ou zona, com cópia síncrona e sem depender de failover para outra região.	**GRS** Ter cópia assíncrona em outra região para desastre regional, aceitando failover e possível perda após a última sincronização.
GZRS Zona e região protegidas, mas a secundária só é lida após failover.	**RA-GZRS** Mesma proteção e leitura da secundária a qualquer momento, sem esperar failover.
Exclusão temporária de blobs Recuperar blob apagado por engano dentro do período de retenção.	**Controle de versão de blobs** Voltar a uma versão anterior de blob sobrescrito.
Replicação de objetos Cópia para outra conta independente e legível, onde outra equipe processa os dados.	**Redundância GRS** Proteção regional da mesma conta; a secundária não é uma conta própria para processamento.
Camada Cold Dados raros, mínimo de 90 dias, que precisam ser lidos na hora.	**Camada Archive** Dados que podem ficar offline por 180 dias ou mais, aceitando reidratação (até 15 horas na prioridade padrão) antes da leitura.
Retenção legal Manter inalterado até segunda ordem, sem prazo definido.	**Retenção baseada em tempo** Manter por prazo regulatório, como sete anos, nem administradores reduzindo com a política bloqueada.
Azure Data Box Migração offline grande com dispositivo fornecido pela Microsoft.	**Azure Import/Export** Enviar os próprios discos rígidos, preparados com a WAImportExport.

Números que caem

Item	Valor
Tamanho do nome da conta de armazenamento	**3 a 24 caracteres (minúsculas e números)**
Período mínimo na camada Cool	**30 dias**
Período mínimo na camada Cold	**90 dias**
Período mínimo na camada Archive	**180 dias**
Reidratação do Archive na prioridade padrão	**Até 15 horas**
Retenção da exclusão temporária de blobs, contêineres e compartilhamentos	**1 a 365 dias**
Políticas de acesso armazenadas por contêiner (também compartilhamentos, filas e tabelas)	**Até cinco**

Compartilhamento Standard do Azure Files	**5 TiB; até 100 TiB com compartilhamentos de arquivos grandes**
Criptografia em repouso padrão	**AES de 256 bits**
Versão mínima de TLS padrão em contas novas	**TLS 1.2**
Porta do SMB	**445**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Usar GRS para recuperar blobs apagados por engano.
Como não cair: A exclusão é replicada para a secundária; quem desfaz exclusão é a exclusão temporária.

⚠ **Alerta de prova:** Aplicar bloqueio Excluir ou ReadOnly para proteger blobs contra exclusão ou alteração.
Como não cair: Bloqueios de recurso atuam no plano de controle e não protegem dados dos blobs; use exclusão temporária ou imutabilidade.

⚠ **Alerta de prova:** Exclusão temporária por sete anos para documentos fiscais.
Como não cair: Ela vai até 365 dias e não impede alterações; WORM regulatório é política de imutabilidade por tempo.

⚠ **Alerta de prova:** Fazer failover da conta ou replicação de objetos para desfazer corrupção causada por script.
Como não cair: A corrupção já foi replicada; para voltar vários contêineres no tempo use a restauração pontual.

⚠ **Alerta de prova:** Gerar uma SAS de leitura para ler um blob em Archive, ou criar regra de ciclo de vida para acelerar.
Como não cair: Archive é offline: reidrate primeiro, com prioridade alta se for urgente; ciclo de vida roda uma vez por dia.

⚠ **Alerta de prova:** Escolher GZRS quando o aplicativo quer ler a secundária a qualquer momento.
Como não cair: Sem o prefixo RA, a secundária só é lida após failover; a resposta é RA-GZRS.

⚠ **Alerta de prova:** Trocar a redundância ou a camada Hot para ganhar SSD ou baixa latência.
Como não cair: Redundância e camada não mudam a mídia; desempenho vem de conta premium (FileStorage ou BlockBlobStorage).

⚠ **Alerta de prova:** Regenerar as duas chaves ao mesmo tempo para rotacionar.
Como não cair: Isso derruba todos os aplicativos; mova-os para a outra chave e regenere uma de cada vez.

⚠ **Alerta de prova:** Exigir transferência segura (HTTPS) para impedir o uso das chaves da conta.
Como não cair: HTTPS protege o tráfego; para proibir chaves e SAS assinadas com elas, desative o acesso por chave compartilhada.

⚠ **Alerta de prova:** Contar com instantâneos manuais para recuperar contêiner ou compartilhamento excluído.
Como não cair: Instantâneos são excluídos junto; é preciso exclusão temporária de contêineres ou de compartilhamentos.

⚠ **Alerta de prova:** Revogar a SAS de serviço de um parceiro trocando a chave ou usando SAS de conta.
Como não cair: Ligue a SAS a uma política de acesso armazenada; remover a política invalida as SAS sem trocar chaves.

⚠ **Alerta de prova:** Habilitar namespace hierárquico ou GRS como pré-requisito da replicação de objetos.
Como não cair: Pré-requisitos são controle de versão nas duas contas e feed de alterações na origem; contas com namespace hierárquico não aceitam a replicação.

⚠ **Alerta de prova:** Usar azcopy copy --recursive para espelhar uma pasta removendo no destino o que sumiu na origem.
Como não cair: copy não remove itens do destino; use azcopy sync com --delete-destination=true.

⚠ **Alerta de prova:** Buscar blobs por atributo usando metadados ou marcas do recurso da conta.
Como não cair: Metadados não são indexados e marcas da conta não se aplicam a blobs; use marcas de índice de blob.

Como cai na prova

📝 **Como cai:** Requisitos de resiliência (zona, região, leitura da secundária, síncrono) e quatro siglas de redundância.
Como resolver: Pergunte em ordem: precisa sobreviver a zona? (Z). A região? (G). Ler a secundária sem failover? (RA). Monte a sigla e elimine as que faltam um requisito.

📝 **Como cai:** Um acidente com dados (apagou, sobrescreveu, corrompeu, contêiner excluído, compartilhamento excluído) e opções de proteção.
Como resolver: Associe o tipo de acidente ao recurso específico e descarte GRS, failover e bloqueios, que replicam o problema ou não atuam no plano de dados.

📝 **Como cai:** Acesso de terceiro ou aplicativo com restrições (sem chave, revogável, só um IP, só HTTPS, por uma hora).
Como resolver: Sem chave: delegação de usuário ou identidade gerenciada. Revogável: política armazenada. IP e protocolo: sip e spr. Cliente sem identidade no diretório: SAS, não função RBAC.

📝 **Como cai:** Escolha de camada pelo padrão de acesso e prazo de retenção.
Como resolver: Verifique se a leitura precisa ser imediata (Archive sai), confira o prazo mínimo (30, 90, 180) e escolha a camada mais fria que ainda atende.

📝 **Como cai:** Transferência ou sincronização de dados (volume, banda, frequência, discos próprios).
Como resolver: Online e por script: AzCopy (sync para espelhar). Gráfico: Storage Explorer. Offline com dispositivo da Microsoft: Data Box. Discos próprios: Import/Export. Cache contínuo de servidor de arquivos: File Sync.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Recuperar blob apagado em até X dias, sem restaurar backup	**Exclusão temporária de blobs**
Voltar contêineres ao estado de horas atrás após corrupção	**Restauração pontual para blobs de blocos**
Inalterado até segunda ordem, sem prazo	**Retenção legal**
Sete anos sem alterar ou excluir, nem pelo administrador	**Política de imutabilidade por tempo**
Ler a cópia secundária a qualquer momento, sem failover	**Prefixo RA (RA-GRS ou RA-GZRS)**
Lido raramente, guardado 90 dias, leitura imediata, menor custo	**Camada Cold**
Revogar acesso do parceiro sem trocar as chaves	**SAS de serviço com política de acesso armazenada**
Gerar SAS com as chaves da conta proibidas	**SAS de delegação de usuário**
Porta 445 bloqueada pelo provedor	**VPN ponto a site (ou site a site, ExpressRoute, File Sync)**

Filiais mantendo localmente só os arquivos usados com frequência	**Azure File Sync com camada de nuvem**
Dezenas de TB com link de internet lento	**Azure Data Box**
Diretórios reais e ACLs POSIX para big data	**Namespace hierárquico (Data Lake Storage)**
Milhões de pequenas gravações de blobs com latência baixa e estável	**Conta premium BlockBlobStorage**
Detectar malware logo após o upload	**Microsoft Defender for Storage com verificação de malware**

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

- GRS replica exclusões e corrupção; recuperar dados é exclusão temporária, versão ou restauração pontual.
- Bloqueios de recurso não protegem o conteúdo dos blobs.
- Archive é offline: reidratar antes de ler, até 15 horas na prioridade padrão.
- Só RA permite ler a secundária sem failover.
- Desativar a chave compartilhada derruba chaves e SAS de conta ou serviço, mas não a SAS de delegação de usuário.

Essenciais para a prova (checklist)

- ☐ Sei escolher entre Standard v2, BlockBlobStorage, FileStorage e blobs de página.
- ☐ Sei montar a sigla de redundância a partir de zona, região e leitura da secundária.
- ☐ Sei os prazos mínimos de Cool, Cold e Archive e quando há cobrança de exclusão antecipada.
- ☐ Sei qual recurso recupera blob apagado, sobrescrito, corrompido e contêiner excluído.
- ☐ Sei os pré-requisitos da restauração pontual e da replicação de objetos.
- ☐ Sei diferenciar SAS de conta, de serviço e de delegação de usuário e como revogar sem trocar chaves.
- ☐ Sei configurar firewall da conta, TLS mínimo, acesso anônimo e chaves gerenciadas pelo cliente.
- ☐ Sei montar Azure Files por SMB ou NFS, com autenticação por identidade e as funções SMB corretas.
- ☐ Sei configurar Azure File Sync com camada de nuvem e suas duas políticas.
- ☐ Sei escolher entre AzCopy (copy, sync, login), Storage Explorer, Data Box e Import/Export.

Questões de revisão do capítulo

R3.1 · Implementar e gerenciar armazenamento

Os blobs de log devem ir para a camada Cool após 30 dias sem modificação e ser excluídos após 365 dias, sem scripts. O que configurar?

A. Exclusão temporária de blobs por 365 dias
B. Replicação de objetos entre duas contas de armazenamento
C. Controle de versão de blobs no contêiner
D. Política de gerenciamento do ciclo de vida

R3.2 · Implementar e gerenciar armazenamento

Qual destes nomes é válido para uma conta de armazenamento do Azure?

A. contoso_dados
B. contosodados2026
C. contoso.dados
D. Contoso-Dados

R3.3 · Implementar e gerenciar armazenamento

Um script do AzCopy em uma VM deve autenticar sem SAS nem chaves, usando a identidade gerenciada da VM. Qual comando usar antes das cópias?

A. azcopy make com a chave
B. azcopy sync com a SAS
C. azcopy login com --identity
D. azcopy copy com a chave

R3.4 · Implementar e gerenciar armazenamento

Filiais usam servidores de arquivos Windows. A empresa quer centralizar os arquivos no Azure Files e manter nas filiais só os arquivos acessados com frequência. Qual solução usar?

A. AzCopy agendado em cada servidor das filiais
B. Azure File Sync com camada de nuvem habilitada
C. Serviço Azure Import/Export com discos físicos
D. Replicação de objetos entre contas de blob

Respostas comentadas

R3.1. D) Política de gerenciamento do ciclo de vida

Por quê: O gerenciamento do ciclo de vida aplica regras por prefixo ou marca de índice para mudar camadas (Hot, Cool, Cold, Archive) e excluir blobs, versões e snapshots.

✗ A) Incorreta. A exclusão temporária guarda dados excluídos, não exclui por idade.
✗ B) Incorreta. A replicação copia blobs para outra conta, sem mudar camadas.
✗ C) Incorreta. O controle de versão mantém versões anteriores, não move camadas.

> **Dica de prova:** Mover e excluir blobs por idade: ciclo de vida.

R3.2. B) contosodados2026

Por quê: O nome da conta forma o ponto de extremidade, como contosodados2026.blob.core.windows.net, e deve ser único em todo o Azure.

✗ A) Incorreta. O sublinhado não é permitido.
✗ C) Incorreta. O ponto não é permitido.
✗ D) Incorreta. Letras maiúsculas e hifens não são permitidos.

> **Dica de prova:** Nome de conta: 3 a 24 caracteres, minúsculas e números, único.

R3.3. C) azcopy login com --identity

Por quê: O AzCopy autentica com o Entra ID (login interativo, identidade gerenciada ou entidade de serviço) ou com SAS.

✗ A) Incorreta. make cria contêineres e também não usa chave.
✗ B) Incorreta. A SAS foi vetada.
✗ D) Incorreta. O AzCopy não aceita chave de conta diretamente.

> **Dica de prova:** AzCopy com identidade gerenciada: azcopy login --identity.

R3.4. B) Azure File Sync com camada de nuvem habilitada

Por quê: O Azure File Sync transforma o Windows Server em um cache do compartilhamento no Azure Files. Com a camada de nuvem, arquivos pouco usados ficam apenas na nuvem.

✗ A) Incorreta. O AzCopy copia dados, mas não faz cache nem sincronização contínua.
✗ C) Incorreta. Import/Export é para transferência única de grandes volumes.
✗ D) Incorreta. A replicação de objetos é para blobs, não para servidores de arquivos.

> **Dica de prova:** Cache local de Azure Files: File Sync com camada de nuvem.

04

CAPÍTULO 4 · 15-20% DA PROVA

Implementar e gerenciar redes virtuais

Aqui eu preciso dominar NSG (prioridade, regras padrão, sub-rede somada à NIC), emparelhamento (não transitivo, trânsito de gateway, tráfego encaminhado), Azure DNS público e privado, os três balanceadores (Load Balancer, Application Gateway e Traffic Manager), conectividade híbrida (VPN site a site, ponto a site e ExpressRoute) e acesso seguro (Bastion, Azure Firewall, gateway da NAT). A prova quase sempre traz um cenário com uma restrição bem específica, como sem IP privado, sem cliente de VPN ou só dentro da VNet, e quatro serviços parecidos: vence o que atende exatamente essa restrição. Também cai muito diagnóstico com o Network Watcher, em que cada ferramenta responde a uma pergunta diferente. Onde mais erro: confundir ponto de extremidade de serviço com ponto de extremidade privado e achar que regra de permissão ou origem mais específica vence no NSG.

Neste capítulo

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

Tópicos-chave

Ordem de avaliação do NSG

O NSG processa as regras da menor para a maior prioridade numérica e para na primeira correspondência. Não existe precedência de permitir sobre negar, a especificidade da origem não importa e a ordem de criação também não. Regra 100 negando a 3389 bloqueia mesmo que a 200 permita o IP do administrador.

Regras padrão de entrada do NSG

São AllowVnetInBound, AllowAzureLoadBalancerInBound e DenyAllInBound. Por isso VMs em sub-redes diferentes da mesma VNet já se comunicam sem regra personalizada, e as investigações de integridade do Load Balancer são liberadas pela marca AzureLoadBalancer, a menos que uma regra de negação com prioridade mais alta as bloqueie.

NSG na sub-rede e na NIC

Na entrada, o NSG da sub-rede é avaliado antes e depois o da NIC; os dois precisam permitir. NSGs não herdam regras entre si: se a NIC tem só as regras padrão, o DenyAllInBound dela bloqueia o tráfego que a sub-rede liberou. As regras de segurança efetivas da NIC mostram a combinação que realmente vale na VM.

Grupos de segurança de aplicativo e marcas de serviço

ASGs agrupam NICs das suas VMs e permitem regras com nomes lógicos, como ASG-Web e ASG-Dados; nova VM ganha as regras só ao entrar no ASG. Marcas de serviço representam serviços do Azure, são mantidas pela Microsoft e podem ser regionais, como Storage.BrazilSouth ou Sql.EastUS. ASG não representa serviço PaaS e marca não representa suas VMs.

Ponto de extremidade de serviço

Mantém o IP público do serviço, mas o tráfego sai pelo backbone com a identidade da sub-rede, usada nas regras de firewall do serviço. Não cria IP privado e não tem cobrança. A política de ponto de extremidade de serviço limita a saída da sub-rede a contas de armazenamento específicas, evitando exfiltração.

Ponto de extremidade privado (Private Link)

Recebe um IP privado da sub-rede para o serviço PaaS, permite desabilitar o acesso público e tem cobrança. Depende de DNS: a zona privada, como privatelink.blob.core.windows.net, precisa estar vinculada à VNet ou ser usada pelo servidor DNS da rede; sem isso, as VMs continuam resolvendo o IP público.

Emparelhamento de rede virtual

Exige espaços de endereços não sobrepostos; funciona entre assinaturas diferentes e entre regiões (emparelhamento global) e não exige gateway. Não é transitivo: VNet1-VNet2 e VNet2-VNet3 não ligam VNet1 a VNet3; a solução é emparelhar direto ou usar um hub com firewall ou NVA e rotas definidas pelo usuário.

Hub-spoke com gateway e NVA

Para os spokes usarem o gateway de VPN do hub, o hub habilita Permitir trânsito de gateway e cada spoke habilita Usar gateway remoto. Com uma NVA no hub, os emparelhamentos precisam Permitir tráfego encaminhado e a NIC da NVA precisa do encaminhamento de IP habilitado. Para muitas VNets, o Azure Virtual Network Manager gerencia conectividade hub-spoke ou malha e regras de administrador de segurança em escala.

Rotas definidas pelo usuário e rotas efetivas

Rotas definidas pelo usuário substituem as rotas do sistema; o próximo salto do tipo Solução de virtualização aponta para o IP da NVA. As rotas efetivas da NIC combinam rotas do sistema, BGP e definidas pelo usuário, e o diagnóstico de próximo salto do Network Watcher mostra a rota usada.

Endereços reservados e delegação de sub-rede

Em cada sub-rede o Azure reserva cinco endereços: rede, broadcast, gateway padrão e dois para DNS; uma /28 deixa 11 utilizáveis. A delegação reserva a sub-rede para que um serviço crie nela os próprios recursos de rede, exigida por Container Instances, integração com VNet do App Service e SQL Managed Instance.

IP público Standard e prefixo

IPs públicos Standard são estáticos, fecham a entrada até um NSG permitir e podem ser com redundância de zona, zonais ou sem zona; o SKU Basic foi desativado em 2025. Só o redundante entre zonas sobrevive à falha de uma zona. O prefixo de IP público reserva uma faixa contígua, como /28, útil para listas de permissão de parceiros.

Azure DNS público

Aceita registros A, AAAA, CAA, CNAME, MX, NS, PTR, SOA, SRV e TXT. CNAME não é permitido no domínio raiz; para apontar o raiz a um IP público, Traffic Manager ou Front Door e acompanhar trocas, usa-se registro de alias. A zona só resolve na internet depois de configurar no registrador os NS atribuídos pelo Azure DNS, e TTL alto mantém valores antigos em cache.

Zonas DNS privadas e Private Resolver

Zonas privadas resolvem nomes nas VNets vinculadas; com registro automático no vínculo, as VMs ganham registros A sozinhas. Cada VNet registra em uma única zona, embora uma zona aceite várias VNets e vínculos só de resolução não tenham esse limite. O DNS Private Resolver tem ponto de entrada (consultas vindas do local) e de saída (encaminhamento para DNS externos); o Azure não permite DHCP próprio na VNet, e após trocar o DNS da VNet é preciso reiniciar as VMs ou renovar o DHCP.

Azure Load Balancer

Balanceador de camada 4, público ou interno (IP privado para camadas internas). Distribui por hash de cinco tuplas; a persistência de sessão por IP do cliente mantém o cliente na mesma VM. Só envia tráfego a instâncias aprovadas na investigação de integridade (HTTP num caminho do aplicativo é mais preciso que TCP na porta), usa regras de NAT de entrada para publicar porta de uma VM específica e o pool fica em uma única VNet; entre regiões, usa-se o Load Balancer entre regiões.

Application Gateway e WAF

Balanceador de camada 7 com roteamento por caminho (/imagens/* e /api/*) e por host, ouvintes multissite para vários domínios no mesmo gateway, terminação TLS e WAF opcional. O WAF usa conjuntos de regras gerenciados, como o do OWASP, contra injeção de SQL e scripts entre sites, e pode ficar no Application Gateway ou no Front Door.

Traffic Manager

Balanceador por DNS global, com métodos prioridade, peso, desempenho, geográfico e multivalor. Desempenho envia cada usuário à região de menor latência. Não enxerga caminho de URL nem cabeçalho de host.

Gateway de VPN e ExpressRoute

Gateways de VPN e ExpressRoute ficam na sub-rede GatewaySubnet, recomendada /27 ou maior e sem NSG. A VPN site a site usa gateway de VPN, gateway de rede local com IP e prefixos locais e conexão com chave compartilhada; no modo ativo-ativo cada instância tem IP público próprio (o SKU Basic não oferece). A ponto a site aceita certificado, RADIUS ou Entra ID, com pool privado sem sobreposição; o ExpressRoute é conexão privada com SLA e banda definida, que não passa pela internet.

Bastion, Azure Firewall e gateway da NAT

O Bastion fica na AzureBastionSubnet e dá RDP e SSH pelo portal por TLS sem IP público nas VMs; Basic só pelo portal, Standard e Premium adicionam cliente nativo, e Developer não tem cliente nativo. O Azure Firewall tem regras DNAT (processadas primeiro), de rede e de aplicativo por FQDN. O gateway da NAT é o método recomendado de saída com IP fixo e escalável sem esgotar SNAT, já que novas VNets não têm mais acesso de saída padrão.

Macetes para memorizar

NSG

Menor número manda, e quem casa primeiro encerra a conversa.

Endereços da sub-rede

Sub-rede no Azure: total menos 5 (/28 = 16 - 5 = 11).

Emparelhamento

Amigo do meu amigo não é meu amigo: emparelhamento não é transitivo.

Hub-spoke

Hub empresta (trânsito de gateway), spoke usa (gateway remoto); NVA no meio pede tráfego encaminhado.

Endpoints

Serviço = mesmo endereço público com crachá da sub-rede; Privado = endereço de casa dentro da VNet (e precisa de DNS).

Balanceadores

4 = Load Balancer (IP/porta); 7 = Application Gateway (URL/host); DNS = Traffic Manager (regiões).

Network Watcher

Qual regra? fluxo de IP. Qual rota? próximo salto. Onde falha agora? solução de problemas de conexão. Sempre? Monitor de Conexão.

Tabela de memorização: não confunda

Quando é...	...e quando é
Ponto de extremidade de serviço Filtrar o acesso por sub-rede, sem IP privado e sem custo; o serviço segue no IP público.	**Ponto de extremidade privado** Acessar o PaaS por um IP privado da VNet, com acesso público desabilitado; exige zona DNS privatelink.

Load Balancer Camada 4 (IP e porta), interno ou público, NAT de entrada, persistência por IP do cliente.	**Application Gateway** Camada 7: roteamento por caminho ou host, ouvintes multissite, terminação TLS e WAF.
Traffic Manager Distribuir usuários entre regiões por DNS (prioridade, peso, desempenho, geográfico, multivalor).	**Application Gateway** Rotear por URL ou nome de host dentro de uma região.
VPN site a site Túnel IPsec criptografado pela internet entre datacenter e VNet.	**ExpressRoute** Conexão privada e dedicada, sem internet, com SLA e banda previsível; a VPN pode ser o backup.
VPN ponto a site Notebooks de usuários remotos acessando a VNet, com cliente Azure VPN e autenticação do Entra.	**Azure Bastion** RDP e SSH pelo navegador, sem IP público nas VMs e sem instalar cliente de VPN.
Azure Firewall Ponto central de saída filtrando por FQDN (*.microsoft.com) ou publicando servidor por DNAT.	**NSG** Filtrar por IP, porta e marcas de serviço na sub-rede ou NIC; não entende FQDN nem conteúdo.
Verificação de fluxo de IP Saber qual regra de NSG permitiu ou negou um fluxo de 5 tuplas.	**Diagnóstico de próximo salto** Saber qual rota o pacote usa, por exemplo depois de associar uma rota definida pelo usuário.

Números que caem

Item	Valor
Endereços reservados pelo Azure em cada sub-rede	**5 (uma /28 deixa 11 utilizáveis)**
Tamanho recomendado da GatewaySubnet	**/27 ou maior**
SKU Basic de IP público	**Desativado em 2025**
Regras padrão de entrada do NSG	**3: AllowVnetInBound, AllowAzureLoadBalancerInBound, DenyAllInBound**
Hash padrão de distribuição do Load Balancer	**Cinco tuplas**
Zonas DNS em que uma VNet pode fazer registro automático	**1**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que a regra 200 que permite o IP do administrador vence a regra 100 que nega a porta, por ser mais específica ou de permissão.
Como não cair: No NSG vale o menor número e a avaliação para na primeira correspondência; especificidade, tipo de ação e ordem de criação não importam.

⚠ **Alerta de prova:** Supor que o NSG da NIC herda a liberação feita no NSG da sub-rede.
Como não cair: NSGs não herdam regras; na entrada os dois são avaliados e os dois precisam permitir, senão o DenyAllInBound da NIC bloqueia.

⚠ **Alerta de prova:** Criar um CNAME no domínio raiz para apontar contoso.com a um recurso do Azure.
Como não cair: CNAME não é permitido no raiz; use registro de alias, que também acompanha a troca do IP.

⚠ **Alerta de prova:** Atribuir a falha do emparelhamento a assinaturas ou regiões diferentes, ou à falta de gateway.
Como não cair: Emparelhamento funciona entre assinaturas e regiões e não exige gateway; o que impede é espaço de endereços sobreposto.

⚠ **Alerta de prova:** Resolver VNet1 sem alcançar VNet3 com regra de NSG, zona DNS ou ponto de extremidade na VNet2.
Como não cair: Emparelhamento não é transitivo: crie o emparelhamento direto ou use hub com NVA e rotas definidas.

⚠ **Alerta de prova:** Concluir que o IP Standard exige recriar a VM, só funciona com balanceador ou usa alocação dinâmica.
Como não cair: O IP Standard é estático, pode ir direto na NIC e fecha a entrada até um NSG permitir.

⚠ **Alerta de prova:** Com o private endpoint resolvendo IP público, criar ponto de extremidade de serviço, abrir porta 443 ou adicionar rota.
Como não cair: O problema é de nome: vincule a zona privatelink.blob.core.windows.net à VNet.

⚠ **Alerta de prova:** Zona pública que não resolve: habilitar registro automático ou vincular a zona à VNet.
Como não cair: Registro automático e vínculos são de zonas privadas; a zona pública precisa dos NS configurados no registrador.

⚠ **Alerta de prova:** Usar NSG com marcas de serviço ou gateway da NAT para liberar saída só para domínios aprovados.
Como não cair: NSG não filtra por FQDN e o gateway da NAT só dá saída; filtrar por domínio é o Azure Firewall com regras de aplicativo.

⚠ **Alerta de prova:** Usar captura de pacotes, topologia ou próximo salto para descobrir qual regra bloqueou a porta 443.
Como não cair: Só a verificação de fluxo de IP retorna a regra que permitiu ou negou o fluxo.

⚠ **Alerta de prova:** Ligar persistência de sessão ou aumentar o tempo limite de ociosidade para parar de enviar tráfego à VM com aplicativo parado.
Como não cair: Quem tira a instância do pool é a investigação de integridade; use HTTP num caminho do aplicativo, pois TCP na porta pode passar com o app falhando.

⚠ **Alerta de prova:** Escolher Bastion Basic ou Developer para usar o mstsc, ou gateway de VPN Basic para ativo-ativo.
Como não cair: Cliente nativo exige Bastion Standard ou Premium; o SKU Basic do gateway de VPN não oferece ativo-ativo.

⚠ **Alerta de prova:** Montar servidor DHCP próprio na VNet ou zona pública com nomes internos para resolver nomes privados.
Como não cair: O Azure não permite DHCP próprio e zona pública expõe nomes; use zona DNS privada com registro automático ou o DNS Private Resolver.

⚠ **Alerta de prova:** Com investigações bloqueadas por NSG personalizado, liberar a marca Internet ou criar rota para o IP de investigação.
Como não cair: É filtragem, não rota: libere a marca de serviço AzureLoadBalancer acima da regra de negação.

Como cai na prova

📝 **Como cai:** Cenário com requisito e restrições negativas (sem IP público, sem VPN, sem custo, sem criar gateways) e quatro serviços de rede.
Como resolver: Sublinhe cada restrição, elimine quem viola qualquer uma (VPN exige cliente, IP público expõe, DNAT publica porta) e escolha o serviço cujo propósito é exatamente o pedido.

📝 **Como cai:** Duas regras de NSG ou dois NSGs (sub-rede e NIC) e a pergunta se o tráfego chega.
Como resolver: Ordene por prioridade, pare na primeira que casa; depois confira se o outro NSG também permite, lembrando que regras padrão terminam em DenyAllInBound.

📝 **Como cai:** Problema de diagnóstico pedindo uma ferramenta do Network Watcher.
Como resolver: Identifique a pergunta: qual regra (verificação de fluxo de IP), qual rota (próximo salto ou rotas efetivas), teste pontual com saltos (solução de problemas de conexão), contínuo com alerta (Monitor de Conexão), pacotes (captura), histórico de fluxos (logs de fluxo de VNet).

📝 **Como cai:** Hub-spoke ou emparelhamentos em que o tráfego não chega.
Como resolver: Verifique na ordem: endereços sobrepostos, falta de emparelhamento direto (não transitivo), trânsito de gateway mais gateway remoto para chegar ao local e Permitir tráfego encaminhado quando há NVA.

📝 **Como cai:** Nome que não resolve ou resolve errado.
Como resolver: Zona pública: NS no registrador. Private endpoint resolvendo IP público: zona privatelink vinculada. Valor antigo por horas: TTL. VMs com DNS velho: reiniciar. Erro no registro automático: VNet já registra em outra zona.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Aceitar tráfego só de uma sub-rede, pelo backbone, sem IP privado e sem pagar	**Ponto de extremidade de serviço**
IP privado da própria VNet para o PaaS, acesso público desabilitado	**Ponto de extremidade privado + zona DNS privatelink**
Limitar a saída a contas de armazenamento específicas, evitar exfiltração	**Política de ponto de extremidade de serviço**
Domínio raiz apontando para IP público do Azure	**Registro de alias**
/imagens/* para um pool e /api/* para outro, com TLS	**Application Gateway com regras baseadas em caminho**
Vários domínios no mesmo gateway, cada um com seu pool	**Ouvintes multissite do Application Gateway**
Cada usuário enviado por DNS à região de menor latência	**Traffic Manager com roteamento por desempenho**
RDP ou SSH pelo navegador, sem IP público e sem cliente de VPN	**Azure Bastion**
Saída com IP fixo e escalável, sem esgotar portas SNAT	**Gateway da NAT associado à sub-rede**
Conexão privada, dedicada, sem internet, banda previsível	**ExpressRoute**
Funcionários remotos com conta do Entra e MFA nos notebooks	**VPN ponto a site com autenticação do Entra**

Spokes usando o gateway do hub sem criar gateways	**Trânsito de gateway no hub + Usar gateway remoto nos spokes**
Datacenter local resolvendo zonas privadas do Azure sem VMs de DNS	**Ponto de entrada do DNS Private Resolver**
Dezenas de VNets em hub-spoke aplicado por grupos de rede	**Azure Virtual Network Manager**

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

- NSG: menor prioridade numérica vence e a avaliação para na primeira correspondência; sub-rede e NIC precisam permitir.
- Emparelhamento não é transitivo e exige endereços sem sobreposição.
- Ponto de extremidade de serviço não cria IP privado; ponto de extremidade privado cria IP e depende de zona DNS privatelink.
- CNAME não vai no domínio raiz: use alias; zona pública só resolve após apontar os NS no registrador.
- IP público Standard é estático e fechado na entrada até um NSG liberar.

Essenciais para a prova (checklist)

☐ Sei calcular se o tráfego passa com regras de NSG na sub-rede e na NIC.

☐ Sei quantos endereços ficam livres em qualquer sub-rede do Azure.

☐ Sei configurar hub-spoke com trânsito de gateway, gateway remoto e tráfego encaminhado.

☐ Sei escolher entre ponto de extremidade de serviço, ponto de extremidade privado e política de ponto de extremidade de serviço.

☐ Sei escolher entre Load Balancer interno ou público, Application Gateway e Traffic Manager pelo requisito.

☐ Sei montar uma VPN site a site e dizer quando usar ponto a site, ativo-ativo ou ExpressRoute.

☐ Sei qual ferramenta do Network Watcher responde a cada pergunta de diagnóstico.

☐ Sei resolver problemas de DNS público, zona privada, registro automático e Private Resolver.

☐ Sei quando usar Bastion (e qual SKU), Azure Firewall com DNAT ou FQDN e gateway da NAT.

Questões de revisão do capítulo

R4.1 · Implementar e gerenciar redes virtuais

Um IP público Standard foi associado a uma VM, mas as conexões de entrada falham. A sub-rede e a NIC não têm NSG. Qual é a causa?

A. O IP Standard fecha a entrada até um NSG permitir
B. A VM precisa ser recriada para usar o IP Standard
C. O IP Standard só funciona com um balanceador de carga
D. O IP Standard só aceita alocação dinâmica de endereço

R4.2 · Implementar e gerenciar redes virtuais

Um servidor interno deve ser publicado na internet pela porta 443 do IP público de um Azure Firewall. Que tipo de regra criar?

A. Regra DNAT no Azure Firewall
B. Regra de rede de saída
C. Marca de serviço no NSG
D. Regra de aplicativo por FQDN

R4.3 · Implementar e gerenciar redes virtuais

Os e-mails do domínio contoso.com, hospedado no Azure DNS, devem ser entregues a um provedor de e-mail. Qual registro criar?

A. Registro MX
B. Registro SRV
C. Registro PTR
D. Registro CNAME

R4.4 · Implementar e gerenciar redes virtuais

Em um Load Balancer Standard, onde podem estar as VMs do pool de back-end?

A. Em servidores locais pela VPN
B. Em uma única rede virtual
C. Em VNets de regiões diferentes
D. Em qualquer VNet da assinatura

Respostas comentadas

R4.1. A) O IP Standard fecha a entrada até um NSG permitir

Por quê: IPs públicos Standard são estáticos, podem ser redundantes entre zonas e fecham a entrada por padrão. O SKU Basic foi desativado em 2025.

✗ B) Incorreta. Não é preciso recriar a VM.
✗ C) Incorreta. Ele pode ser associado diretamente a uma NIC.
✗ D) Incorreta. O IP Standard usa alocação estática.

> **Dica de prova:** IP público Standard: fechado até um NSG liberar.

R4.2. A) Regra DNAT no Azure Firewall

Por quê: Regras DNAT são processadas antes das regras de rede e de aplicativo e criam implicitamente a regra de rede correspondente.

✗ B) Incorreta. Regras de rede tratam o tráfego entre redes.
✗ C) Incorreta. Marcas não publicam servidores.
✗ D) Incorreta. Regras de aplicativo tratam saída HTTP e HTTPS.

> **Dica de prova:** Publicar servidor pelo firewall: DNAT.

R4.3. A) Registro MX

Por quê: O Azure DNS aceita registros A, AAAA, CAA, CNAME, MX, NS, PTR, SOA, SRV e TXT.

✗ B) Incorreta. O SRV localiza serviços como SIP.
✗ C) Incorreta. O PTR é para resolução reversa.
✗ D) Incorreta. O CNAME cria um apelido para outro nome.

> **Dica de prova:** E-mail do domínio: registro MX.

R4.4. B) Em uma única rede virtual

Por quê: Para distribuir entre regiões, usa-se o Load Balancer entre regiões (global) na frente de balanceadores regionais.

✗ A) Incorreta. O pool contém recursos da VNet.
✗ C) Incorreta. Balanceadores regionais atendem uma região.
✗ D) Incorreta. O pool não mistura VNets diferentes.

> **Dica de prova:** Pool do Load Balancer: uma VNet.

05

CAPÍTULO 5 · 10-15% DA PROVA

Monitorar e manter recursos do Azure

Aqui eu preciso saber o que o Azure Monitor coleta sozinho e o que exige configuração, escolher o tipo de alerta certo e configurar grupos de ações e regras de processamento, escrever KQL básico e usar o Network Watcher. Na parte de manutenção, preciso dominar o Azure Backup (cofres, políticas, opções de restauração, exclusão temporária) e o Azure Site Recovery (replicação, planos de recuperação, failover de teste). A prova cobra muito a diferença entre backup e recuperação de desastres, entre os dois tipos de cofre e entre log de atividades e logs de recurso. Onde mais erro: achar que o log de atividades mostra operações de dados, que o agente MMA ainda é a resposta e que take seguido de sort traz os maiores valores.

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

Tópicos-chave

Dados coletados automaticamente

Métricas de plataforma e log de atividades são coletados sem configuração. Logs de recurso exigem configuração de diagnóstico, e eventos do Windows, Syslog e contadores do SO exigem agente e regra de coleta. Métricas de plataforma ficam 93 dias no banco de métricas.

Log de atividades

Registra operações do plano de controle, como quem excluiu uma VM, e guarda 90 dias; para retenção maior, envie-o a um workspace por configuração de diagnóstico. Não mostra operações de dados, como leitura de segredos do Key Vault, que exigem logs de recurso (AuditEvent).

Configurações de diagnóstico

Enviam logs de recurso e métricas para workspace do Log Analytics (consulta com KQL), conta de armazenamento (arquivamento barato), Hubs de Eventos ou soluções de parceiros. Cofres, grupos de ações e Key Vault não são destinos.

Azure Monitor Agent e regras de coleta de dados

O Azure Monitor Agent usa regras de coleta de dados (DCR) para definir fontes, filtros e destinos, e uma regra pode ser associada a várias VMs. O agente do Log Analytics (MMA) foi desativado em 2024 e deu lugar ao AMA.

Workspace do Log Analytics

Tabelas têm retenção interativa, para consultas frequentes, e retenção de longo prazo, mais barata, consultada por pesquisa ou restauração, até 12 anos. O modo de acesso no contexto do recurso (Usar permissões de recurso ou workspace) deixa cada dono ver só os logs dos próprios recursos. Tabelas mais cobradas na prova: Heartbeat (agente ativo), Perf (contadores), Event (eventos do Windows) e Syslog (Linux).

KQL essencial

where filtra linhas, project escolhe colunas, extend cria colunas calculadas e summarize agrega por grupo, como summarize avg(CounterValue) by Computer. top 10 by CounterValue desc ordena e limita; take devolve linhas quaisquer, para exploração; distinct lista valores únicos.

Gerenciador de métricas

Métricas multidimensionais podem ser filtradas e divididas por dimensões, como API name, Response type e Authentication, para separar transações por tipo de operação. A agregação (Máximo, Média) não separa por dimensão.

Tipos de regra de alerta

Alertas de métrica avaliam séries numéricas quase em tempo real e podem usar limites dinâmicos, que aprendem sazonalidade horária, diária e semanal. Alertas de pesquisa de logs usam consultas KQL com frequência e janela, como mais de cinco erros 500 em dez minutos. Alertas do log de atividades monitoram operações administrativas, como exclusão de VM, além de eventos do Service Health e do Resource Health.

Grupos de ações e regras de processamento

A regra de alerta define a condição; o grupo de ações define quem é avisado (e-mail, SMS, push, voz) e o que roda (webhook, função, Logic App, runbook, Event Hubs). Regras de processamento de alertas adicionam ou suprimem grupos de ações em alertas disparados, com escopo, filtros e agenda: silenciam notificações na manutenção ou avisam a central em todos os alertas sem editar cada regra.

Service Health, Resource Health e Advisor

Service Health mostra incidentes, manutenções planejadas e avisos da plataforma para os serviços e regiões usados, com alertas. Resource Health diz se um recurso está disponível, degradado ou indisponível e se a causa foi da plataforma ou do usuário. O Advisor traz recomendações de Custo, Segurança, Confiabilidade, Excelência Operacional e Desempenho, sem registrar operações.

Pastas de trabalho e VM insights

Pastas de trabalho (Workbooks) são relatórios interativos que combinam KQL, métricas, texto e parâmetros. VM insights coleta desempenho e, com o recurso Mapa, processos e conexões entre VMs e serviços externos, usando o Azure Monitor Agent e um workspace.

Network Watcher para monitoramento

Monitor de Conexão mede de forma contínua latência, perda e topologia entre Azure e local, com alertas. Captura de pacotes usa extensão na VM, filtra por protocolo, IP e porta e salva arquivo para o Wireshark. Logs de fluxo de rede virtual registram fluxos com origem, destino, portas e decisão, substituem os logs de fluxo de NSG e alimentam a Análise de Tráfego.

Tipos de cofre do Azure Backup

O Cofre dos Serviços de Recuperação atende VMs, Azure Files, SQL em VM e SAP HANA; o Cofre de Backup atende blobs, discos, PostgreSQL e AKS. O cofre precisa estar na mesma região e assinatura dos recursos protegidos (o grupo de recursos pode ser outro). A restauração entre regiões exige cofre GRS e deve ser definida antes de proteger itens, pois a redundância do cofre não muda depois.

Backup de VM e políticas

O backup de VM do Azure usa uma extensão instalada pelo serviço, sem agente MARS: basta cofre e política. A política padrão faz um backup por dia; a aprimorada permite backups por hora, com intervalos a partir de quatro horas, e suporta Trusted Launch. Uma VM tem só uma política, que combina retenções diária, semanal, mensal e anual; a restauração instantânea usa os snapshots e é mais rápida que a camada do cofre.

Opções de restauração e exclusão temporária

Restaurar VM pode criar uma nova VM (mantendo a atual para comparação), restaurar discos ou substituir discos; a recuperação de arquivos baixa um script que monta os discos do ponto de recuperação para copiar só o necessário. A exclusão temporária mantém dados de backup excluídos por 14 dias adicionais, sem custo, habilitada por padrão, e pode ser ampliada na exclusão temporária aprimorada.

Agente MARS e Backup de Disco

O agente MARS envia arquivos e pastas de Windows local ou VMs diretamente ao Cofre dos Serviços de Recuperação, com agenda e retenção, sem outra infraestrutura local. O Backup de Disco do Azure é sem agente, gerenciado pelo Cofre de Backup, com snapshots incrementais agendados e restauração para novos discos.

Azure Site Recovery

Solução de recuperação de desastres com replicação contínua entre regiões e RPO de poucos minutos; usa a extensão Mobility Service, cofre dos Serviços de Recuperação na região de destino e política de replicação com retenção e frequência de pontos consistentes com o aplicativo. Planos de recuperação agrupam VMs e definem ordem, scripts e ações manuais; o failover de teste em rede isolada valida sem impacto, com limpeza depois.

Centro de continuidade de negócios

Sucessor do Centro de backup, reúne em um só lugar proteção, trabalhos, alertas e políticas de backup e replicação de vários cofres e assinaturas.

Macetes para memorizar

💡 Retenções do Monitor

Métrica 93, atividade 90: os dois chegam juntos e sozinhos; o resto precisa de diagnóstico ou agente.

💡 Alerta e ação

A regra diz quando; o grupo de ações diz quem e o quê; a regra de processamento diz quando calar ou somar.

💡 Backup x DR

Backup guarda o passado (pontos); Site Recovery mantém um gêmeo vivo em outra região.

💡 Cofres

Serviços de Recuperação = VM, Files, SQL, SAP HANA; Backup vault = blobs, discos, PostgreSQL, AKS.

💡 KQL

where filtra, project escolhe, extend cria, summarize agrupa, top ranqueia.

💡 Agentes

MARS = arquivos locais; Mobility = Site Recovery; AMA = monitoramento; extensão de backup = VM no cofre.

Tabela de memorização: não confunda

Quando é...	...e quando é
Azure Backup Proteger contra perda de dados com pontos de recuperação e restaurar VM, discos ou arquivos.	**Azure Site Recovery** Recuperação de desastres: replicação contínua, failover para outra região e RPO de minutos.
Cofre dos Serviços de Recuperação VMs, Azure Files, SQL em VM, SAP HANA, agente MARS e Site Recovery.	**Cofre de Backup** Blobs, discos gerenciados, PostgreSQL e AKS.
Alerta de métrica Condição numérica quase em tempo real, com limite estático ou dinâmico.	**Alerta de pesquisa de logs** Condição sobre registros de log consultados com KQL, como contagem de erros 500.

Log de atividades Quem criou, alterou ou excluiu recursos (plano de controle), automático, 90 dias.	**Logs de recurso** Operações de dados do serviço, como leitura de segredos, via configuração de diagnóstico.
Service Health Incidentes e manutenções da plataforma nos serviços e regiões que eu uso.	**Resource Health** Se um recurso específico ficou indisponível e se a causa foi da plataforma.
Monitor de Conexão Medir latência e perda continuamente, com alertas.	**Solução de problemas de conexão** Testar uma vez, agora, e ver em qual salto a conexão falha.
top N by coluna desc Trazer os N maiores valores.	**take N** Pegar N linhas quaisquer para exploração rápida.

Números que caem

Item	Valor
Retenção das métricas de plataforma	**93 dias**
Retenção do log de atividades	**90 dias**
Retenção de longo prazo no Log Analytics	**Até 12 anos**
Exclusão temporária no Azure Backup	**14 dias adicionais, sem custo**
Intervalo mínimo da política aprimorada de backup de VM	**A partir de 4 horas**
Backups por dia na política padrão de VM	**1**
Desativação do agente do Log Analytics (MMA)	**2024**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Instalar o agente do Log Analytics (MMA) para coletar eventos do Windows e Syslog.
Como não cair: O MMA foi desativado em 2024; use o Azure Monitor Agent com regra de coleta de dados.

⚠ **Alerta de prova:** Procurar no log de atividades quem leu segredos do Key Vault.
Como não cair: O log de atividades é plano de controle; habilite configuração de diagnóstico com os logs AuditEvent.

⚠ **Alerta de prova:** Responder 30 dias ou 2 anos para a retenção padrão das métricas de plataforma.
Como não cair: São 93 dias; para mais, envie a um workspace.

⚠ **Alerta de prova:** Excluir o grupo de ações ou baixar a gravidade para não notificar na janela de manutenção.
Como não cair: Use regra de processamento de alertas com agenda para suprimir as ações; os alertas continuam sendo gerados.

⚠ **Alerta de prova:** Ajustar um limite estático para CPU que varia entre dias úteis e fins de semana.
Como não cair: Limites dinâmicos aprendem a sazonalidade e reduzem alertas falsos.

⚠ **Alerta de prova:** Escrever Perf | take 10 | sort by CounterValue para obter os 10 maiores.
Como não cair: take pega 10 linhas quaisquer antes de ordenar; use top 10 by CounterValue desc.

⚠ **Alerta de prova:** Associar duas políticas de backup à mesma VM para ter retenção diária e mensal.
Como não cair: Cada VM tem uma política, e ela combina retenções diária, semanal, mensal e anual.

⚠ **Alerta de prova:** Achar que o cofre não aparece porque precisa ser GRS ou estar no mesmo grupo de recursos.
Como não cair: O cofre precisa estar na mesma região e assinatura da VM; LRS e ZRS também servem e o grupo pode ser outro.

⚠ **Alerta de prova:** Instalar o agente MARS para fazer backup de VMs do Azure ou para o Site Recovery.
Como não cair: Backup de VM usa extensão do serviço e o Site Recovery usa a Mobility Service; MARS é para arquivos e pastas.

⚠ **Alerta de prova:** Fazer failover planejado para validar o plano de DR.
Como não cair: Failover real afeta a produção; valide com failover de teste em rede isolada.

⚠ **Alerta de prova:** Usar Site Recovery ou restaurar a VM inteira para recuperar um arquivo apagado.
Como não cair: Use a recuperação de arquivos a partir do ponto de recuperação, com menor impacto.

⚠ **Alerta de prova:** Atender RPO de poucos minutos com Azure Backup diário ou snapshots agendados.
Como não cair: Backup diário dá RPO de até 24 horas; replicação contínua com failover é o Site Recovery.

⚠ **Alerta de prova:** Dar Leitor do Log Analytics no workspace para cada dono ver só as próprias VMs.
Como não cair: Essa função abre todos os dados; use o acesso no contexto do recurso.

⚠ **Alerta de prova:** Concluir que dados de backup excluídos do cofre não podem ser recuperados.
Como não cair: A exclusão temporária, habilitada por padrão, guarda por 14 dias adicionais sem custo.

Como cai na prova

📝 **Como cai:** Precisa ser avisado de algo e há quatro tipos de alerta.
Como resolver: Pergunte a origem do sinal: número de desempenho (métrica, dinâmico se sazonal), texto de log (pesquisa de logs com KQL), operação administrativa (log de atividades), falha da plataforma (Service Health).

📝 **Como cai:** Requisito de proteção com tempo de recuperação, retenção e escopo.
Como resolver: Perda de dados e restauração: Azure Backup (política padrão ou aprimorada). Desastre regional com RPO de minutos: Site Recovery. Um arquivo só: recuperação de arquivos. Manter a VM atual: restaurar como nova VM.

📝 **Como cai:** Qual cofre ou por que o cofre não aparece.
Como resolver: Classifique o item (VM, Files, SQL, SAP HANA no Serviços de Recuperação; blobs, discos, PostgreSQL, AKS no Cofre de Backup) e confira região e assinatura iguais às do recurso.

📝 **Como cai:** Consulta KQL com quatro variações de operador.
Como resolver: Identifique a intenção (filtrar, escolher colunas, criar coluna, agregar, ranquear) e escolha o operador; desconfie de take antes de ordenar.

📝 **Como cai:** Dados que não aparecem no Monitor (eventos de VM, leituras de segredos, logs antigos).
Como resolver: Lembre que só métricas de plataforma e log de atividades são automáticos; o resto precisa de AMA com DCR ou configuração de diagnóstico, e retenção longa vai para workspace ou armazenamento.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Quem excluiu a VM ontem	**Log de atividades**
Avisar toda vez que alguém excluir uma VM	**Alerta do log de atividades**
Mais de N erros em X minutos num log de aplicativo	**Alerta de pesquisa de logs**
Alertas gerados mas sem notificações durante a manutenção	**Regra de processamento de alertas (suprimir)**
Falha da própria plataforma Azure nos serviços da região	**Alerta de integridade do serviço (Service Health)**

VM indisponível por minutos: foi a plataforma?	**Resource Health**
Relatório interativo com KQL, métricas, texto e parâmetros	**Pastas de trabalho**
Processos e conexões entre VMs	**VM insights com Mapa**
Agente da VM ainda se comunica com o workspace?	**Tabela Heartbeat**
Logs por dois anos, consultas raras, menor custo	**Retenção de longo prazo na tabela**
Backup a cada quatro horas	**Política aprimorada de backup de VM**
Restaurar na região secundária em desastre	**Restauração entre regiões em cofre GRS**
Banco sobe antes dos servidores web no failover	**Plano de recuperação com grupos em ordem**
Arquivos de servidor Windows local para o Azure toda noite	**Agente MARS + Cofre dos Serviços de Recuperação**

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

- Só métricas de plataforma (93 dias) e log de atividades (90 dias) são coletados sem configuração.
- Log de atividades é plano de controle; leitura de dados exige logs de recurso por diagnóstico.
- Backup protege dados; Site Recovery faz DR com failover e RPO de minutos.
- Cofre na mesma região e assinatura do recurso; restauração entre regiões exige GRS definido antes.
- Testar DR é failover de teste em rede isolada.

Essenciais para a prova (checklist)

☐ Sei o que o Azure Monitor coleta automaticamente e o que exige agente ou diagnóstico.

☐ Sei escolher entre alerta de métrica, de pesquisa de logs, do log de atividades e de integridade do serviço.

☐ Sei configurar grupos de ações e regras de processamento de alertas.

☐ Sei escrever KQL com where, project, extend, summarize e top.

☐ Sei configurar retenção e controle de acesso de um workspace do Log Analytics.

☐ Sei qual ferramenta do Network Watcher monitora, testa, captura ou registra tráfego.

☐ Sei qual cofre protege cada tipo de recurso e os requisitos de região e redundância.

☐ Sei montar políticas de backup de VM (padrão e aprimorada) com várias retenções.

☐ Sei escolher a opção de restauração certa, inclusive recuperação de arquivos e restauração instantânea.

☐ Sei configurar Site Recovery com plano de recuperação e validar com failover de teste.

Questões de revisão do capítulo

R5.1 · Monitorar e manter recursos do Azure

A equipe quer ver e gerenciar em um só lugar os backups e a replicação de vários cofres e assinaturas. O que usar?

A. Log de atividades de cada assinatura
B. Painel de cada cofre, um por vez
C. Centro de continuidade de negócios
D. Recomendações do Azure Advisor

R5.2 · Monitorar e manter recursos do Azure

A equipe quer backup agendado de discos gerenciados com snapshots incrementais, sem fazer backup da VM inteira. O que usar?

A. Agente MARS no cofre dos Serviços de Recuperação
B. Exclusão temporária nos discos gerenciados
C. Backup de Disco do Azure em um Cofre de Backup
D. Azure Site Recovery entre regiões

R5.3 · Monitorar e manter recursos do Azure

Uma VM corrompida será restaurada do Azure Backup, mas a VM atual deve ficar disponível para comparação. Qual opção de restauração usar?

A. Failover de teste do Site Recovery
B. Substituir os discos da VM existente pelos do ponto
C. Recuperação de arquivos com o script
D. Criar nova VM do ponto de recuperação

R5.4 · Monitorar e manter recursos do Azure

Uma VM de produção foi excluída ontem, e o gestor quer saber quem fez isso. Onde verificar?

A. Log de atividades da assinatura
B. Métricas de plataforma da VM
C. Painel do Service Health
D. Recomendações do Azure Advisor na assinatura

Respostas comentadas

R5.1. C) Centro de continuidade de negócios

Por quê: O Centro de continuidade de negócios do Azure (sucessor do Centro de backup) reúne proteção, trabalhos, alertas e políticas em escala.

✗ A) Incorreta. O log mostra operações, sem gestão de backup.
✗ B) Incorreta. Isso não centraliza a visão.
✗ D) Incorreta. O Advisor não gerencia backups.

> **Dica de prova:** Visão central de backup e DR: Centro de continuidade de negócios.

R5.2. C) Backup de Disco do Azure em um Cofre de Backup

Por quê: O Backup de Disco do Azure é uma solução sem agente, gerenciada pelo Cofre de Backup, com restauração para novos discos.

✗ A) Incorreta. O agente MARS é para arquivos e pastas.
✗ B) Incorreta. Discos gerenciados não têm exclusão temporária própria.
✗ D) Incorreta. O Site Recovery replica para recuperação de desastres.

> **Dica de prova:** Backup só do disco: Backup de Disco do Azure.

R5.3. D) Criar nova VM do ponto de recuperação

Por quê: As opções de restauração de VM incluem criar uma nova VM, restaurar discos e substituir discos existentes. Recuperação de arquivos atende itens pontuais.

✗ A) Incorreta. O Site Recovery não usa pontos do Azure Backup.
✗ B) Incorreta. A substituição altera a VM atual.
✗ C) Incorreta. Ela recupera arquivos, não a VM inteira.

> **Dica de prova:** Manter a VM atual: restaurar como nova VM.

R5.4. A) Log de atividades da assinatura

Por quê: O log de atividades guarda 90 dias de eventos do plano de controle. Para retenção maior, envie-o a um workspace por configuração de diagnóstico.

✗ B) Incorreta. Métricas mostram desempenho, não quem agiu.
✗ C) Incorreta. Ele mostra incidentes da plataforma.
✗ D) Incorreta. O Advisor não registra operações.

> **Dica de prova:** Quem excluiu o recurso: log de atividades.

DIA DA PROVA

Estratégia de prova

A AZ-104 é uma prova de administrador: quase toda questão descreve um cenário operacional e pede o recurso, a configuração ou o diagnóstico que resolve exatamente aquele requisito. As alternativas costumam ser serviços reais e parecidos, todos úteis em outro contexto, e a diferença está numa restrição do enunciado, como sem IP público, sem scripts, menor privilégio ou sem alterar a definição. Há questões de múltipla resposta (Escolha DUAS) e muitas cobram fatos fixos: prioridade de NSG, prazos das camadas, retenções do Monitor, SLAs e escopos de bloqueios. A pontuação vai de 1 a 1000 com mínimo de 700, e os maiores pesos estão em identidade e governança e em computação (20-25% cada).

Como responder

✓ Controle o tempo: são 100 minutos para cerca de 50 questões (a Microsoft não divulga o número exato, entre 40 e 60), o que dá perto de 2 minutos por questão; marque as demoradas e volte depois.

✓ Leia a última frase primeiro e sublinhe as restrições (sem X, apenas Y, menor custo, menor privilégio, sem indisponibilidade); depois elimine toda alternativa que viole uma delas.

✓ Classifique o problema antes de olhar as alternativas: plano de controle ou de dados, entrada ou saída, camada 4 ou 7, backup ou DR, Entra ou RBAC.

✓ Quando o enunciado traz um código de erro, use-o como pista direta: RequestDisallowedByPolicy, ScopeLocked, AuthorizationFailed, MissingSubscriptionRegistration ou limite de vCPUs.

✓ Em Escolha DUAS, julgue cada alternativa como verdadeira ou falsa isoladamente; não procure duas que combinem entre si.

✓ Distribua a revisão pelos pesos: identidade e governança e computação (20-25% cada), armazenamento e redes (15-20% cada) e monitoramento (10-15%).

✓ Desconfie de alternativas que exigem recriar, excluir ou copiar tudo quando existe recurso nativo para o caso (conversão de redundância, reimplantar, exclusão temporária); e o contrário quando a propriedade é imutável (conjunto de disponibilidade, VNet da VM).

✓ Para diagnóstico, associe a pergunta à ferramenta: qual regra, qual rota, onde falha, quem fez, a plataforma caiu, o recurso caiu.

Erros que derrubam candidatos

✗ Escolher a função do Azure RBAC para tarefas do Entra (criar usuários, redefinir senhas) ou o contrário.

✗ Confundir ponto de extremidade de serviço com ponto de extremidade privado e esquecer a zona DNS privatelink.

✗ Achar que GRS, failover ou bloqueios de recurso recuperam dados apagados ou corrompidos.

✗ Tratar conjunto de disponibilidade como proteção contra perda de datacenter.

✗ Supor que marcas são herdadas, que NotActions nega e que orçamento bloqueia gastos.

✗ Usar ferramentas legadas ou erradas: agente MMA, log de atividades para operações de dados, agente MARS para VMs do Azure.

✗ Ignorar a regra do NSG: menor número vence e sub-rede e NIC precisam permitir.

Na semana da prova

- ☐ Refaça as provas práticas e, em cada erro, anote a restrição do enunciado que você deixou passar.
- ☐ Revise as tabelas de números: endereços reservados por sub-rede, prazos de Cool, Cold e Archive, 93 e 90 dias do Monitor, 30 dias de usuário excluído, 14 dias de exclusão temporária do backup, SLAs de VM.
- ☐ Revise os pares que a prova confunde: Load Balancer x Application Gateway x Traffic Manager, Backup x Site Recovery, CanNotDelete x ReadOnly, Deny x Modify x Audit, ACI x Container Apps.
- ☐ Leia os checklists de cada domínio e estude de novo só os itens que você não consegue afirmar com segurança.
- ☐ Na véspera, revise apenas os quadros de lembrar e os macetes; descanse e chegue com folga de tempo.

REVISÃO FINAL

Folha de cola

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

1. Gerenciar identidades e governança do Azure

‣ Erro RequestDisallowedByPolicy → **Atribuição do Azure Policy com efeito Deny**

‣ Erro ScopeLocked ou AuthorizationFailed → **ScopeLocked = bloqueio; AuthorizationFailed = falta de RBAC**

‣ Erro MissingSubscriptionRegistration → **Registrar o provedor de recursos na assinatura**

‣ Ver o impacto de uma política sem bloquear nem mudar a definição → **enforcementMode DoNotEnforce**

‣ Liberar só um grupo da política, por três meses → **Isenção de política com data de expiração**

⚠ Gerenciar usuários é função do Entra, como Administrador de Usuários; funções do RBAC tratam recursos.

⚠ RBAC é aditivo: as permissões se somam e o escopo amplo não restringe o específico.

⚠ NotActions apenas subtrai do conjunto daquela função; outra atribuição pode conceder a ação.

2. Implantar e gerenciar recursos de computação

‣ Adicionar VMs com CPU acima de um limite e remover abaixo de outro → **Conjunto de dimensionamento com escala automática**

‣ Continuar atendendo se um datacenter inteiro cair → **Zonas de disponibilidade (VMSS com zonas 1, 2 e 3)**

‣ Latência de rede mínima entre camadas → **Grupo de posicionamento por proximidade**

‣ Servidores físicos sem VMs de outros clientes → **Host Dedicado do Azure**

‣ Carga interrompível, menor custo de computação → **VMs Spot**

⚠ Conjunto fica num só datacenter e grupo de posicionamento aproxima as VMs; use zonas de disponibilidade.

⚠ As duas coisas são definidas na criação: recrie a VM usando os discos existentes.

⚠ Mover entre grupos não muda a região; use o Azure Resource Mover.

3. Implementar e gerenciar armazenamento

‣ Recuperar blob apagado em até X dias, sem restaurar backup → **Exclusão temporária de blobs**

‣ Voltar contêineres ao estado de horas atrás após corrupção → **Restauração pontual para blobs de blocos**

‣ Inalterado até segunda ordem, sem prazo → **Retenção legal**

‣ Sete anos sem alterar ou excluir, nem pelo administrador → **Política de imutabilidade por tempo**

‣ Ler a cópia secundária a qualquer momento, sem failover → **Prefixo RA (RA-GRS ou RA-GZRS)**

⚠ A exclusão é replicada para a secundária; quem desfaz exclusão é a exclusão temporária.

⚠ Bloqueios de recurso atuam no plano de controle e não protegem dados dos blobs; use exclusão temporária ou imutabilidade.

⚠ Ela vai até 365 dias e não impede alterações; WORM regulatório é política de imutabilidade por tempo.

4. Implementar e gerenciar redes virtuais

‣ Aceitar tráfego só de uma sub-rede, pelo backbone, sem IP privado e sem pagar → **Ponto de extremidade de serviço**

‣ IP privado da própria VNet para o PaaS, acesso público desabilitado → **Ponto de extremidade privado + zona DNS privatelink**

‣ Limitar a saída a contas de armazenamento específicas, evitar exfiltração → **Política de ponto de extremidade de serviço**

‣ Domínio raiz apontando para IP público do Azure → **Registro de alias**

‣ /imagens/* para um pool e /api/* para outro, com TLS → **Application Gateway com regras baseadas em caminho**

⚠ No NSG vale o menor número e a avaliação para na primeira correspondência; especificidade, tipo de ação e ordem de criação não importam.

⚠ NSGs não herdam regras; na entrada os dois são avaliados e os dois precisam permitir, senão o DenyAllInBound da NIC bloqueia.

⚠ CNAME não é permitido no raiz; use registro de alias, que também acompanha a troca do IP.

5. Monitorar e manter recursos do Azure

‣ Quem excluiu a VM ontem → **Log de atividades**

‣ Avisar toda vez que alguém excluir uma VM → **Alerta do log de atividades**

‣ Mais de N erros em X minutos num log de aplicativo → **Alerta de pesquisa de logs**

‣ Alertas gerados mas sem notificações durante a manutenção → **Regra de processamento de alertas (suprimir)**

‣ Falha da própria plataforma Azure nos serviços da região → **Alerta de integridade do serviço (Service Health)**

⚠ O MMA foi desativado em 2024; use o Azure Monitor Agent com regra de coleta de dados.

⚠ O log de atividades é plano de controle; habilite configuração de diagnóstico com os logs AuditEvent.

⚠ São 93 dias; para mais, envie a um workspace.

GABARITO

Respostas do diagnóstico

D1. B) Recurso Verificar acesso, no IAM → revise o capítulo 1

Por quê: Em Controle de acesso (IAM), Verificar acesso lista as funções atribuídas a um usuário, grupo ou identidade, com o escopo de origem de cada uma.

✗ A) Incorreta. O log mostra operações feitas, não as permissões vigentes.
✗ C) Incorreta. A conformidade mostra políticas, não funções.
✗ D) Incorreta. O Advisor não lista atribuições de função.

> **Dica de prova:** Quem tem acesso e de onde vem: Verificar acesso no IAM.

D2. A) Política com efeito Modify que herda a marca do grupo → revise o capítulo 1

Por quê: O efeito Modify altera propriedades como marcas durante a criação ou atualização. Para recursos já existentes, usa-se uma tarefa de correção.

✗ B) Incorreta. Bloqueios não tratam marcas.
✗ C) Incorreta. A função dá permissão, mas não aplica a marca automaticamente.
✗ D) Incorreta. Audit mostra a não conformidade, mas não adiciona a marca.

> **Dica de prova:** Adicionar ou herdar marcas automaticamente: Azure Policy com Modify.

D3. C) Onde ficam os metadados do grupo → revise o capítulo 1

Por quê: Se a região do grupo ficar indisponível, não é possível atualizar os recursos pelo plano de controle, embora eles continuem funcionando.

✗ A) Incorreta. O grupo não define regiões de backup.
✗ B) Incorreta. A região do grupo não afeta a cobrança.
✗ D) Incorreta. Os recursos podem ficar em outras regiões.

> **Dica de prova:** Região do grupo: onde ficam os metadados.

D4. C) Job com gatilho agendado → revise o capítulo 2

Por quê: Jobs do Container Apps têm gatilhos manuais, agendados (cron) ou por eventos.

✗ A) Incorreta. Container Apps não usa slots.
✗ B) Incorreta. Revisões são para aplicativos contínuos.
✗ D) Incorreta. Always reinicia o contêiner sem parar.

> **Dica de prova:** Tarefa agendada no Container Apps: job com agenda.

D5. D) Recurso Executar comando da VM → revise o capítulo 2

Por quê: O Executar comando (Run Command) usa o agente de VM para executar scripts PowerShell ou shell, útil para diagnóstico e correções.

✗ A) Incorreta. O Advisor não executa comandos.
✗ B) Incorreta. Ela protege a VM, sem executar comandos.
✗ C) Incorreta. Ele mostra o boot, sem executar comandos.

> **Dica de prova:** Comando pontual sem RDP: Executar comando.

D6. C) Recriar a VM na nova VNet com os discos → revise o capítulo 2

Por quê: Uma NIC fica vinculada à VNet. Para mudar de VNet, recria-se a VM com os discos existentes e uma NIC na nova rede.

✗ A) Incorreta. O grupo não define a VNet.
✗ B) Incorreta. O emparelhamento não move interfaces.
✗ D) Incorreta. A NIC só muda de sub-rede dentro da mesma VNet.

> **Dica de prova:** Trocar a VM de VNet: recriar com os mesmos discos.

D7. A) Replicação de objetos entre as contas → revise o capítulo 3

Por quê: A replicação de objetos permite escolher contêineres e filtros, e o destino é uma conta independente, com camada e redundância próprias.

✗ B) Incorreta. Ela guarda exclusões, não copia dados.
✗ C) Incorreta. O ciclo de vida muda camadas e exclui.
✗ D) Incorreta. A secundária do GRS não é uma conta própria para processamento.

> **Dica de prova:** Cópia para outra conta legível: replicação de objetos.

D8. C) Conta premium do tipo FileStorage → revise o capítulo 3

Por quê: Os tipos de conta premium são BlockBlobStorage, FileStorage e blobs de página. A conta Standard de uso geral v2 atende a maioria dos cenários em HDD.

✗ A) Incorreta. A redundância não muda o tipo de mídia.
✗ B) Incorreta. BlockBlobStorage é para blobs de blocos premium.
✗ D) Incorreta. Contas Standard usam HDD para o Azure Files.

> **Dica de prova:** Azure Files em SSD: conta FileStorage premium.

D9. C) Usar a chave secundária e regenerar a primária → revise o capítulo 3

Por quê: O recomendado é guardar as chaves no Key Vault e rotacionar periodicamente. Melhor ainda é usar autenticação do Entra e evitar chaves.

✗ A) Incorreta. Mudar de conta é desnecessário para rotacionar chaves.
✗ B) Incorreta. A redundância não afeta as chaves.
✗ D) Incorreta. Isso interrompe todos os aplicativos até a atualização.

> **Dica de prova:** Rotação sem parada: usar a outra chave enquanto regenera uma.

D10. B) Permitir tráfego encaminhado → revise o capítulo 4

Por quê: Com uma NVA no hub, os emparelhamentos precisam permitir tráfego encaminhado, e a NIC da NVA precisa ter o encaminhamento de IP habilitado.

✗ A) Incorreta. Isso é para usar o gateway de VPN do hub.
✗ C) Incorreta. Ele é para serviços PaaS.
✗ D) Incorreta. DNS não afeta o encaminhamento de pacotes.

> **Dica de prova:** NVA no hub: permitir tráfego encaminhado.

D11. B) É negado, pois a regra 100 é avaliada antes da 200 → revise o capítulo 4

Por quê: O NSG processa as regras da menor para a maior prioridade numérica. Quando o tráfego corresponde a uma regra, a avaliação termina.

✗ A) Incorreta. A especificidade da origem não muda a ordem de avaliação.
✗ C) Incorreta. Não há precedência de permissão sobre negação no NSG.
✗ D) Incorreta. A ordem de criação não importa, só a prioridade.

> **Dica de prova:** NSG: número menor vence e a avaliação para na primeira correspondência.

D12. A) Persistência de sessão por IP do cliente → revise o capítulo 4

Por quê: O Load Balancer usa por padrão um hash de cinco tuplas. A persistência por IP do cliente, ou por IP e protocolo, mantém o cliente na mesma VM.

✗ B) Incorreta. A investigação só verifica se a VM responde.
✗ C) Incorreta. O NAT de entrada publica portas de VMs específicas.
✗ D) Incorreta. O tempo limite controla conexões ociosas.

> **Dica de prova:** Cliente sempre na mesma VM: persistência de sessão.

Agora, treine no formato real

Faça as 6 provas completas do curso AZ-104: 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.