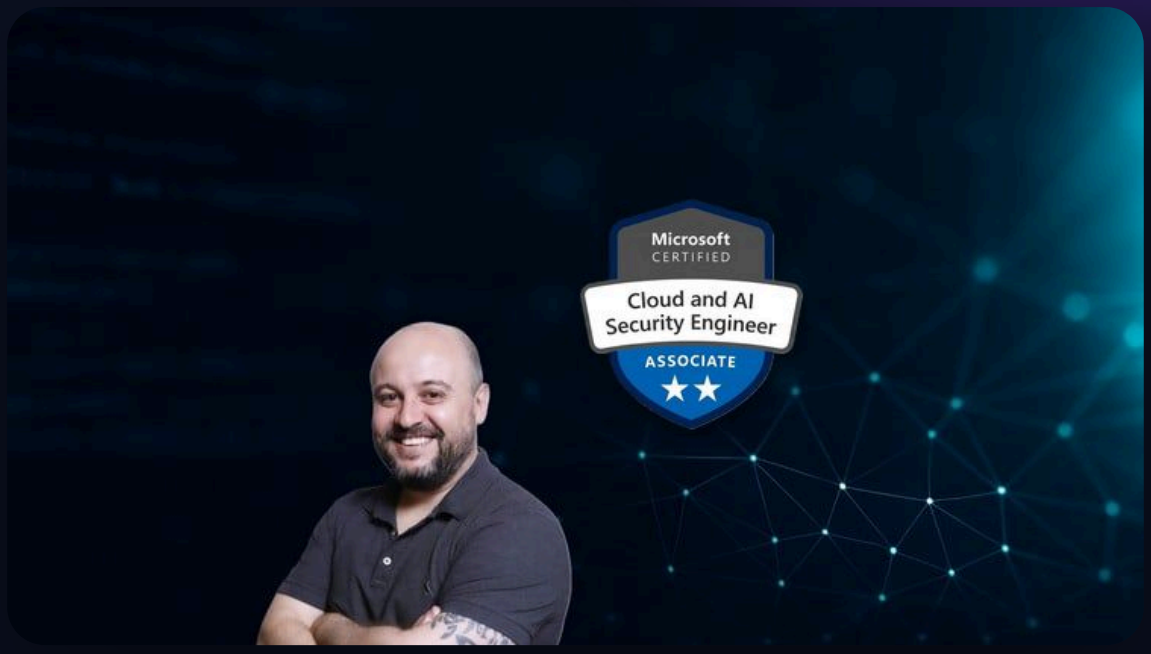


Guia de preparação SC-500

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

4 capítulos por domínio	**28** questões comentadas	**70%** nota de corte
6 provas completas no curso		

ANTES DE COMEÇAR

Como usar este guia

Este guia foi feito para ser estudado junto com as 6 provas completas do curso SC-500: 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 120 minutos, no formato do exame. Referência de aprovação: 70%.

Domínio (capítulo)	Peso	Neste guia
1. Gerenciar e monitorar a postura de segurança	20-25%	18 conceitos · 14 pegadinhas
2. Gerenciar identidade, acesso e governança	20-25%	18 conceitos · 14 pegadinhas
3. Proteger a computação	20-25%	18 conceitos · 14 pegadinhas
4. Proteger armazenamento, bancos de dados e redes	25-30%	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 e monitorar a postura de segurança

A equipe de segurança de uma operadora quer avaliar os plug-ins pré-instalados da Microsoft no Security Copilot antes de liberá-los a todos. Até lá, só os owners devem poder usá-los, inclusive nas experiências incorporadas aos portais. O que fazer?

A. Um contribuidor desativa os plug-ins na própria sessão e orienta os demais usuários
B. Um owner define, nas configurações de plug-ins, a disponibilidade dos pré-instalados como só para owners
C. Um administrador remove a função de contribuidor da capacidade de SCU no Azure
D. Um administrador do Entra atribui a função Security Reader somente aos usuários autorizados a usar os plug-ins

D2 · Gerenciar e monitorar a postura de segurança

A Andes Mineração tem operações no Brasil e na Alemanha, e a regulamentação exige que os logs de segurança de cada país fiquem armazenados na região correspondente. A empresa vai implantar o Microsoft Sentinel. Qual desenho atende?

A. Workspace único na Alemanha com RBAC de contexto de recurso aplicado aos analistas do Brasil
B. Workspace único no Brasil com retenção diferente por tabela para os dados vindos das filiais alemãs
C. Workspace por equipe de analistas do SOC, criado na região mais barata, sem considerar os dados
D. Workspaces separados em cada região exigida, já que o workspace fica ligado à região onde foi criado

D3 · Gerenciar e monitorar a postura de segurança

O comitê de riscos de uma seguradora quer acompanhar, mês a mês, a evolução da conformidade das assinaturas com o PCI DSS e a ISO 27001 avaliadas pelo Defender for Cloud, com detalhamento até a recomendação e exportação dos painéis para Excel. Qual recurso usar?

A. A pasta de trabalho Compliance Over Time da galeria do Defender for Cloud
B. O relatório de conformidade do Azure Policy em cada assinatura
C. A pasta de trabalho Secure Score Over Time da galeria do Defender for Cloud
D. Os relatórios de auditoria da Microsoft no painel de conformidade

D4 · Gerenciar identidade, acesso e governança

Na Agropecuária Cerrado Verde, os novos colaboradores devem começar sem senha e registrar uma passkey no Microsoft Authenticator logo no primeiro dia. A identidade do colaborador é conferida presencialmente pelo suporte, que entrega a credencial inicial. Qual credencial emitir e qual função administrativa pode emiti-la para um usuário comum?

A. Temporary Access Pass, emitido por um Administrador de Usuários do locatário
B. Temporary Access Pass, emitido por um Administrador de Autenticação
C. Senha temporária com troca obrigatória no primeiro acesso ao portal
D. Senha de aplicativo (app password) gerada no portal pelo time de suporte

D5 · Gerenciar identidade, acesso e governança

A software house Nimbus registrou no próprio locatário um aplicativo multilocatário de gestão de frotas. Três clientes já o usam após consentir. Um cliente pergunta onde o aplicativo aparece no locatário dele e o que foi criado ali no momento do consentimento. Qual resposta está correta?

A. Nada é criado no locatário do cliente, pois o token é emitido pelo locatário de origem da Nimbus
B. Uma identidade gerenciada atribuída pelo usuário, criada para representar o aplicativo no locatário
C. Uma cópia do objeto de aplicativo, exibida em Registros de aplicativo, com os mesmos segredos do cliente
D. Uma entidade de serviço, em Aplicativos empresariais; o objeto de aplicativo fica no locatário da Nimbus

D6 · Gerenciar identidade, acesso e governança

O auditor da Fintech Capital pediu duas evidências: o status atual da assinatura de produção frente ao PCI DSS e os relatórios de certificação da própria Microsoft (como SOC e ISO) para a nuvem do Azure. Onde o engenheiro obtém ambos no Defender for Cloud?

A. Na exportação contínua para o Log Analytics e em consultas KQL salvas como pastas de trabalho
B. Na exportação da pontuação segura pela API REST e no relatório de recomendações do Azure Advisor
C. Na opção Baixar relatório do painel de conformidade regulatória e na guia Relatórios de auditoria
D. No relatório de conformidade do Azure Policy e em um chamado de suporte pedindo os certificados

D7 · Proteger a computação

Uma rede de farmácias vai criar novas VMs Linux e precisa que discos temporários e caches de disco também fiquem criptografados, sem consumir CPU da VM com dm-crypt. A solução usada até agora, o Azure Disk Encryption, tem aposentadoria marcada para 15 de setembro de 2028. O que habilitar nas novas VMs?

A. Criptografia no host (encryption at host)
B. Azure Disk Encryption com dm-crypt e chave no Key Vault
C. Criptografia de disco confidencial em VM do tipo padrão
D. A criptografia padrão do lado do servidor (SSE)

D8 · Proteger a computação

A API de cotação da seguradora Atlas, publicada no API Management no nível Standard v2, precisa limitar cada assinante a 20 chamadas a cada 60 segundos para conter picos e bloquear um intervalo de IPs abusivo. Quais políticas usar?

A. quota-by-key com período de 60 segundos e ip-filter com action allow
B. rate-limit-by-key por assinatura e ip-filter com action forbid
C. quota-by-key com período de 60 segundos e validate-azure-ad-token
D. validate-jwt com claim de IP e rate-limit-by-key pelo IP do gateway

D9 · Proteger a computação

O cluster AKS de uma healthtech usa integração gerenciada com o Microsoft Entra. A segurança quer que as permissões no Kubernetes sejam dadas por atribuições de função do Azure, com escopo por namespace, e que ninguém consiga obter credenciais estáticas de administrador do cluster. O que configurar?

A. Habilitar o Azure RBAC para autorização do Kubernetes e desabilitar as contas locais
B. Habilitar intervalos de IP autorizados no servidor de API do cluster
C. Habilitar o Azure RBAC e entregar get-credentials --admin aos administradores
D. Criar RoleBindings do Kubernetes por usuário e manter as contas locais ativas

D10 · Proteger armazenamento, bancos de dados e redes

O DBA da Rede Escolar Saber revisou os achados da avaliação de vulnerabilidades do Defender for Azure SQL, em configuração expressa. Algumas permissões apontadas são intencionais. Ele quer que essas regras apareçam como aprovadas nas próximas verificações, a menos que algo mude. O que fazer?

A. Isentar o banco de dados inteiro da recomendação de vulnerabilidades do Defender for Cloud
B. Definir esses resultados como linha de base, que na configuração expressa vale na hora
C. Voltar para a configuração clássica, que oculta automaticamente os achados repetidos
D. Remover as regras correspondentes da iniciativa do Azure Policy atribuída ao servidor

D11 · Proteger armazenamento, bancos de dados e redes

Os Laticínios Serra Gaúcha restringiram uma conta de armazenamento a redes selecionadas. Um workspace específico do Azure Synapse, que não está em nenhuma VNet permitida, precisa ler os dados com a própria identidade gerenciada, e nenhum outro workspace do locatário deve ganhar acesso de rede à conta. O que configurar?

A. A exceção Permitir serviços confiáveis da Microsoft no firewall, mais uma função de dados no contêiner
B. Uma regra de instância de recurso para esse workspace, mais uma função de dados para a identidade dele
C. Uma regra de IP com a marca de serviço do Synapse no firewall da conta de armazenamento de destino
D. Uma política de acesso armazenada no contêiner que restrinja o acesso ao identificador do workspace

D12 · Proteger armazenamento, bancos de dados e redes

A Corretora Horizonte Azul quer impedir que um servidor lógico do Azure SQL Database envie dados (por auditoria, importação e exportação ou OPENROWSET) para contas de armazenamento que não sejam as da própria empresa. O que configurar?

A. Restringir a rede de saída do servidor e listar os FQDNs das contas de armazenamento permitidas
B. Negar o acesso à rede pública do servidor e criar um ponto de extremidade privado na VNet
C. Habilitar a autenticação somente Microsoft Entra no servidor lógico e remover os logins SQL
D. Criar regras de firewall de entrada no nível do servidor com os IPs públicos das redes da empresa e dos parceiros

01

CAPÍTULO 1 · 20-25% DA PROVA

Gerenciar e monitorar a postura de segurança

Neste domínio eu preciso dominar o Defender for Cloud como ferramenta de postura (Foundational x Defender CSPM, caminhos de ataque, explorador, conformidade, conectores AWS e GCP, MDVM e EASM), o Microsoft Sentinel no portal do Defender (workspaces, funções, hub de conteúdo, conectores, Syslog/CEF, eventos do Windows, tabelas personalizadas, automação e retenção), a auditoria do Purview no Defender XDR e o Microsoft Security Copilot (workspaces, funções, plug-ins, SCUs e agentes). As questões trocam o plano gratuito pelo pago, a tabela de destino errada ou a função do Sentinel com privilégio demais. Também caem muitos detalhes de coleta: qual conector, qual conjunto de eventos e qual tabela recebe os dados. Onde mais erro é em retenção e custo (planos de tabela, data lake, camadas de compromisso) e nas funções de quem pode fazer o quê no Sentinel e no Copilot.

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

Tópicos-chave

Foundational CSPM x Defender CSPM

O gratuito traz inventário, exportação de dados, workbooks, MCSB, secure score, recomendações, correção e automação de fluxo de trabalho. O Defender CSPM acrescenta caminhos de ataque, explorador de segurança na nuvem, governança, conformidade além do MCSB, nível de risco por recomendação, DSPM, postura de IA (AI BOM) e recomendações personalizadas em KQL. Em AWS e GCP, o Defender CSPM é cobrado por recurso faturável.

Análise de caminho de ataque e explorador

Caminhos de ataque mostram rotas de pontos de entrada até alvos críticos, ordenados por risco, e exigem Defender CSPM com varredura sem agente; um caminho resolvido pode levar até 24 horas para sair. O explorador de segurança na nuvem faz consultas em grafo combinando exposição, vulnerabilidades, identidades e permissões. O componente Sensitive data discovery leva dados confidenciais ao contexto.

Conformidade regulatória no Defender for Cloud

O MCSB vem por padrão; outros padrões (PCI DSS, ISO 27001, CIS AWS) exigem plano pago e Owner ou Policy Contributor. Baixar relatório dá o status do padrão e Relatórios de auditoria trazem as certificações da Microsoft. Controles de processo são atestados manualmente com evidência; a pasta de trabalho Compliance Over Time mostra a evolução e exporta para Excel; padrão personalizado agrupa recomendações escolhidas.

Conectores AWS e GCP

AWS: conta única ou conta de gerenciamento (que cobre contas-membro atuais e futuras), com template CloudFormation (StackSet) ou Terraform criando funções IAM com confiança federada; sem chaves de acesso. GCP: escopo de organização ou projeto, com projetos excluídos e script gcloud; usa federação de identidade de carga de trabalho, sem chave JSON. Padrões para AWS são atribuídos no escopo AWS, idealmente na conta de gerenciamento.

Planos de proteção sem agente

Defender for Resource Manager detecta operações de gerenciamento suspeitas (IP malicioso, MicroBurst, extensões em VMs). Defender for App Service alerta sobre DNS pendente quando o site é desativado, mas não varre o histórico do registrador. O conector DevOps do GitHub exige Organization Owner no GitHub e Contributor na assinatura.

Defender Vulnerability Management em servidores

Vem ativado por padrão no Defender for Servers, configurável em Vulnerability assessment for machines > Edit configuration. Plano 1 traz o básico; Plano 2 traz as funcionalidades premium (linhas de base CIS, certificados, extensões de navegador, compartilhamentos, bloqueio de apps vulneráveis). Exceção a uma CVE se faz com isenção com condição por CVE e data de expiração; regras de desabilitação estão sendo descontinuadas.

Defender EASM

A descoberta parte de sementes externas (domínios, blocos de IP públicos, hosts, ASNs); ativos chegam como Candidatos e, aprovados, vão para Approved Inventory, verificado diariamente. A cobrança considera só domínios, IPs e host:IP em Approved Inventory. Prioridade de exposição: painel Resumo da superfície de ataque, severidade alta.

Workspaces do Sentinel e portal do Defender

Comece com um workspace e crie outros só por motivo como residência de dados. No portal do Defender há um workspace primário (recebe o conector do Defender XDR e os incidentes unificados) e vários secundários; o Sentinel no portal do Azure tem suporte só até 31/03/2027. RBAC de contexto de recurso dá a equipes acesso só aos logs dos próprios recursos; MSSP consulta workspace secundário de outro locatário com Azure Lighthouse e workspace().

Funções no Sentinel

Microsoft Sentinel Reader vê; Responder também gerencia incidentes; Contributor também cria regras, conectores e instala soluções do hub. Logic App Contributor cria e edita playbooks; Microsoft Sentinel Automation Contributor é dado à conta do Sentinel no grupo do playbook para regras de automação o executarem. Identidade do playbook que altera incidentes precisa de Responder.

Hub de conteúdo

Soluções empacotam conectores, modelos de regras, pastas de trabalho e playbooks; instalar não cria regras ativas, é preciso criar a partir dos modelos. Atualizar a solução não mexe nas regras já criadas, que mostram a marca Update para comparar. Itens standalone atualizam sozinhos; suporte Microsoft vai ao Suporte do Azure, Partner ao parceiro e Community por issue no GitHub.

Conectores de dados do Azure e da Microsoft

Azure Activity em várias assinaturas usa a atribuição do Azure Policy com tarefa de correção. O conector do Entra ID traz auditoria com qualquer licença, mas logs de entrada exigem P1 ou P2. O conector Tenant-based Microsoft Defender for Cloud coleta alertas do locatário inteiro. No portal do Defender o conector Defender XDR é ligado sozinho e os conectores individuais são desconectados; alertas e incidentes não têm custo, eventos brutos de caça avançada são cobrados.

Syslog e CEF via AMA

Encaminhador Linux com rsyslog ou syslog-ng escutando na porta 514 e o Azure Monitor Agent (máquina fora do Azure precisa do Arc). A DCR define facilidades e nível mínimo (que inclui os níveis mais severos). CEF vai para CommonSecurityLog; usar a mesma facilidade para Syslog e CEF duplica dados.

Eventos de segurança do Windows

Windows Security Events via AMA grava em SecurityEvent com conjuntos All (Security e AppLocker, sem System), Common (trilha completa com menos volume), Minimal (sem logoff 4634) ou Custom XPath (Log!*[System[(EventID=...)]], até 20 expressões, sem contains). Eventos via WEF com o conector Windows Forwarded Events vão para WindowsEvent, e regras que consultam SecurityEvent não disparam.

Tabelas personalizadas e transformações

Logs de texto via AMA exigem a tabela _CL criada antes, com TimeGenerated e RawData. A Logs Ingestion API usa token do Entra, uma DCR com o fluxo Custom-<tabela>_CL e a função Monitoring Metrics Publisher na DCR; a HTTP Data Collector API com chave é o método legado. Transformações KQL na DCR filtram linhas e colunas antes da ingestão, reduzindo custo.

Regras de automação

Rodam em sequência pelo número de ordem dentro de cada gatilho, e as de criação de incidente antes das de atualização; cada regra vê as mudanças das anteriores. Têm data de expiração, ideal para fechar incidentes de um teste de intrusão. Playbooks com gatilho de entidade não podem ser chamados por regras de automação.

Retenção e custo no Sentinel

Retenção de análise até 2 anos (regras e caça) e retenção total até 12 anos no data lake, mais barato; dados só no data lake não alimentam regras. Planos de tabela: Analytics (alto valor), Basic (investigação, consultas cobradas, alertas simples) e Auxiliary (baixo uso, sem alertas). Trabalho de pesquisa grava em _SRCH (uma tabela por vez); restauração cria _RST com cobrança mínima de 2 TB e 12 horas. Camadas de compromisso vão de 100 a 50.000 GB/dia, com 31 dias para reduzir.

Auditoria do Purview no Defender XDR

A página Audit do portal do Defender é a mesma pesquisa do Purview: exige auditoria ativada e as funções Audit Logs ou View-Only Audit Logs. Interações do Copilot ficam no tipo CopilotInteraction, com AccessedResources listando os arquivos usados. Retenção: 180 dias no Audit (Standard), 1 ano no Premium e até 10 anos com política e complemento.

Microsoft Security Copilot

Funções Copilot owner (configura) e Copilot contributor (usa); Security Administrator e Global Administrator herdam owner, e grupos precisam ser atribuíveis a funções. O acesso a dados é em nome do usuário, então ele precisa das funções de cada serviço. SCUs provisionadas são por hora, sem acúmulo; excedente é cobrado pelo uso com uma casa decimal até o limite. Associar capacidade exige Owner ou Contributor do Azure no recurso; o local de armazenamento é fixado na criação do workspace.

Macetes para memorizar

💡 Funções do Sentinel

Reader olha, Responder trata incidente, Contributor constrói regra. Playbook é Logic App; quem dispara é o Automation Contributor.

💡 Tabelas de eventos

SecurityEvent = AMA direto. WindowsEvent = WEF. CommonSecurityLog = CEF. Syslog = Linux.

💡 Conjuntos de eventos

All é tudo do Security (sem System); Common é a trilha completa enxuta; Minimal só violação; Custom é XPath.

💡 Retenção

Análise corre 2 anos; lago guarda 12. Agulha = _SRCH; período a fundo = _RST (2 TB, 12 h).

💡 Security Copilot

Owner configura, Contributor usa, e o dado é sempre do bolso do usuário (on-behalf-of).

💡 CSPM grátis x pago

Grátis mostra o placar (score e recomendações); pago mostra o caminho do ataque, o risco e quem corrige até quando.

> **Suporte no hub de conteúdo**
>
> Microsoft = chamado no Azure; Partner = parceiro; Community = GitHub.

Tabela de memorização: não confunda

Quando é...	...e quando é
Foundational CSPM Secure score, recomendações do MCSB, inventário, automação de fluxo de trabalho e exportação de dados sem custo.	**Defender CSPM** Caminhos de ataque, explorador, nível de risco, governança, padrões regulatórios além do MCSB, dados confidenciais e AI BOM.
Windows Security Events via AMA AMA nos próprios servidores (Arc se on-premises), gravando em SecurityEvent, compatível com as regras internas.	**Windows Forwarded Events** Eventos centralizados em coletor WEC, gravados em WindowsEvent; regras que consultam SecurityEvent precisam ser adaptadas.
Trabalho de pesquisa Achar uma agulha (ex.: um IP) em meses de dados antigos de uma tabela; resultado em _SRCH.	**Restauração** Analisar a fundo um período com KQL completo e repetido; tabela _RST com mínimo de 2 TB e 12 horas, não suporta Auxiliary.
Plano de tabela Basic Dados de investigação com ingestão mais barata, consultas otimizadas e alertas simples.	**Plano de tabela Auxiliary** Dados de baixo uso, como auditoria, com a menor ingestão, consultas mais lentas e sem alertas.
Microsoft Sentinel Responder Ver dados e atribuir, comentar e fechar incidentes (nível 1 ou identidade de playbook que atualiza incidentes).	**Microsoft Sentinel Contributor** Criar e manter regras de análise, conectores e soluções do hub de conteúdo.
Copilot owner Alterar capacidade de SCUs, compartilhamento de dados e disponibilidade de plug-ins.	**Copilot contributor** Usar prompts e promptbooks, com acesso a dados conforme as funções do usuário em cada serviço.
Retenção de análise Dados disponíveis para regras de análise e caça, até 2 anos.	**Retenção total (data lake)** Guarda longa e barata até 12 anos, consultada por jobs KQL ou Spark, sem alimentar regras.

Números que caem

Item	Valor
Peso do domínio no exame	**20-25%**
Retenção de análise no Sentinel	**até 2 anos**
Retenção total no Sentinel	**até 12 anos**

Camadas de compromisso	**100 a 50.000 GB por dia, 31 dias para reduzir**
Cobrança mínima da restauração	**2 TB e 12 horas**
Expressões XPath por DCR	**até 20**
Porta de escuta do encaminhador Syslog/CEF	**514**
Suporte do Sentinel no portal do Azure	**até 31/03/2027**
Retenção da auditoria do Purview	**180 dias (Standard), 1 ano (Premium), até 10 anos com complemento**
Saída de um caminho de ataque resolvido	**até 24 horas**
Agente de otimização de acesso condicional	**roda a cada 24 horas (ou sob demanda), exige Entra ID P1 e consome SCUs**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Regras de governança e análise de caminho de ataque fazem parte do CSPM gratuito.
Como não cair: Governança, caminhos de ataque, explorador e nível de risco exigem Defender CSPM; o gratuito tem secure score, recomendações, automação e exportação.

⚠ **Alerta de prova:** Selecionar Enforce na recomendação do MCSB para impedir a criação de recursos fora do padrão.
Como não cair: Enforce usa DeployIfNotExists e corrige na criação; para barrar, defina o efeito Deny em Políticas de segurança.

⚠ **Alerta de prova:** Instalar a solução do hub de conteúdo já cria incidentes.
Como não cair: Soluções trazem modelos; é preciso criar as regras de análise a partir deles. Atualizar a solução também não altera regras existentes.

⚠ **Alerta de prova:** O conjunto All do Windows Security Events traz também o log System.
Como não cair: All cobre Security e AppLocker. System e Application vão por DCR de eventos do Windows do Azure Monitor, para outra tabela.

⚠ **Alerta de prova:** Eventos encaminhados por WEF caem em SecurityEvent e disparam as regras internas.
Como não cair: O conector Windows Forwarded Events grava em WindowsEvent; ajuste as regras ou use Windows Security Events via AMA.

⚠ **Alerta de prova:** Escolher LOG_ERR na DCR de Syslog coleta só esse nível.
Como não cair: O nível mínimo inclui os mais severos (LOG_CRIT, LOG_ALERT, LOG_EMERG).

⚠ **Alerta de prova:** Atribuir a política do conector Azure Activity alcança as assinaturas existentes.
Como não cair: Sem marcar a tarefa de correção, só recursos novos ou alterados são configurados; a atribuição exige Owner no escopo.

⚠ **Alerta de prova:** Dar Logic App Contributor ao analista resolve a regra de automação que não executa o playbook.
Como não cair: Quem executa é o Sentinel; conceda Microsoft Sentinel Automation Contributor à conta do Sentinel no grupo de recursos do playbook.

⚠ **Alerta de prova:** Copilot contributor enxerga os dados do Sentinel por ter acesso ao Copilot.
Como não cair: O Copilot acessa dados em nome do usuário; sem função no Sentinel a resposta vem vazia.

⚠ **Alerta de prova:** SCU não usada numa hora fica de saldo e o excedente é arredondado para unidade inteira.
Como não cair: SCUs provisionadas renovam a cada hora sem acúmulo, e o excedente é cobrado pelo uso com uma casa decimal.

⚠ **Alerta de prova:** Restaurar tabela Auxiliary por algumas horas sem cobrança mínima.
Como não cair: Restauração suporta Analytics e Basic, exige pelo menos dois dias de dados e cobra no mínimo 2 TB e 12 horas.

⚠ **Alerta de prova:** Configurar a camada de análise com 7 anos de retenção para guardar logs de auditoria.
Como não cair: A retenção de análise vai até 2 anos; use retenção total (até 12 anos) no data lake.

⚠ **Alerta de prova:** Todo ativo descoberto pelo EASM é cobrado.
Como não cair: Só domínios, IPs e host:IP em Approved Inventory contam; Candidate e Dependency não.

⚠ **Alerta de prova:** Regras de desabilitação na recomendação de vulnerabilidades para aceitar uma CVE por seis meses.
Como não cair: Regras de desabilitação estão saindo e não expiram; use isenção com condição de CVE e data de expiração.

Como cai na prova

📝 **Como cai:** Recurso do Defender for Cloud não disponível ou embaçado.
Como resolver: Verifique se é recurso do Defender CSPM (caminhos de ataque, explorador, risco, governança, padrões além do MCSB) ou de outro plano, e as funções exigidas (Owner ou Policy Contributor para padrões, Security Admin para recomendação personalizada).

📝 **Como cai:** Dados chegam ao Sentinel, mas regras não disparam ou a tabela está errada.
Como resolver: Rastreie o caminho: conector usado, tabela de destino (SecurityEvent, WindowsEvent, CommonSecurityLog, Syslog, _CL) e o que a regra consulta. Depois confira se as regras foram criadas a partir dos modelos.

📝 **Como cai:** Função mínima para uma tarefa no Sentinel ou no Copilot.
Como resolver: Separe gerenciar incidentes (Responder), criar regras e conteúdo (Contributor), playbooks (Logic App Contributor), executar playbook por regra (Automation Contributor), configurar o Copilot (owner) e usar (contributor mais funções de dados).

📝 **Como cai:** Requisito de retenção ou custo de logs.
Como resolver: Pergunte se o dado precisa alimentar regras (retenção de análise até 2 anos), se é para guarda longa (retenção total até 12 anos), se é investigação (Basic) ou baixo uso (Auxiliary) e se o corte deve ser antes da ingestão (transformação na DCR).

📝 **Como cai:** Conectar AWS ou GCP com cobertura de contas ou projetos futuros.
Como resolver: Use a conta de gerenciamento da AWS (CloudFormation StackSet com funções IAM federadas) ou o escopo Organização do GCP (projetos excluídos e script gcloud); descarte chaves de acesso, chave JSON e agente do Log Analytics.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
VM exposta + vulnerável + com permissão em Storage, consulta em grafo	**Explorador de segurança na nuvem (Defender CSPM)**
rota explorável até dados confidenciais para priorizar correção	**Análise de caminho de ataque (Defender CSPM + varredura sem agente)**
colunas de risco embaçadas nas recomendações	**Habilitar o Defender CSPM**
dados do Defender for Cloud para SIEM externo	**Exportação contínua para Event Hubs (streaming e snapshots semanais)**
dono e prazo automáticos para recomendações	**Regra de governança**

operações suspeitas pelo portal ou CLI, extensão em VM	**Defender for Resource Manager**
subdomain takeover em App Service desativado	**Defender for App Service**
firewall que só envia CEF por Syslog	**Encaminhador Linux + AMA + DCR do CEF via AMA (CommonSecurityLog)**
controladores de domínio on-premises com logon, logoff e Kerberos sem todo o volume	**Arc + Windows Security Events via AMA, conjunto Common**
enviar JSON de sistema próprio para tabela _CL	**Logs Ingestion API: DCR + Monitoring Metrics Publisher**
reduzir custo de ingestão cortando heartbeat e colunas	**Transformação KQL na DCR**
fechar incidentes de teste de intrusão por período definido	**Regra de automação com data de expiração**
quais arquivos o Copilot leu para um usuário	**Página Audit, CopilotInteraction, AccessedResources**
plug-in do Sentinel no Copilot responde do workspace errado	**Workspace padrão nas configurações do plug-in ou citar no prompt**

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

- Caminhos de ataque, explorador, nível de risco, governança e padrões além do MCSB exigem Defender CSPM.
- WEF cai em WindowsEvent; AMA direto cai em SecurityEvent; o conjunto All não traz o log System.
- Funções do Sentinel: Reader vê, Responder trata incidente, Contributor cria regra; Automation Contributor deixa a regra rodar playbook.
- Retenção de análise até 2 anos e retenção total até 12 anos; restauração cobra no mínimo 2 TB e 12 horas.
- No Security Copilot, owner configura, contributor usa, e o acesso a dados segue as funções do próprio usuário.

Essenciais para a prova (checklist)

☐ Sei listar o que o Foundational CSPM oferece e o que só o Defender CSPM habilita.

☐ Sei usar caminhos de ataque, explorador de segurança na nuvem, painel de conformidade e exportação contínua.

☐ Sei conectar AWS e GCP ao Defender for Cloud e atribuir padrões no escopo certo.

☐ Sei configurar o MDVM nos servidores e isentar uma CVE com prazo.

☐ Sei como o Defender EASM descobre ativos e o que é cobrado.

☐ Sei desenhar workspaces do Sentinel e integrá-los ao portal do Defender.

- ☐ Sei atribuir as funções do Sentinel e do Logic Apps para incidentes, regras e playbooks.
- ☐ Sei coletar Syslog, CEF, eventos de segurança do Windows e logs personalizados com AMA e DCR.
- ☐ Sei configurar retenção, planos de tabela, trabalhos de pesquisa e restauração.
- ☐ Sei configurar funções, plug-ins, SCUs e agentes do Security Copilot.

Questões de revisão do capítulo

R1.1 · Gerenciar e monitorar a postura de segurança

A Telecom Brasilis usa o Microsoft Defender External Attack Surface Management. O gerente de segurança quer saber quais ativos externos descobertos têm CVEs críticos e outras exposições de alta prioridade. Onde olhar primeiro?

A. Na lista de sementes de descoberta, conferindo os domínios cadastrados
B. No painel Conformidade com o GDPR, nos ativos com dados pessoais expostos
C. No painel Resumo da superfície de ataque, em severidade alta
D. No painel Alterações de inventário, nos ativos adicionados na semana

R1.2 · Gerenciar e monitorar a postura de segurança

No Microsoft Sentinel de um banco, a regra de automação A (ordem 2) atribui incidentes de phishing à equipe de e-mail, e a regra B (ordem 1) eleva para Alta a severidade de incidentes com a marca VIP. As duas usam o gatilho de criação de incidente. Chega um incidente de phishing com a marca VIP. O que acontece?

A. Só a regra B roda, porque cada incidente aciona uma única regra de automação
B. As duas rodam em paralelo e o resultado depende de qual termina por último
C. A regra B roda primeiro e a regra A já recebe o incidente com severidade Alta
D. A regra A roda primeiro, porque regras de atribuição têm precedência sobre as demais

R1.3 · Gerenciar e monitorar a postura de segurança

A fábrica de software Nimbus quer encontrar VMs expostas à internet que têm vulnerabilidades de alta severidade e uma identidade com permissão sobre contas de armazenamento, usando consultas baseadas em grafo e modelos de consulta prontos. Qual recurso usar?

A. O painel de conformidade com o padrão MCSB atribuído
B. O explorador de segurança na nuvem do Defender CSPM
C. A pasta de trabalho de pontuação segura do Defender
D. O Azure Resource Graph Explorer com consulta de inventário

R1.4 · Gerenciar e monitorar a postura de segurança

Um analista instalou pelo hub de conteúdo a solução do Microsoft Sentinel para um firewall de terceiros e configurou o conector. Uma semana depois, os logs chegam normalmente, mas nenhum incidente foi criado. O que falta fazer?

A. Criar regras de análise a partir dos modelos de regra instalados pela solução
B. Aguardar a ativação automática das regras, feita 14 dias após a instalação
C. Atualizar a solução, porque as regras só ficam ativas na versão mais recente
D. Reinstalar a solução usando a função Microsoft Sentinel Responder no workspace

Respostas comentadas

R1.1. C) No painel Resumo da superfície de ataque, em severidade alta

Por quê: O Defender EASM oferece painéis como Resumo da superfície de ataque, Postura de segurança, GDPR, OWASP Top 10, CWE Top 25 e CISA known exploits; os insights podem ser marcados como não aplicáveis.

✗ A) Incorreta. Sementes iniciam a descoberta; não mostram vulnerabilidades.
✗ B) Incorreta. O painel de GDPR foca riscos de privacidade, não priorização de CVEs.
✗ D) Incorreta. Alterações de inventário mostram o que mudou, não as exposições prioritárias.

> **Dica de prova:** Prioridade de exposição externa no EASM = insights de severidade alta no Resumo da superfície de ataque.

R1.2. C) A regra B roda primeiro e a regra A já recebe o incidente com severidade Alta

Por quê: Regras de automação são processadas pelo número de ordem dentro de cada gatilho; as de criação de incidente rodam antes das de atualização. Cada regra avalia o incidente já alterado pelas anteriores. Com o mesmo número de ordem, a sequência entre elas é aleatória.

✗ A) Incorreta. Todas as regras cujas condições correspondem são executadas, uma após a outra.
✗ B) Incorreta. Regras de automação nunca rodam em paralelo; a execução é sequencial.
✗ D) Incorreta. Não há precedência por tipo de ação; vale o número de ordem.

> **Dica de prova:** Regras de automação: sequenciais, pela ordem, e cada uma vê as mudanças das anteriores.

R1.3. B) O explorador de segurança na nuvem do Defender CSPM

Por quê: O explorador de segurança na nuvem faz consultas baseadas em grafo sobre o contexto de segurança (exposição à internet, vulnerabilidades, identidades e permissões) e requer o Defender CSPM.

✗ A) Incorreta. O painel de conformidade avalia controles de um padrão, não monta consultas contextuais.

✗ C) Incorreta. A pasta de trabalho mostra a evolução da pontuação segura, não relações entre exposição, vulnerabilidade e identidade.

✗ D) Incorreta. O Resource Graph consulta propriedades de recursos, mas não tem o contexto de segurança do grafo do Defender.

> **Dica de prova:** Pergunta contextual (exposta + vulnerável + com permissão) = explorador de segurança na nuvem do Defender CSPM.

R1.4. A) Criar regras de análise a partir dos modelos de regra instalados pela solução

Por quê: No hub de conteúdo, soluções empacotam conectores, modelos de regras de análise, pastas de trabalho e playbooks. Depois de instalar, o analista cria as regras a partir dos modelos (Gerenciar > modelo > Create rule). Instalar e gerenciar conteúdo exige Microsoft Sentinel Contributor no grupo de recursos.

✗ B) Incorreta. Não há ativação automática das regras de análise de uma solução.

✗ C) Incorreta. Atualizar a solução atualiza o conteúdo, mas também não cria regras ativas.

✗ D) Incorreta. Responder gerencia incidentes e não instala soluções; o hub de conteúdo exige Microsoft Sentinel Contributor.

> **Dica de prova:** Solução instalada não cria incidente sozinha: crie as regras a partir dos modelos.

02

CAPÍTULO 2 · 20-25% DA PROVA

Gerenciar identidade, acesso e governança

Aqui eu preciso dominar Microsoft Entra ID (PIM, acesso condicional, métodos de autenticação, identidades de aplicativos, consentimento OAuth e identidades gerenciadas), Azure Key Vault (rede, RBAC, chaves, segredos, certificados e Defender for Key Vault) e governança (Azure Policy, conformidade no Defender for Cloud, bloqueios, RBAC, funções personalizadas, Azure Backup e infraestrutura como código). A prova adora menor privilégio: a alternativa certa costuma ser a função mais estreita no escopo mais estreito que resolve o caso. Também cobra muito o que é plano de controle e o que é plano de dados, porque bloqueios, Contributor e log de atividades não alcançam dados. Meus erros mais comuns são achar que NotActions nega, que bloqueio protege blobs e que exp de segredo impede a leitura.

Neste capítulo

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

Tópicos-chave

Privileged Identity Management (PIM)

Atribuições qualificadas precisam ser ativadas; as regras de ativação (aprovação, justificativa, tíquete, MFA ou contexto de autenticação e duração de 1 a 24 horas) ficam nas configurações da função. Para recursos do Azure, as configurações valem por função e por recurso e não descem da assinatura para o grupo de recursos. PIM for Groups torna qualificada a associação a um grupo que concede vários acessos de uma vez.

Acesso condicional

Modo somente relatório mede impacto nos logs de entrada, e o What If simula considerando políticas ativadas ou em somente relatório (não as desativadas). Contas de acesso de emergência ficam fora das políticas de bloqueio. Local nomeado por país bloqueia geografias, mas só locais por intervalo de IP podem ser confiáveis. Risco de entrada e risco de usuário ficam em políticas separadas, e padrões de segurança não convivem com acesso condicional.

Avaliação contínua de acesso (CAE)

Permite que Exchange Online, SharePoint Online e Teams revoguem sessões quase em tempo real em eventos críticos, como conta desabilitada, mesmo com tokens de vida longa (até 28 horas). Frequência de entrada e tokens curtos ainda deixam janela.

Métodos de autenticação

Temporary Access Pass (10 minutos a 30 dias, um por usuário, emitido por Administrador de Autenticação ou de Autenticação Privilegiada) integra usuários direto em sem senha. A força resistente a phishing aceita só Windows Hello for Business ou credencial de plataforma, chave FIDO2 e CBA multifator. Campanha de registro convida ao Authenticator com adiamentos limitados; perfis de chave de acesso na política Passkey (FIDO2) definem atestado e tipo de chave por grupo.

Migração dos métodos legados

Desde 30/09/2025 as políticas legadas de MFA e SSPR não gerenciam métodos. Estados: Pre-migration (política de métodos só para entrada), Migration in Progress (entrada e SSPR, legadas ainda respeitadas, permite voltar atrás) e Migration Complete (só a política de métodos).

Objeto de aplicativo x entidade de serviço

O registro de aplicativo (objeto global) fica no locatário de origem; em cada locatário que consente é criada uma entidade de serviço em Aplicativos empresariais, onde ficam consentimentos e atribuições. Atribuição obrigatória = Sim restringe quem obtém token, e app roles atribuídas a grupos (Entra P1 ou P2) aparecem no claim roles.

Credenciais de aplicativos

Segredos de cliente valem no máximo 24 meses e a recomendação é menos de 12; prefira certificados ou credenciais federadas, e limite vida útil de senhas com política de gerenciamento de aplicativos. GitHub Actions sem segredo usa credencial de identidade federada (OIDC) com issuer, subject (ex.: Environment) e audience api://AzureADTokenExchange coincidindo exatamente.

Consentimento OAuth

Consentimento do usuário restrito a editores verificados e permissões delegadas classificadas como de baixo impacto. No fluxo de consentimento do administrador, revisor sem função adequada vê e nega, mas não aprova; permissões de aplicativo do Graph exigem Global Administrator. Em consent phishing, remova as concessões delegadas (oauth2PermissionGrants) e bloqueie a entrada no aplicativo empresarial; trocar senha não resolve.

Identidades gerenciadas

Atribuída pelo sistema nasce e morre com o recurso; atribuída pelo usuário é independente e pode servir várias instâncias recriadas. Para associar uma identidade existente a um recurso, Managed Identity Operator (assign/action); Managed Identity Contributor cria e exclui, mas não atribui. No código, informe o client ID (AZURE_CLIENT_ID) para usar a atribuída pelo usuário.

Azure RBAC e funções personalizadas

Owner atribui funções, Contributor gerencia sem atribuir, Reader só vê; permissões são aditivas. NotActions apenas subtrai e não é negação; atribuições de negação são criadas pelo Azure (deployment stacks com deny settings, aplicativos gerenciados). Funções personalizadas usam Actions (controle), DataActions (dados) e AssignableScopes (não aceita a raiz). Atribuição herdada só se remove no escopo de origem (Check access mostra).

Funções personalizadas do Microsoft Entra

Cobrem registros de aplicativo, aplicativos empresariais, consentimento, dispositivos, usuários e grupos, com escopo de locatário, unidade administrativa ou recurso específico. Para gerenciar só um registro de aplicativo, atribua a função personalizada no escopo desse registro.

Firewall do Key Vault

Redes selecionadas combinam regras de IPv4 públicos (até 1000), regras de rede virtual com ponto de extremidade de serviço (até 200) e a exceção de serviços confiáveis da Microsoft (Azure DevOps não está na lista). Com acesso público Desabilitado, regras de IP e de VNet deixam de valer, ficam só pontos de extremidade privados e serviços confiáveis.

Funções do Key Vault (modelo Azure RBAC)

Key Vault Secrets User lê valores de segredos (pode ter escopo no próprio segredo); Key Vault Reader lê só metadados; Secrets Officer gerencia segredos; Crypto Service Encryption User faz get, wrap e unwrap para CMK; Crypto Officer faz tudo com chaves; Key Vault Contributor é plano de controle. Com RBAC, políticas de acesso não são avaliadas; desde a versão de API 2026-02-01, RBAC é o padrão para cofres novos.

Proteção de objetos do Key Vault

Exclusão temporária vem ativa e não se desliga; a retenção vai de 7 a 90 dias (padrão 90) e só é definida na criação. Proteção contra limpeza é irreversível e impede purge durante a retenção; o nome fica reservado, então o caminho é recuperar. Para segredos, exp e nbf são informativos; bloquear leitura de fato é enabled = false.

Chaves, certificados e Managed HSM

Política de rotação gera novas versões automaticamente e o evento KeyNearExpiry no Event Grid avisa antes da expiração. Renovação automática de certificado exige CA integrada (DigiCert ou GlobalSign) ou autoassinado com ação autoRenew; emailContacts só avisa. Standard usa chaves de software, Premium chaves em HSM multilocatário, Managed HSM é locatário único FIPS 140-3 nível 3 com domínio de segurança do cliente.

Azure Policy

Deny bloqueia criação ou alteração e marca existentes como não conformes; Audit só registra; deployIfNotExists e modify têm identidade gerenciada e precisam de tarefa de correção para recursos já existentes. A definição salva numa assinatura só pode ser atribuída nela; para várias assinaturas, salve no grupo de gerenciamento. Isenções: Waiver (risco aceito) e Mitigated (controle compensatório), com expiração opcional; notScopes não registra motivo nem expira.

Bloqueios de recurso

CanNotDelete impede exclusão e ReadOnly impede qualquer alteração, inclusive POSTs como listar chaves e criar atribuições de função. São herdados e o mais restritivo prevalece, valem para todos (inclusive Owner) e só atuam no plano de controle, nunca em blobs. Criar e remover bloqueio exige Microsoft.Authorization/locks/*, presente em Owner e User Access Administrator.

Segurança do Azure Backup

Autorização multiusuário com Resource Guard (de preferência em outro locatário) exige aprovação de outra equipe para operações críticas. Cofre imutável Habilitado é reversível; Habilitado e bloqueado é irreversível. Exclusão temporária do backup retém de 14 a 180 dias. CMK no cofre dos Serviços de Recuperação precisa ser configurada antes de proteger qualquer item.

Macetes para memorizar

💡 Plano de controle x plano de dados

Bloqueio, Contributor, Owner e log de atividades mexem na casa; blob, segredo lido e AuditEvent estão dentro da casa.

💡 Funções do Key Vault

User usa, Officer administra, Reader só lê a etiqueta, Crypto Service Encryption User embrulha e desembrulha (wrap/unwrap).

💡 Efeitos do Azure Policy

Deny barra na porta; Audit anota; DINE e Modify consertam o novo, e o velho só com tarefa de correção.

💡 Isenções

Waiver = Aceitei o risco. Mitigated = Já resolvi de outro jeito. notScopes = Nem olho (sem motivo, sem prazo).

💡 Proteção contra limpeza

Ligou, casou: não desliga, não purga antes do prazo, só recupera.

💡 Resistente a phishing

Três chaves de verdade: Hello (ou credencial de plataforma), FIDO2 e CBA multifator. Authenticator por telefone e SMS ficam de fora.

Identidade de app

Registro mora em casa (locatário de origem); entidade de serviço é a cópia de visita em cada cliente.

Tabela de memorização: não confunda

Quando é...	...e quando é
Key Vault Secrets User A identidade precisa ler o valor de segredos (menor privilégio no escopo do segredo ou do cofre).	**Key Vault Reader** Só é preciso ver metadados do cofre e dos objetos, sem conteúdo dos segredos.
Managed Identity Operator Associar uma identidade atribuída pelo usuário existente a um recurso, sem poder alterá-la.	**Managed Identity Contributor** Criar, atualizar e excluir identidades atribuídas pelo usuário (não inclui atribuí-las).
Efeito Deny Impedir que recursos fora do padrão sejam criados.	**Enforce (DeployIfNotExists) no MCSB** Deixar criar e corrigir automaticamente o recurso não conforme na criação.
Isenção Waiver A diretoria aceitou o risco por um prazo (use data de expiração).	**Isenção Mitigated** O objetivo da política é atendido por outro controle compensatório.
Identidade atribuída pelo sistema Um recurso estável que precisa da própria identidade, com o mesmo ciclo de vida.	**Identidade atribuída pelo usuário** Várias VMs ou recursos recriados com frequência que precisam manter as mesmas permissões.
PIM for Groups Um grupo concede vários acessos (assinaturas e app SaaS) e tudo deve virar just-in-time de uma vez.	**PIM para recursos do Azure** Tornar qualificada uma função do Azure em um escopo específico, configurada por recurso.
Cofre imutável Habilitado Bloquear operações destrutivas mantendo a possibilidade de desfazer.	**Cofre imutável Habilitado e bloqueado** Proteção irreversível contra redução de retenção e exclusão de backups por administrador mal-intencionado.

Números que caem

Item	Valor
Peso do domínio no exame	**20-25%**
Duração máxima de ativação no PIM	**1 a 24 horas**
Vida útil do Temporary Access Pass	**10 minutos a 30 dias**
Validade máxima de segredo de cliente	**24 meses (recomendado menos de 12)**

Tokens de vida longa com CAE	**até 28 horas**
Retenção da exclusão temporária do Key Vault	**7 a 90 dias (padrão 90), definida na criação**
Regras do firewall do Key Vault	**até 1000 regras de IPv4 público e até 200 regras de rede virtual**
Funções personalizadas do Azure por locatário	**5.000**
Exclusão temporária do Azure Backup	**14 a 180 dias**
Políticas legadas de MFA e SSPR deixam de gerenciar métodos	**30/09/2025**
Validação do Managed HSM	**FIPS 140-3 nível 3**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** NotActions com delete na função personalizada impede a exclusão mesmo que o usuário tenha outra função.
Como não cair: Permissões são aditivas e NotActions só subtrai daquela função. Negar de verdade exige atribuição de negação, criada por deployment stack com deny settings ou aplicativo gerenciado.

⚠ **Alerta de prova:** Bloqueio ReadOnly ou CanNotDelete na conta de armazenamento protege os blobs.
Como não cair: Bloqueios atuam só no plano de controle; gravar e excluir blobs continua possível. Já o ReadOnly quebra listKeys e a criação de atribuições de função.

⚠ **Alerta de prova:** Definir exp do segredo para ontem faz o aplicativo parar de lê-lo.
Como não cair: Para segredos, exp e nbf são informativos e o get continua funcionando. Use enabled = false para bloquear mantendo a versão.

⚠ **Alerta de prova:** Key Vault Reader permite ler o valor dos segredos.
Como não cair: Reader lê metadados. O valor vem de Key Vault Secrets User; em cofre RBAC, política de acesso Get nem é avaliada.

⚠ **Alerta de prova:** Com acesso público Desabilitado, a regra de IP do pipeline continua valendo e os serviços confiáveis são bloqueados.
Como não cair: É o contrário: regras de IP e de VNet param, serviços confiáveis seguem. Azure DevOps não é serviço confiável e precisa de rede privada.

⚠ **Alerta de prova:** Purgar o segredo excluído para recriar com o mesmo nome em cofre com proteção contra limpeza.
Como não cair: A proteção impede purge até o fim da retenção e não pode ser desligada. Recupere o segredo excluído.

⚠ **Alerta de prova:** Atribuir Reader na VM tem precedência sobre o Owner herdado.
Como não cair: RBAC é aditivo; remova o Owner no escopo de origem (Check access mostra qual) e atribua a função correta.

⚠ **Alerta de prova:** Revisor do fluxo de consentimento do administrador consegue aprovar qualquer pedido.
Como não cair: A designação como revisor não eleva privilégio; ele precisa de função que permita conceder o consentimento pedido.

⚠ **Alerta de prova:** Atribuir a política deployIfNotExists corrige automaticamente os recursos antigos.
Como não cair: Ela age no que é criado ou alterado. Recursos existentes exigem tarefa de correção com a identidade gerenciada da atribuição.

⚠ **Alerta de prova:** A duração de ativação definida na assinatura vale para o grupo de recursos no PIM.
Como não cair: Configurações de função do PIM para recursos do Azure são por função e por recurso, sem herança; configure em cada escopo onde há atribuição.

⚠ **Alerta de prova:** Contributor consegue remover bloqueios de recurso.
Como não cair: Gerenciar bloqueios exige Microsoft.Authorization/locks/*, presente em Owner e User Access Administrator, em qualquer escopo.

⚠ **Alerta de prova:** Habilitar CMK no cofre de backup depois do primeiro backup.
Como não cair: Com itens já protegidos ou registrados não é possível; configure identidade, acesso à chave e a chave antes de proteger qualquer item.

⚠ **Alerta de prova:** Atribuir Owner ou Contributor dá acesso aos dados de blobs quando a chave compartilhada está desabilitada.
Como não cair: Essas são funções de plano de controle sem DataActions. Use Storage Blob Data Reader (mais Reader para navegar no portal), atribuídas a grupo.

⚠ **Alerta de prova:** Política de acesso condicional desativada aparece no What If.
Como não cair: O What If considera só políticas ativadas ou em somente relatório; para medir impacto, use somente relatório.

Como cai na prova

📝 **Como cai:** Pede a função de menor privilégio para uma identidade fazer algo específico.
Como resolver: Identifique se a ação é de controle ou de dados, escolha a função mais estreita que contém a ação (Secrets User, Crypto Service Encryption User, Managed Identity Operator, Storage Blob Data Reader) e o menor escopo possível (segredo, identidade, grupo de recursos). Descarte Owner, Contributor e funções Officer.

📝 **Como cai:** Um controle não teve o efeito esperado (segredo ainda lido, bloqueio não protegeu, Reader não restringiu).
Como resolver: Pergunte em qual plano o controle atua e se ele é aditivo ou informativo. exp de segredo é informativo, bloqueio é plano de controle, RBAC é aditivo e NotActions não nega.

📝 **Como cai:** Política de acesso condicional a ser criada com teste prévio.
Como resolver: Somente relatório para medir nos logs de entrada, What If para simular um usuário, exclusão das contas de emergência; risco de entrada e de usuário em políticas separadas.

📝 **Como cai:** Configuração do Key Vault por IaC ou na criação.
Como resolver: Lembre o que só se define na criação (retenção da exclusão temporária) e o que é irreversível (proteção contra limpeza). Em Bicep: enableRbacAuthorization, enablePurgeProtection e softDeleteRetentionInDays de 7 a 90; em template ARM com segredo: enabledForTemplateDeployment, vaults/deploy/action e securestring.

📝 **Como cai:** Governança em várias assinaturas, inclusive futuras.
Como resolver: Atribua no grupo de gerenciamento correto (não no raiz), com a definição salva nele ou acima; use Deny para impedir e tarefa de correção para corrigir o que já existe.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
primeiro acesso sem senha, registrar passkey no primeiro dia	**Temporary Access Pass emitido por Administrador de Autenticação**
aprovação, justificativa e MFA na ativação de função	**Configurações da função no PIM (atribuição qualificada)**
acesso revogado quase em tempo real após desabilitar conta	**Avaliação contínua de acesso (CAE)**
medir impacto antes de impor e não perder acesso administrativo	**Somente relatório + What If + excluir contas de emergência**

usuário pode consentir só apps de baixo risco	**Editores verificados + permissões delegadas classificadas como de baixo impacto**
pipeline sem segredo no GitHub Actions	**Credencial de identidade federada (OIDC) no registro de aplicativo**
erro em userAssignedIdentities/assign/action	**Managed Identity Operator no escopo da identidade**
delegar atribuição de funções só de algumas funções e só a grupos	**Role Based Access Control Administrator com condição**
wrap e unwrap da chave para CMK de Storage, SQL ou discos	**Key Vault Crypto Service Encryption User**
quem leu o segredo do cofre	**Configuração de diagnóstico com AuditEvent no Log Analytics (log de atividades só vê plano de controle)**
HSM de locatário único e domínio de segurança do cliente	**Azure Key Vault Managed HSM**
impedir novos recursos fora da região, mantendo os existentes como não conformes	**Política Allowed locations com efeito Deny**
segunda aprovação para mexer na segurança do backup	**Autorização multiusuário com Resource Guard**
controle de processo (treinamento) no painel de conformidade	**Atestação manual com evidência**

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

- Bloqueios, Contributor e log de atividades são plano de controle; não protegem nem registram dados.
- NotActions não é negação; atribuições de negação só são criadas pelo Azure.
- Proteção contra limpeza é irreversível e a retenção da exclusão temporária só é definida na criação do cofre.
- Para segredos, exp e nbf são informativos; enabled = false bloqueia a leitura.
- Somente relatório + What If antes de impor, sempre excluindo contas de emergência das políticas de bloqueio.

Essenciais para a prova (checklist)

☐ Sei configurar o PIM para funções do Entra, recursos do Azure e grupos, com aprovação, justificativa e MFA.

☐ Sei criar e testar políticas de acesso condicional com locais nomeados, risco, somente relatório e What If.

☐ Sei quais métodos atendem a força resistente a phishing e quando usar TAP, campanha de registro e perfis de passkey.

☐ Sei diferenciar objeto de aplicativo e entidade de serviço e responder a um consent phishing.

☐ Sei escolher entre identidade gerenciada atribuída pelo sistema e pelo usuário e as funções para associá-las.

☐ Sei configurar rede, RBAC, exclusão temporária e proteção contra limpeza do Key Vault.

☐ Sei rotacionar chaves, renovar certificados e bloquear segredos no Key Vault.

☐ Sei usar Azure Policy com Deny, Audit, deployIfNotExists, tarefas de correção e isenções.

☐ Sei o efeito de bloqueios CanNotDelete e ReadOnly e quem pode gerenciá-los.

☐ Sei proteger backups com MUA, cofre imutável bloqueado e CMK.

Questões de revisão do capítulo

R2.1 · Gerenciar identidade, acesso e governança

Na Editora Horizonte, usuários não podem consentir com aplicativos que pedem permissões amplas. O engenheiro habilitou o fluxo de trabalho de consentimento do administrador e designou como revisor um analista do service desk sem função administrativa. O analista vê as solicitações na guia Minhas pendentes, mas não consegue aprovar nenhuma. Qual é a causa?

A. Cada solicitação precisa ser validada antes pelo editor verificado do aplicativo para liberar a aprovação
B. O fluxo de trabalho aceita grupos e funções como revisores, mas não aceita usuários designados individualmente
C. A designação como revisor não eleva privilégios; ele precisa de função que permita conceder consentimento
D. A aprovação fica bloqueada até a solicitação atingir o prazo de expiração configurado no fluxo de trabalho

R2.2 · Gerenciar identidade, acesso e governança

A Mineradora Serra Azul vai habilitar criptografia com chave gerenciada pelo cliente em uma conta de armazenamento, usando uma chave guardada em um cofre com modelo de permissão RBAC. A identidade gerenciada da conta precisa ler os metadados da chave e executar as operações wrap e unwrap, sem nenhum outro privilégio. Qual função atribuir a ela?

A. Key Vault Crypto Officer com escopo no cofre
B. Key Vault Crypto Service Encryption User
C. Key Vault Contributor com escopo no cofre
D. Key Vault Secrets User com escopo no cofre

R2.3 · Gerenciar identidade, acesso e governança

O Banco Cooperativo Centro teme que um administrador de backup com credencial comprometida desative a exclusão temporária ou reduza a retenção do cofre dos Serviços de Recuperação antes de apagar os backups. Qual controle exige aprovação de outra equipe?

A. Bloqueio CanNotDelete no cofre dos Serviços de Recuperação e no grupo de recursos de backup
B. Política do Azure que audita cofres de backup sem criptografia com chave gerenciada pelo cliente
C. Autorização multiusuário com Resource Guard em outro locatário, gerido pela equipe de segurança
D. Função Backup Contributor atribuída de forma permanente ao administrador de backup da empresa

R2.4 · Gerenciar identidade, acesso e governança

A rede de restaurantes Sabor Mineiro emite os certificados TLS dos seus sites pelo Azure Key Vault e quer que eles sejam renovados antes do vencimento, sem pedido manual à autoridade certificadora. Qual configuração atende?

A. Usar uma CA integrada (DigiCert ou GlobalSign) como emissor e a ação autoRenew com gatilho antes da expiração
B. Definir a ação emailContacts com gatilho de 30 dias antes da expiração para renovar o certificado no cofre
C. Importar o certificado como segredo e configurar uma política de rotação de chave com notificação no Event Grid
D. Usar uma CA não integrada como emissor e a ação autoRenew com gatilho em 80% do tempo de vida do certificado

Respostas comentadas

R2.1. C) A designação como revisor não eleva privilégios; ele precisa de função que permita conceder consentimento

Por quê: No fluxo de trabalho de consentimento do administrador, revisores podem ver, bloquear ou negar solicitações, mas só aprovam se tiverem permissão para conceder consentimento; permissões de aplicativo do Microsoft Graph exigem Global Administrator.

✗ A) Incorreta. Não há etapa de validação pelo editor do aplicativo no fluxo de consentimento do administrador.
✗ B) Incorreta. Usuários, grupos e funções podem ser designados como revisores.
✗ D) Incorreta. O prazo de expiração define até quando a solicitação é válida; ele não libera a aprovação.

> **Dica de prova:** Revisor do admin consent workflow sem função administrativa vê e nega, mas não aprova.

R2.2. B) Key Vault Crypto Service Encryption User

Por quê: Para serviços que usam chave gerenciada pelo cliente (Storage, SQL, discos), a função de menor privilégio no plano de dados é Key Vault Crypto Service Encryption User.

✗ A) Incorreta. Crypto Officer executa qualquer ação sobre chaves (criar, excluir, rotacionar), muito além do necessário.
✗ C) Incorreta. Key Vault Contributor atua no plano de controle e não dá acesso a operações com chaves no plano de dados.
✗ D) Incorreta. Secrets User lê conteúdo de segredos, não executa operações criptográficas com chaves.

> **Dica de prova:** Wrap/unwrap para CMK = Key Vault Crypto Service Encryption User; Contributor é plano de controle.

R2.3. C) Autorização multiusuário com Resource Guard em outro locatário, gerido pela equipe de segurança

Por quê: Na autorização multiusuário do Azure Backup, o administrador de backup precisa receber temporariamente Backup MUA Operator no Resource Guard para executar operações críticas protegidas.

✗ A) Incorreta. O bloqueio impede excluir o cofre, mas não impede alterar políticas e configurações de segurança.
✗ B) Incorreta. Auditar criptografia não impede operações destrutivas do administrador.
✗ D) Incorreta. Permissão permanente amplia o risco em vez de exigir uma segunda aprovação.

> **Dica de prova:** Segunda aprovação para mexer em segurança do backup = MUA com Resource Guard (de preferência em outro locatário).

R2.4. A) Usar uma CA integrada (DigiCert ou GlobalSign) como emissor e a ação autoRenew com gatilho antes da expiração

Por quê: A política do certificado tem ações de tempo de vida (autoRenew ou emailContacts) com gatilho por dias antes da expiração ou porcentagem do tempo de vida; a renovação automática exige emissor autoassinado ou CA integrada.

✗ B) Incorreta. emailContacts só avisa os contatos de certificado do cofre; a renovação continuaria manual.
✗ C) Incorreta. Guardar certificado como segredo é desaconselhado, e a política de rotação de chaves não renova certificados junto à CA.
✗ D) Incorreta. Com CA não integrada, o Key Vault não renova automaticamente; só é possível notificar por e-mail.

> **Dica de prova:** Renovação automática no Key Vault: CA parceira (DigiCert/GlobalSign) ou autoassinado, com a ação autoRenew.

03

CAPÍTULO 3 · 20-25% DA PROVA

Proteger a computação

Este domínio junta três mundos: segurança de IA (SharePoint, Purview DSPM, Copilot Studio, Entra Agent ID, AI Gateway no API Management, Defender for AI Services, guardrails do Foundry e agentes no Microsoft 365 admin center), servidores e VMs (criptografia de disco, Bastion, JIT, Arc, Defender for Servers, varredura sem agente, Trusted Launch e Machine Configuration) e plataformas de aplicativos (contêineres, AKS, ACR, Functions, Logic Apps, App Service, WAF e APIM). A prova cobra muito o recurso exato e o plano que o oferece: o que é Plano 1 ou Plano 2, Standard ou Premium, com ou sem agente. Nos temas de IA, a dificuldade é saber onde se configura cada coisa (Power Platform admin center, Entra admin center, Defender for Cloud, Foundry, Microsoft 365 admin center). Eu erro mais quando duas alternativas usam o produto certo no lugar errado, então sempre confirmo o portal e o escopo antes de marcar.

Neste capítulo

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

Tópicos-chave

Políticas do API Management

validate-azure-ad-token valida tokens do Entra (tenant-id, client-application-ids, audiences); validate-jwt serve a outros provedores. rate-limit-by-key contém picos e devolve 429; quota-by-key limita volume em períodos maiores (mínimo 300 segundos, não disponível nos níveis v2) e devolve 403. ip-filter com action forbid bloqueia endereços.

AI Gateway no API Management

llm-token-limit (que reúne a antiga azure-openai-token-limit) só vale na seção inbound, limita tokens por counter-key com tokens-per-minute (excesso 429) ou token-quota (excesso 403). authentication-managed-identity elimina a chave do back-end do Foundry. llm-content-safety envia ao Azure AI Content Safety com identidade gerenciada (Cognitive Services User), shield-prompt detecta ataques e o bloqueio retorna 403; o limite vai de 0 (mais restritivo) a 7.

Trusted Launch e tipos de segurança

Tipos: Standard, Trusted Launch e Confidential VM. Trusted Launch (VM Geração 2) combina inicialização segura, vTPM e, com a extensão Guest Attestation, monitoramento de integridade que alerta no Defender for Cloud. Em VM existente: Gen2, backup na política Enhanced e VM desalocada antes de trocar o tipo.

Criptografia de disco de VMs

Criptografia no host cifra discos temporários, efêmeros e caches no host físico, sem usar CPU da VM; exige registrar EncryptionAtHost e não pode ser ativada em VM que já usou Azure Disk Encryption (aposentadoria em 15/09/2028). CMK em discos gerenciados usa conjunto de criptografia de disco com chave no Key Vault da mesma região e proteção contra limpeza. VM confidencial tem criptografia de disco do SO confidencial com chave vinculada ao vTPM, escolhida só na criação.

Azure Bastion por SKU

Basic já dá RDP/SSH pelo navegador sem expor as portas da VM. Standard e Premium acrescentam cliente nativo pela CLI, link compartilhável, IP-Connect, portas personalizadas, transferência de arquivos e escala. Premium acrescenta gravação de sessão e implantação private-only (definida na criação). Basic, Standard e Premium usam AzureBastionSubnet /26 ou maior; Developer é gratuito e compartilhado.

Acesso just-in-time (JIT)

Recurso do Defender for Servers Plano 2: mantém negação nas portas de gerenciamento e abre para o IP solicitado pelo tempo definido (padrão máximo de 3 horas), via NSG ou DNAT no Azure Firewall. Exige a permissão jitNetworkAccessPolicies/initiate/action; não suporta firewall gerenciado pelo Firewall Manager nem VMs clássicas. Cada solicitação fica no log de atividades da VM.

Defender for Servers Plano 1 x Plano 2

Os dois incluem Defender for Endpoint (extensão MDE.Windows ou MDE.Linux, sem licença separada), inventário de software e avaliação de vulnerabilidades do Defender Vulnerability Management. O Plano 2 acrescenta FIM, JIT, varredura sem agente (vulnerabilidades, segredos e malware), recursos premium do MDVM e 500 MB por dia de ingestão gratuita.

Varredura sem agente de máquinas

Lê instantâneos dos discos fora da VM, sem instalar nada e sem impacto no desempenho; disponível no Defender CSPM e no Defender for Servers Plano 2 (malware só no Plano 2). Discos com CMK exigem permissões de chave no Key Vault para o scanner, e máquinas são excluídas por tag configurada no plano.

Azure Arc e multinuvem para servidores

Integração em escala usa entidade de serviço com a função Azure Connected Machine Onboarding. Em AWS, o provisionamento automático do Arc depende do SSM Agent com AmazonSSMManagedInstanceCore; em GCP, do agente OS Config. O agente do Log Analytics foi aposentado e não participa.

Azure Machine Configuration

Audita e configura o SO como código, incluindo as linhas de base de segurança de computação do Azure (Windows e Linux). VMs do Azure precisam da extensão e de identidade gerenciada atribuída pelo sistema, implantadas pela iniciativa de pré-requisitos; servidores do Arc já trazem o recurso no Connected Machine agent.

Defender for Containers

Sem agente: descoberta do Kubernetes, avaliação de vulnerabilidades de imagens (MDVM, com reavaliação diária) e proteção do plano de controle. Com o sensor do Defender (DaemonSet): detecção de ameaças em runtime, antimalware, DNS e desvio de binários. Implantação controlada exige sensor com Security Gating; a regra padrão só audita, bloquear exige regra personalizada com ação Deny.

AKS, ACR e ACI

AKS sem credencial estática: Azure RBAC para Kubernetes + contas locais desabilitadas; intervalos de IP autorizados mantêm o endpoint público e não combinam com cluster privado. Workload ID exige credencial federada com emissor OIDC do cluster e assunto da conta de serviço. ACR: usuário administrador desabilitado e AcrPull para identidades; tokens com mapa de escopo para quem não tem identidade Entra. ACI só puxa do ACR com identidade atribuída pelo usuário.

App Service, Functions, Logic Apps e Container Apps

App Service: HTTPS Only, TLS mínimo 1.2, desligar autenticação básica de FTP e SCM; referências do Key Vault usam keyVaultReferenceIdentity quando a identidade é atribuída pelo usuário; só via Front Door = AzureFrontDoor.Backend + X-Azure-FDID. Functions no plano Consumo não tem ponto privado nem integração de VNet (use Flex Consumption, Premium ou Dedicado). Logic Apps Consumo: política de autorização do Entra (emissor e público) e sasAuthenticationPolicy Disabled. Container Apps: URI de segredo sem versão acompanha rotações.

WAF

No Application Gateway, modo de detecção só registra e prevenção bloqueia com 403; falso positivo se trata com exclusão por regra (CRS 3.2 ou posterior), não desligando o WAF. No Front Door, regras personalizadas são MatchRule (ex.: GeoMatch) ou RateLimitRule.

Superexposição no SharePoint e DSPM for AI

Restricted Content Discovery tira o site da pesquisa da organização e do Copilot sem mudar permissões; controle de acesso restrito bloqueia o acesso. Relatórios de governança de acesso a dados e revisão de acesso do site deixam o proprietário revisar. O DSPM for AI depende da auditoria do Purview; a avaliação de risco padrão roda semanalmente nos 100 sites mais usados, e apps de IA de terceiros exigem dispositivos integrados, extensão do navegador e DLP de endpoint.

Microsoft Entra Agent ID

Patrocinador (sponsor) é obrigatório e responde pelo agente (pode desabilitar); proprietário cuida de credenciais e pode restaurar; gerente pede pacotes de acesso. Desabilitar o blueprint para todos os agentes criados dele; para um agente comprometido, desabilite a identidade de agente. Acesso condicional para agentes usa o controle Bloquear (agentes não fazem MFA), escopo por agente, blueprint ou atributo de segurança personalizado; no fluxo on-behalf-of o sujeito avaliado é o usuário.

Defender for AI Services e guardrails do Foundry

O plano AI services do Defender for Cloud, sem agente e só sobre tokens de texto, gera alertas de jailbreak (bloqueado ou detectado), vazamento de dados e roubo de credenciais, enviados ao Defender XDR; a evidência do prompt mostra o trecho suspeito e o UserSecurityContext identifica usuário e IP. No Foundry, o guardrail do agente substitui por completo o do modelo; Prompt Shields cobre ataques de prompt do usuário e ataques de documento; Task Adherence detecta chamadas de ferramenta fora da intenção do usuário.

Copilot Studio e agentes no Microsoft 365 admin center

Proteção em tempo real do Copilot Studio: configurada por ambiente no Power Platform admin center (Security > Threat detection), com registro de aplicativo com credencial federada; só para orquestração generativa, e o comportamento de erro padrão deixa o agente responder (Block the query bloqueia). No Microsoft 365 admin center, Block impede o agente na organização e remove de quem instalou; Uninstall permite reinstalar; Delete é recuperável por 30 dias; Agent settings controla Sharing (All users, No users, Specific users).

Macetes para memorizar

💡 Códigos HTTP do APIM

Pico = 429 (rate-limit, tokens por minuto). Cota ou bloqueio de conteúdo = 403 (quota, token-quota, content safety).

💡 Defender for Servers

Plano 2 = FJS: FIM, JIT e Sem agente (com malware). O resto (MDE e MDVM básico) os dois têm.

💡 Bastion

Basic navega; Standard Nativo e Link; Premium Grava e Esconde (private-only).

💡 Entra Agent ID

Sponsor responde pelo negócio, Owner cuida da chave, Manager só pede acesso. Blueprint é a mãe: desligou, caem todos os filhos.

💡 Guardrail no Foundry

Agente com guardrail próprio não herda nada: substitui, não soma.

💡 Sensor do Defender for Containers

Ver o que está rodando (runtime, drift, malware) precisa de sensor; olhar de fora (descoberta, imagens, plano de controle) é sem agente.

Arc multinuvem

AWS fala SSM, Google fala OS Config.

Tabela de memorização: não confunda

Quando é...	...e quando é
rate-limit-by-key Conter picos em janela curta (ex.: 20 chamadas por 60 segundos); excesso devolve 429.	**quota-by-key** Limitar volume total em períodos longos (mínimo 300 segundos, não existe nos níveis v2); excesso devolve 403.
Trusted Launch Inicialização segura e vTPM contra bootkits e rootkits, sem custo adicional, em VM Geração 2.	**Confidential VM** Isolamento e criptografia de memória por hardware, com chave do disco do SO vinculada ao vTPM e protegida dos operadores do host.
Criptografia no host Cobrir discos temporários e caches no host sem gastar CPU da VM, substituindo o Azure Disk Encryption.	**Conjunto de criptografia de disco (SSE com CMK)** Discos gerenciados cifrados em repouso com chave da empresa no Key Vault, rotacionável pela segurança.
Defender for Servers Plano 1 EDR com Defender for Endpoint e avaliação de vulnerabilidades pelo sensor, sem outro agente.	**Defender for Servers Plano 2** Também FIM, JIT, varredura sem agente com malware, recursos premium do MDVM (linhas de base, certificados) e 500 MB/dia gratuitos.
Prompt Shields para ataques de prompt do usuário Jailbreak digitado por quem usa o assistente.	**Prompt Shields para ataques de documento** Instruções escondidas em conteúdo de terceiros, como currículos, e-mails e páginas (injeção indireta).
Desabilitar a identidade de agente Parar um agente comprometido mantendo os demais do mesmo blueprint funcionando.	**Desabilitar o blueprint de agente** Bloquear todas as identidades de agente criadas a partir daquele blueprint.
Restricted Content Discovery Esconder o site do Copilot e da pesquisa sem mudar permissões nem bloquear quem já trabalha nele.	**Controle de acesso restrito do SharePoint** Bloquear o acesso de quem não está nos grupos permitidos do site.

Números que caem

Item	Valor
Peso do domínio no exame	**20-25%**
Aposentadoria do Azure Disk Encryption	**15/09/2028**
Janela máxima padrão do JIT	**3 horas**

Ingestão gratuita do Defender for Servers Plano 2	**500 MB por dia**
AzureBastionSubnet (Basic, Standard e Premium)	**/26 ou maior**
Período mínimo do quota-by-key	**300 segundos**
Limite de severidade do llm-content-safety	**0 (mais restritivo) a 7 (menos restritivo)**
Avaliação de risco padrão do DSPM for AI	**100 sites mais usados, semanal, primeiros resultados em cerca de 4 dias**
Delete de agente no Microsoft 365 admin center	**recuperável por 30 dias**
Referência do Key Vault sem versão no App Service	**nova versão usada em até 24 horas**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** O Plano 1 do Defender for Servers não inclui o Defender for Endpoint, então é preciso migrar para o Plano 2 ou comprar licenças.
Como não cair: Os dois planos incluem a integração com o Defender for Endpoint, provisionada como extensão MDE. O Plano 2 só acrescenta FIM, JIT, varredura sem agente e recursos premium.

⚠ **Alerta de prova:** JIT disponível no Plano 1 ou funcionando com firewall do Firewall Manager.
Como não cair: JIT é do Plano 2, usa NSG ou DNAT no Azure Firewall e não suporta firewalls gerenciados pelo Firewall Manager nem VMs clássicas.

⚠ **Alerta de prova:** A varredura sem agente instala um agente temporário ou não lê discos com CMK.
Como não cair: Nada é instalado; ela analisa instantâneos dos discos. Discos com CMK são suportados com permissões de chave no Key Vault.

⚠ **Alerta de prova:** Atribuir ao agente um guardrail com só Violência e Ódio mantém o controle de material protegido que estava no modelo.
Como não cair: O guardrail do agente substitui totalmente o da implantação do modelo; repita nele todos os controles necessários.

⚠ **Alerta de prova:** Exigir MFA para identidades de agente de risco alto no acesso condicional.
Como não cair: Agentes não fazem login interativo nem MFA; o controle aplicável é Bloquear, começando em somente relatório para medir impacto.

⚠ **Alerta de prova:** Política de acesso condicional com a identidade do agente como alvo bloqueia o agente que lê e-mails em nome do usuário.
Como não cair: No fluxo on-behalf-of o sujeito do token é o usuário, então valem as políticas dos usuários. A política de identidade de agente vale para o acesso somente aplicativo.

⚠ **Alerta de prova:** Usar validate-jwt na seção de back-end para o APIM autenticar no modelo do Foundry.
Como não cair: validate-jwt valida tokens recebidos dos chamadores. Para o APIM autenticar no back-end sem chave, use identidade gerenciada com authentication-managed-identity.

⚠ **Alerta de prova:** Colocar llm-token-limit na seção outbound para usar o consumo real informado pelo modelo.
Como não cair: A política só é válida na seção inbound; com estimate-prompt-tokens o bloqueio acontece antes de chamar o modelo.

⚠ **Alerta de prova:** Atualizar o Bastion Standard para Premium e trocar o IP público por privado no recurso existente.
Como não cair: Private-only é definido na implantação; é preciso remover e implantar de novo um Bastion Premium. Gravação de sessão também é só Premium.

⚠ **Alerta de prova:** Identidade atribuída pelo sistema do ACI puxando imagem do ACR com AcrPull.
Como não cair: No ACI, o pull do ACR com identidade só é suportado com identidade gerenciada atribuída pelo usuário.

⚠ **Alerta de prova:** Editar a regra padrão de auditoria da implantação controlada para bloquear imagens vulneráveis.
Como não cair: A regra padrão tem ação Audit e só gera evento de admissão. Para impedir, crie regra personalizada com ação Deny e escopo no namespace.

⚠ **Alerta de prova:** Restringir o App Service ao Front Door só com a marca AzureFrontDoor.Backend.
Como não cair: A marca cobre o Front Door de todos os clientes; inclua o filtro do cabeçalho X-Azure-FDID com o ID do seu perfil.

⚠ **Alerta de prova:** Desinstalar o agente no Microsoft 365 admin center para impedir o uso na organização.
Como não cair: Uninstall não impede a reinstalação. Para impedir o uso em todo o locatário e remover o agente de quem já o instalou, use Block em Agents > All agents.

⚠ **Alerta de prova:** O DSPM for AI não mostra interações do Copilot porque falta a extensão do navegador.
Como não cair: A extensão é para sites de IA de terceiros. Para o Microsoft 365 Copilot, o pré-requisito é a auditoria do Purview ativada.

Como cai na prova

📝 **Como cai:** Pedido de recurso de VM com uma restrição de plano (Plano 1 ou 2, sem agente, sem licença extra).
Como resolver: Separe o que está nos dois planos (MDE, MDVM básico) do que é exclusivo do Plano 2 (FIM, JIT, varredura sem agente, malware sem agente, MDVM premium). Elimine alternativas que citam o agente do Log Analytics ou o Qualys integrado, ambos aposentados.

📝 **Como cai:** Cenário de IA com a pergunta onde configurar.
Como resolver: Mapeie o produto ao portal: Copilot Studio no Power Platform admin center; Agent ID e acesso condicional no Entra admin center; jailbreak de modelos no Defender for Cloud (AI services); guardrails no Foundry; bloqueio e publicação de agentes no Microsoft 365 admin center; superexposição no SharePoint admin center e no DSPM for AI do Purview.

📝 **Como cai:** Agente de IA comprometido ou de risco, pedindo a ação de menor impacto.
Como resolver: Veja o escopo: um agente = desabilitar a identidade de agente; vários aprovados com regra estável = atributo de segurança personalizado com política de bloqueio por exclusão; sempre comece políticas em somente relatório.

📝 **Como cai:** Política do APIM para um requisito de segurança da API ou do modelo.
Como resolver: Classifique o requisito: validar token (validate-azure-ad-token ou validate-jwt), limitar chamadas (rate-limit-by-key/quota-by-key), limitar tokens (llm-token-limit), conteúdo (llm-content-safety), autenticar no back-end (authentication-managed-identity), bloquear IP (ip-filter forbid).

📝 **Como cai:** Aplicativo PaaS exposto ou usando segredo compartilhado.
Como resolver: Prefira identidade: Easy Auth no lugar de chave de função, política de autorização do Entra com SAS desativada no Logic Apps, identidade gerenciada com AcrPull no ACR, referência do Key Vault sem versão. Verifique se o plano suporta rede privada (Functions Consumo não suporta).

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
token do Microsoft Entra no APIM, só de aplicativos específicos	**validate-azure-ad-token com client-application-ids**

uma equipe consumiu a cota de tokens do modelo	**llm-token-limit inbound com counter-key da assinatura**
porta 3389 fechada por padrão e aberta sob demanda	**JIT do Defender for Servers Plano 2**
proibido instalar agente, mas quer vulnerabilidades e segredos dos discos	**Varredura sem agente (instantâneos de disco)**
EC2 não vira servidor do Arc / Compute Engine não vira servidor do Arc	**SSM Agent com AmazonSSMManagedInstanceCore / agente OS Config**
rootkits e bootkits, vTPM, alerta de integridade de boot	**Trusted Launch + Guest Attestation**
disco temporário e cache cifrados sem dm-crypt	**Criptografia no host**
instrução escondida em documento enviado ao modelo	**Prompt Shields para ataques de documento**
chamada de ferramenta que não corresponde ao pedido do usuário	**Guardrail com Task Adherence atribuído ao agente**
alerta de jailbreak em modelos do Foundry com trecho do prompt	**Plano AI services do Defender for Cloud + evidência do prompt do usuário**
até onde chega um agente comprometido	**Caminhos de ataque e raio de alcance no Exposure Management (corrigir o ponto de estrangulamento)**
esconder site do Copilot sem mexer em permissões	**Restricted Content Discovery**
Copilot Studio avaliado pelo Defender em tempo de execução	**Power Platform admin center > Security > Threat detection, por ambiente**
pull de um repositório do ACR por dispositivos sem identidade Entra	**Token por dispositivo + mapa de escopo**

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

- Defender for Endpoint vem nos dois planos do Defender for Servers; FIM, JIT e varredura sem agente com malware são do Plano 2.
- Trusted Launch exige VM Geração 2; a troca em VM existente pede backup Enhanced e VM desalocada.
- O guardrail do agente no Foundry substitui o do modelo, não soma.
- Identidade de agente não faz MFA: no acesso condicional o controle é Bloquear.
- Defender for AI Services não usa agente e analisa só tokens de texto.

Essenciais para a prova (checklist)

- ☐ Sei escolher a política do APIM para validar token, limitar chamadas, limitar tokens e filtrar conteúdo, e o código HTTP de cada bloqueio.
- ☐ Sei diferenciar Trusted Launch, Confidential VM, criptografia no host e conjunto de criptografia de disco.
- ☐ Sei quais recursos do Bastion estão no Basic, no Standard e no Premium.
- ☐ Sei os requisitos e limitações do JIT e onde auditar as solicitações.
- ☐ Sei o que é Plano 1 e Plano 2 do Defender for Servers e como funciona a varredura sem agente.
- ☐ Sei integrar servidores AWS, GCP e on-premises ao Arc e aplicar Machine Configuration.
- ☐ Sei separar recursos com e sem sensor no Defender for Containers e bloquear imagens com implantação controlada.
- ☐ Sei proteger AKS, ACR, ACI, Container Apps, App Service, Functions e Logic Apps sem segredos compartilhados.
- ☐ Sei onde configurar cada controle de IA: Restricted Content Discovery, DSPM for AI, Copilot Studio, Agent ID, Defender for AI Services e guardrails do Foundry.
- ☐ Sei bloquear, publicar e governar agentes no Microsoft 365 admin center.

Questões de revisão do capítulo

R3.1 · Proteger a computação

A logtech Rota Certa implanta grupos de contêineres do Azure Container Instances em uma VNet. As imagens vêm de um Azure Container Registry Premium acessível por ponto de extremidade privado e com usuário administrador desabilitado. Como o ACI deve autenticar o pull?

A. Identidade gerenciada atribuída pelo usuário com AcrPull no registro, informada como identidade do pull
B. Usuário administrador do registro com a senha guardada em variável de ambiente segura de cada contêiner do grupo
C. Identidade gerenciada atribuída pelo sistema do grupo de contêineres, com a função AcrPull no registro
D. Pull anônimo habilitado no registro, mantendo o acesso à rede pública do registro desabilitado

R3.2 · Proteger a computação

Um cluster AKS de uma varejista baixa imagens do Azure Container Registry com o usuário administrador do registro, cuja senha está em um segredo do Kubernetes. A segurança quer eliminar essa credencial compartilhada mantendo o menor privilégio. O que fazer?

A. Dar Owner do registro à identidade kubelet e desligar o administrador
B. Manter o usuário administrador e girar as duas senhas dele a cada 30 dias
C. Desabilitar o administrador e dar AcrPull à identidade kubelet
D. Dar AcrPush à identidade kubelet e manter o administrador como contingência

R3.3 · Proteger a computação

Uma empresa de software hospeda implantações de modelos no Microsoft Foundry e quer receber, no Defender for Cloud e no Defender XDR, alertas quando usuários tentarem jailbreak contra essas implantações, com o trecho suspeito do prompt incluído no alerta. O que configurar?

A. Criar uma regra de análise no Sentinel sobre os logs de diagnóstico das implantações
B. Ativar o plano Defender CSPM e a análise de caminho de ataque da assinatura do Foundry
C. Ativar o plano AI services no Defender for Cloud e habilitar a evidência do prompt do usuário
D. Ativar a verificação de malware no upload do Defender for Storage nas contas do Foundry

R3.4 · Proteger a computação

Pelo DSPM for AI do Microsoft Purview, a Indústria Química Paulista viu que funcionários colam dados de clientes no ChatGPT usando o Chrome em dispositivos Windows. A empresa quer impedir que informações confidenciais sejam coladas ou enviadas a sites de IA de terceiros. O que deve ser implementado?

A. Dispositivos integrados ao Purview, extensão do Purview no Chrome e política de DLP de endpoint com bloqueio
B. Política de acesso condicional que bloqueia o ChatGPT para usuários que não usam um dispositivo compatível
C. Auditoria do Purview habilitada para registrar as interações dos usuários com o ChatGPT no navegador
D. Rótulos de sensibilidade com criptografia aplicados aos documentos guardados no SharePoint e no OneDrive

Respostas comentadas

R3.1. A) Identidade gerenciada atribuída pelo usuário com AcrPull no registro, informada como identidade do pull

Por quê: O ACI em VNet pode puxar imagens de um ACR privado usando identidade gerenciada atribuída pelo usuário com AcrPull, configurada via ARM/Bicep ou CLI.

✗ B) Incorreta. O usuário administrador está desabilitado e usar senha compartilhada é o que se quer evitar.
✗ C) Incorreta. A identidade atribuída pelo sistema não é suportada para o pull de imagens do ACR no ACI.
✗ D) Incorreta. Pull anônimo expõe as imagens sem autenticação e não atende ao requisito de segurança.

> **Dica de prova:** ACI puxando do ACR com identidade: tem de ser atribuída pelo usuário, com AcrPull.

R3.2. C) Desabilitar o administrador e dar AcrPull à identidade kubelet

Por quê: O usuário administrador do ACR vem desabilitado por padrão, é uma conta única com duas senhas e acesso total, sem RBAC. O recomendado é usar identidades gerenciadas com AcrPull; em registros no modo RBAC com ABAC por repositório, a função equivalente é Container Registry Repository Reader.

✗ A) Incorreta. Owner concede controle total do registro, violando o menor privilégio.
✗ B) Incorreta. Girar as senhas mantém uma credencial compartilhada com acesso total de push e pull.
✗ D) Incorreta. AcrPush permite também enviar imagens, mais do que o necessário, e o administrador continua ativo.

> **Dica de prova:** Pull de imagem sem senha = identidade gerenciada com AcrPull e usuário administrador desabilitado.

R3.3. C) Ativar o plano AI services no Defender for Cloud e habilitar a evidência do prompt do usuário

Por quê: O plano AI services do Defender for Cloud é habilitado por assinatura e gera alertas como tentativa de jailbreak bloqueada ou detectada pelo Prompt Shields. Nas configurações do plano, a evidência do prompt do usuário mostra o conteúdo suspeito; com ela desligada, a detecção continua, mas o prompt fica mascarado.

✗ A) Incorreta. Exigiria escrever e manter a detecção; o plano AI services já fornece alertas prontos com evidência do prompt.
✗ B) Incorreta. O Defender CSPM avalia postura e caminhos de ataque; não gera alertas de jailbreak em tempo de execução.
✗ D) Incorreta. A verificação de malware analisa blobs carregados, não prompts enviados aos modelos.

> **Dica de prova:** Alerta de jailbreak em modelos do Foundry = plano AI services do Defender for Cloud.

R3.4. A) Dispositivos integrados ao Purview, extensão do Purview no Chrome e política de DLP de endpoint com bloqueio

Por quê: Para apps de IA de terceiros, o DSPM for AI depende de dispositivos integrados ao Purview, da extensão do navegador (no Chrome) e de políticas de DLP de endpoint; o uso com apps de terceiros exige cobrança pague conforme o uso (pay-as-you-go).

✗ B) Incorreta. Usuários com dispositivo compatível continuariam colando dados confidenciais no site.
✗ C) Incorreta. Auditoria registra, mas não bloqueia o compartilhamento de dados.
✗ D) Incorreta. Rótulos protegem arquivos, mas não impedem copiar e colar texto no navegador.

> **Dica de prova:** Bloquear colagem de dado sensível em site de IA = DLP de endpoint + dispositivo integrado + extensão do Purview.

04

CAPÍTULO 4 · 25-30% DA PROVA

Proteger armazenamento, bancos de dados e redes

É o domínio de maior peso (25-30%), então preciso dominar três blocos: Storage (SAS, firewall, proteção de dados e Defender for Storage), Azure SQL (criptografia, firewall, auditoria e Defender for Databases) e rede (NSG/ASG, Virtual Network Manager, Azure Firewall, Virtual WAN, VPN, Private Endpoint/Private Link, Entra Private Access e Network Watcher). As questões trazem um cenário com requisito bem específico e alternativas que resolvem um problema vizinho: proteger a entrada quando o pedido era a saída, liberar o serviço inteiro quando o pedido era um recurso só, ou usar um recurso do SKU errado. Onde mais erro é na ordem de avaliação (NSG, regras do Azure Firewall, RBAC antes de ACL) e nos detalhes de SAS e DNS de ponto de extremidade privado. Antes de escolher, eu sublinho no enunciado a palavra que define o escopo: um banco, uma conta, uma sub-rede, sem trocar chave, sem IP público.

Neste capítulo

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

Tópicos-chave

Endurecimento da conta de armazenamento

Transferência segura obrigatória força HTTPS; MinimumTlsVersion rejeita versões abaixo da definida (TLS 1.2 bloqueia 1.0 e 1.1); AllowBlobPublicAccess desabilitado impede acesso anônimo em qualquer contêiner, mesmo que alguém altere o nível de um contêiner. Em escala, Azure Policy com efeito Deny impõe essas propriedades.

Tipos de SAS e chave compartilhada

SAS de conta e SAS de serviço são assinadas com a chave da conta; girar a chave as invalida. A SAS de delegação de usuário é assinada com chave de delegação obtida pelo Microsoft Entra (ação generateUserDelegationKey) e vale no máximo 7 dias. Com AllowSharedKeyAccess = false, Shared Key, SAS de conta e SAS de serviço recebem 403; tokens do Entra e SAS de delegação continuam valendo.

Política de acesso armazenada

Fica no contêiner, fila, tabela ou compartilhamento (até cinco por recurso) e só funciona com SAS de serviço. Alterar ou apagar a política revoga as SAS ligadas a ela sem trocar a chave. Não se aplica a SAS de conta nem a SAS de delegação de usuário.

Firewall do Armazenamento

Regras de IP aceitam só IPv4 públicos (sem faixas privadas e sem /31 ou /32) e não valem para clientes na mesma região da conta. Sub-redes do Azure entram por regra de rede virtual com ponto de extremidade de serviço Microsoft.Storage (mesma região) ou Microsoft.Storage.Global. Regra de instância de recurso libera uma instância específica de serviço do Azure (ex.: um workspace do Synapse); a exceção de serviços confiáveis vale para a lista de serviços confiáveis como um todo.

Política de ponto de extremidade de serviço

Política aplicada à sub-rede que só deixa o tráfego via ponto de extremidade de serviço alcançar as contas de armazenamento listadas. É o controle contra exfiltração para contas de outras empresas; o firewall da conta só controla quem entra nela.

Ponto de extremidade privado e DNS

Dá a um recurso específico um IP privado da VNet, acessível também por ExpressRoute/VPN. O nome do serviço ganha CNAME para o subdomínio privatelink; sem a zona privada (ex.: privatelink.blob.core.windows.net) vinculada à VNet o cliente continua recebendo o IP público. Cada serviço de Storage é um subrecurso separado: ADLS Gen2 precisa de ponto para blob e para dfs.

DNS híbrido para ponto de extremidade privado

Clientes on-premises resolvem pelo DNS local com encaminhador condicional da zona pública do serviço (ex.: database.windows.net) para o ponto de extremidade de entrada do Azure DNS Private Resolver, numa VNet vinculada à zona privatelink. O IP 168.63.129.16 só é alcançável de dentro do Azure, e o ponto de extremidade de saída atende o sentido Azure para on-premises.

Serviço Azure Private Link

Expõe um serviço próprio atrás de Standard Load Balancer (mesma região, pool baseado em NIC) para consumidores de qualquer assinatura ou locatário. Usa IPs de NAT da sub-rede do provedor (até 8), exige privateLinkServiceNetworkPolicies Disabled nessa sub-rede, e o IP real do cliente só aparece com TCP Proxy Protocol v2. Visibilidade define quem pode pedir conexão; aprovação automática define quem entra sem revisão.

Controle de acesso no ADLS Gen2

A ordem de avaliação é RBAC, depois ABAC, depois ACL: se uma função de dados como Storage Blob Data Reader já concede o acesso, as ACLs nem são consultadas. Condições ABAC em funções de dados de blob usam tags de índice de blob, nunca metadados definidos pelo usuário.

Proteção de dados de blob

Exclusão temporária de blobs e de contêineres (1 a 365 dias) recupera itens apagados; controle de versão recupera blobs sobrescritos. Armazenamento imutável tem retenção baseada em tempo (1 a 146.000 dias) e retenção legal; só a retenção por tempo BLOQUEADA impede reduzir ou remover o prazo. GRS replica também as exclusões, e bloqueio de recurso protege só a conta (plano de controle).

Chave do cliente e dupla criptografia no Storage

CMK exige cofre com exclusão temporária e proteção contra limpeza, chave RSA 2048, 3072 ou 4096 e identidade gerenciada com acesso à chave; na criação da conta usa-se identidade atribuída pelo usuário. A criptografia de infraestrutura (segunda camada AES-256) só pode ser habilitada na criação da conta.

Defender for Storage

Monitoramento de atividade detecta acessos anômalos (SAS permissiva usada externamente, local incomum). Verificação de malware no upload é cobrada por GB, tem limite mensal por conta ou herdado da assinatura e grava resultado em marcas de índice do blob. Detecção de ameaças a dados confidenciais usa os tipos de informação do Purview para priorizar alertas. Override Defender for Storage subscription-level settings permite configuração própria em uma conta.

Criptografia no Azure SQL

Always Encrypted cifra no cliente com chave mestra fora do banco, escondendo dados até de db_owner; determinística permite busca por igualdade, aleatória não (sem enclaves). Mascaramento dinâmico só altera a exibição para quem não tem UNMASK. TDE com CMK exige cofre com exclusão temporária e proteção contra limpeza e identidade do servidor com get, wrapKey e unwrapKey; HSM e rotação automática são opcionais.

Rede e autenticação no Azure SQL

Regra de firewall no nível do servidor vale para todos os bancos; no nível do banco é criada por T-SQL (sp_set_database_firewall_rule). Restrição de rede de saída com FQDNs permitidos evita exfiltração por auditoria, importação/exportação, OPENROWSET e BULK INSERT (não vale para Managed Instance). Política Redirect exige saída nas portas 11000 a 11999 além da 1433. Autenticação somente Microsoft Entra exige administrador do Entra definido.

Auditoria do Azure SQL

Destinos: conta de armazenamento, Log Analytics ou Event Hubs (streaming para SIEM externo). Auditoria no servidor cobre bancos atuais e futuros; ligar também no banco com a mesma configuração duplica registros. Na Managed Instance, é T-SQL: TO URL para Storage ou TO EXTERNAL_MONITOR com diagnóstico SQLSecurityAuditEvents. Operações do suporte da Microsoft têm auditoria própria (categoria DevOpsOperationsAudit).

Defender for Databases e avaliação de vulnerabilidades

O plano Databases agrupa Azure SQL, SQL Servers on Machines, open-source relational (PostgreSQL e MySQL flexíveis) e Cosmos DB, com Select types e cobrança por tipo. Habilitar o Defender for Azure SQL na assinatura cobre servidores futuros. A avaliação de vulnerabilidades em configuração expressa dispensa conta de armazenamento e aplica linha de base na hora. SQL Server local entra pelo Azure Arc.

NSG, ASG e Virtual Network Manager

Regras de NSG têm prioridade 100 a 4096, número menor vence e a avaliação para na primeira correspondência; padrões vão de 65000 a 65500 e não se removem. Entrada passa pelo NSG da sub-rede e depois da NIC (saída ao contrário), e NSGs são stateful. ASG permite regra por camada sem IP. Regras de administrador de segurança do AVNM são avaliadas antes dos NSGs: Deny bloqueia, Allow ainda passa pelos NSGs, Always Allow libera sem consultá-los.

Azure Firewall e Firewall Manager

Ordem: inteligência contra ameaças, depois DNAT, rede e aplicativo, seja qual for a prioridade numérica; política pai vem antes da filha. Basic: até 250 Mbps, inteligência contra ameaças só alerta, sem proxy DNS. Standard: FQDN, categorias da web, proxy DNS, Alertar e negar. Premium: inspeção TLS, IDPS, URL completa. Túnel forçado exige interface de gerenciamento com AzureFirewallManagementSubnet /26 e IP público próprio.

Macetes para memorizar

Ordem do Azure Firewall

TI-D-R-A: Threat Intel, DNAT, Rede, Aplicativo. O tipo manda antes do número; pai manda antes da filha.

Ordem dos NSGs

Entrando em casa: portão (sub-rede) e depois porta (NIC). Saindo: porta e depois portão. Os dois precisam deixar.

SAS

Conta e Serviço = Chave. Delegação = Diretório (Entra). Revogar sem trocar chave = Política no contêiner, só para Serviço.

ADLS Gen2

R-A-A: RBAC, ABAC, ACL. Quem chega primeiro e diz sim encerra a conversa.

Network Watcher

Qual regra bloqueou? Fluxo IP. Por onde vai? Próximo salto. O que vale na NIC? Regras efetivas. Latência e perda? Monitor de conexão.

SKUs do Azure Firewall

Basic só Alerta; Standard Alerta e Nega; Premium Abre o pacote (TLS, IDPS, URL).

Proteção de blobs

Apagou = exclusão temporária; sobrescreveu = versão; contêiner sumiu = exclusão temporária de contêiner; regulador = imutável BLOQUEADO.

Tabela de memorização: não confunda

Quando é...	...e quando é
Ponto de extremidade privado Acesso a UM recurso específico por IP privado, inclusive do datacenter via ExpressRoute/VPN; exige zona DNS privatelink.	**Ponto de extremidade de serviço** Sub-rede do Azure acessando o serviço pelo endpoint público, liberada por regra de rede virtual; não atende on-premises e não muda a resolução de nomes.
SAS de serviço com política de acesso armazenada Precisa revogar SAS emitidas sem girar a chave da conta (a política fica no contêiner).	**SAS de delegação de usuário** Precisa eliminar a dependência da chave da conta e ligar o token à identidade do Entra, com validade máxima de 7 dias.
Always Encrypted O DBA ou db_owner não pode ver o dado em claro em nenhuma hipótese.	**Mascaramento dinâmico de dados** Só é preciso ocultar a exibição para usuários sem UNMASK; administradores continuam vendo os dados.
Azure Firewall Standard Regras por FQDN, categorias da web por FQDN, proxy DNS e inteligência contra ameaças em Alertar e negar.	**Azure Firewall Premium** Inspeção TLS, IDPS por assinaturas e filtragem de URL completa (caminho) em HTTPS.
Regra de administrador Allow Liberar no AVNM mas ainda deixar os NSGs das equipes decidirem.	**Regra de administrador Always Allow** Garantir que o tráfego (ex.: scanners do SOC) passe mesmo que os NSGs das equipes neguem.
Verificação de fluxo IP Testar um fluxo de 5 tuplas e saber qual regra permite ou nega, sem gerar tráfego.	**Regras de segurança efetivas** Ver o conjunto combinado de tudo que vale na NIC (NSG da sub-rede, da NIC e regras de administrador).
Quick Access do Private Access Transição da VPN agrupando vários segmentos (FQDN, IP, portas) em um único aplicativo.	**Acesso por aplicativo do Private Access** Um servidor interno precisa de atribuição ou acesso condicional próprio, diferente dos demais.

Números que caem

Item	Valor
Peso do domínio no exame	**25-30%**
Validade máxima da chave de delegação (SAS de delegação de usuário)	**7 dias**

Políticas de acesso armazenadas por contêiner, fila, tabela ou compartilhamento	**até 5**
Retenção da exclusão temporária de blobs e contêineres	**1 a 365 dias**
Retenção baseada em tempo do armazenamento imutável	**1 a 146.000 dias**
Prioridade das regras personalizadas de NSG	**100 a 4096 (padrões de 65000 a 65500)**
AllowInternetOutBound / DenyAllOutBound	**65001 / 65500**
Portas de redirecionamento do Azure SQL (política Redirect)	**11000 a 11999, além da 1433**
AzureFirewallManagementSubnet	**/26 ou maior, com IP público próprio**
Throughput do Azure Firewall Basic	**até 250 Mbps**
IPs de NAT do serviço Private Link	**até 8**
Origem das sondas do Load Balancer (marca AzureLoadBalancer)	**168.63.129.16**
Aposentadoria dos logs de fluxo de NSG	**30/09/2027**
Aposentadoria das APIs da avaliação de vulnerabilidades clássica do SQL	**16/08/2027**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Bloquear o FQDN numa regra de aplicativo de prioridade 100 basta, porque a coleção de rede com permissão está em 300.
Como não cair: No Azure Firewall o tipo vem antes do número: DNAT, depois rede, depois aplicativo. Uma regra de rede permissiva libera o tráfego antes de a regra de aplicativo ser avaliada.

⚠ **Alerta de prova:** Criar regra de IP no firewall do Storage com o IP público da NAT Gateway das VMs da mesma região.
Como não cair: Regras de IP não afetam requisições da mesma região da conta. Use regra de rede virtual com ponto de extremidade de serviço ou ponto de extremidade privado.

⚠ **Alerta de prova:** Revogar uma SAS de conta vazada apagando uma política de acesso armazenada ou o repositório onde ela vazou.
Como não cair: Política armazenada só vale para SAS de serviço e apagar o repositório não invalida o token copiado. SAS de conta vazada se resolve girando a chave que a assinou.

⚠ **Alerta de prova:** Exigir só HTTPS na SAS ou restringir IP faz dela uma SAS revogável.
Como não cair: Restrição de IP, HTTPS e permissão mínima reduzem exposição, mas não revogam. Revogação sem troca de chave = SAS de serviço com política de acesso armazenada.

⚠ **Alerta de prova:** A regra de negação personalizada em 4096 fica abaixo das regras padrão e não afeta as sondas do Load Balancer.
Como não cair: Qualquer regra personalizada (100 a 4096) é avaliada antes das padrões (65000 em diante). Permita a marca AzureLoadBalancer (origem 168.63.129.16) com número menor que o da negação.

⚠ **Alerta de prova:** Permitir 443 para a marca Storage e confiar no DenyAllOutBound para bloquear o resto da internet.
Como não cair: AllowInternetOutBound (65001) vem antes de DenyAllOutBound (65500). Permita a marca regional (ex.: Storage.BrazilSouth) primeiro e crie negação explícita de Internet com número maior.

⚠ **Alerta de prova:** Proteger o SQL contra exfiltração negando acesso público e criando ponto de extremidade privado.
Como não cair: Isso protege a entrada. Para impedir que o próprio servidor envie dados a outras contas, use a restrição de rede de saída com os FQDNs de Storage permitidos.

⚠ **Alerta de prova:** Habilitar a auditoria no servidor e também em cada banco para garantir cobertura dos bancos novos.
Como não cair: A auditoria no servidor já cobre bancos futuros; com a mesma configuração nos dois níveis os eventos são gravados em duplicidade. Auditoria no banco só quando aquele banco precisa de destino ou retenção diferentes.

⚠ **Alerta de prova:** Usar Always Encrypted aleatório na coluna de CPF porque é mais forte.
Como não cair: Sem enclaves seguros, a criptografia aleatória não permite busca por igualdade. Busca exata por CPF pede criptografia determinística.

⚠ **Alerta de prova:** Para ativar autenticação somente Microsoft Entra, primeiro excluir os logins SQL.
Como não cair: Os logins SQL podem continuar existindo, apenas ficam bloqueados. O pré-requisito é ter um administrador do Microsoft Entra definido no servidor.

⚠ **Alerta de prova:** Dar Storage Blob Data Reader ao analista e restringir uma pasta pela ACL do ADLS Gen2.
Como não cair: RBAC é avaliado antes da ACL; se a função de dados concede acesso amplo, a ACL não é consultada. Para granularidade por pasta, não dê função de dados ampla.

⚠ **Alerta de prova:** Habilitar a criptografia de infraestrutura depois, quando a chave do cliente estiver pronta.
Como não cair: A dupla criptografia só é definida na criação da conta; depois seria preciso nova conta e migração. Na criação, a CMK usa identidade atribuída pelo usuário.

⚠ **Alerta de prova:** Remover o certificado raiz do gateway P2S para bloquear um notebook roubado.
Como não cair: Remover a raiz derruba todos os certificados emitidos por ela. Adicione a impressão digital do certificado do cliente à lista de revogados.

⚠ **Alerta de prova:** Criar logs de fluxo de NSG pelo PowerShell porque o portal não deixa.
Como não cair: Logs de fluxo de NSG não aceitam novas criações e serão aposentados em 30/09/2027. Use logs de fluxo de rede virtual com análise de tráfego.

Como cai na prova

📝 **Como cai:** Cenário de Storage com requisitos de acesso a parceiros e uma restrição (sem trocar chave, sem chave da conta, só alguns blobs).
Como resolver: Identifique quem assina o token: chave da conta (conta/serviço) ou Entra (delegação). Depois veja o requisito de revogação (política armazenada só em SAS de serviço) ou granularidade (ABAC com tag de índice). Descarte alternativas que dependem da chave quando o enunciado quer eliminá-la.

📝 **Como cai:** Tráfego bloqueado ou liberado inesperadamente com NSG ou Azure Firewall, pedindo a causa.
Como resolver: Aplique a ordem: no NSG, menor número primeiro e sub-rede antes da NIC na entrada; no Firewall, tipo de regra (rede antes de aplicativo) e pai antes da filha. A causa quase sempre é a ordem, não um prazo de propagação.

📝 **Como cai:** Ponto de extremidade privado criado, mas o acesso não funciona.
Como resolver: Verifique na sequência: DNS (zona privatelink vinculada; on-premises com encaminhador condicional para o resolvedor), subrecurso correto (blob e dfs), estado da conexão (Pending de aprovação em outro locatário) e políticas de rede da sub-rede se NSG/UDR devem valer.

📝 **Como cai:** Escolher o recurso do Network Watcher para um diagnóstico.
Como resolver: Leia o verbo: descobrir a regra que bloqueia (verificação de fluxo IP), ver a rota (próximo salto), listar o que vale na NIC (regras efetivas), medir latência contínua (monitor de conexão), registrar fluxos reais (logs de fluxo de VNet).

📝 **Como cai:** Escolha DUAS ou TRÊS sobre requisitos de um recurso (Private Link service, TDE com CMK, VPN ativo-ativo).
Como resolver: Liste os pré-requisitos obrigatórios e descarte os que são boa prática opcional (HSM, rotação automática, rede do cofre) ou SKU errado (Basic).

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
revogar SAS sem trocar a chave da conta	**SAS de serviço vinculada a política de acesso armazenada**
token ligado à identidade do Entra, sem chave da conta, validade curta	**SAS de delegação de usuário (máximo 7 dias)**
esconder o dado do DBA / db_owner	**Always Encrypted (determinística se houver busca por igualdade)**
um parceiro com IP fixo deve acessar só um banco do servidor	**Regra de firewall no nível do banco com sp_set_database_firewall_rule**
auditoria do SQL para SIEM de terceiros em streaming	**Event Hubs**
nome do PaaS ainda resolve para o IP público após criar o ponto privado	**Zona DNS privada privatelink vinculada à VNet**
ADLS Gen2: leitura funciona, criar diretório ou ACL falha via ponto privado	**Falta ponto de extremidade privado do subrecurso dfs**
regra por camada (web, app, banco) sem depender de IP	**Grupos de segurança de aplicativo como origem e destino no NSG**
bloquear em todas as VNets sem que o NSG das equipes consiga liberar	**Regra de administrador de segurança Deny no Virtual Network Manager**
filtrar caminho de URL ou inspecionar HTTPS / IDPS	**Azure Firewall Premium com inspeção TLS**
FQDN em regra de rede do Azure Firewall	**Proxy DNS ligado e VNets usando o IP privado do firewall como DNS**
hub da Virtual WAN inspecionando tráfego privado e internet	**Hub protegido + intenção de roteamento (WAN Standard)**
endereços sobrepostos entre rede local e VNet em VPN S2S	**Regras de NAT no VPN Gateway (IngressSNAT/EgressSNAT)**
tráfego não chega ao NVA; resultado System Route	**Próximo salto do Network Watcher: falta UDR 0.0.0.0/0 associada à sub-rede**

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

- Ordem decide: NSG por número (menor primeiro) e sub-rede antes da NIC na entrada; Azure Firewall por tipo (DNAT, rede, aplicativo) e pai antes da filha.
- Política de acesso armazenada só funciona com SAS de serviço; SAS de conta vazada se resolve girando a chave.
- Regras de IP do Storage e do Key Vault aceitam só IPs públicos e, no Storage, não valem para a mesma região.
- Ponto de extremidade privado sem zona privatelink vinculada continua resolvendo para o IP público.
- Inspeção TLS, IDPS e URL completa são Premium; inteligência contra ameaças que nega já existe no Standard.

Essenciais para a prova (checklist)

☐ Sei qual tipo de SAS é assinado com a chave da conta e qual com o Microsoft Entra, e como revogar cada um.

☐ Sei configurar o firewall do Storage com regra de IP, regra de rede virtual, regra de instância de recurso e serviços confiáveis.

☐ Sei diferenciar ponto de extremidade privado, de serviço e política de ponto de extremidade de serviço.

☐ Sei resolver DNS de ponto de extremidade privado dentro da VNet e a partir do on-premises.

☐ Sei escolher entre Always Encrypted, mascaramento dinâmico e TDE com CMK, e os requisitos do cofre para TDE.

☐ Sei configurar auditoria do Azure SQL e da Managed Instance para Storage, Log Analytics e Event Hubs.

☐ Sei calcular o resultado de regras de NSG com prioridades, regras padrão e NSGs na sub-rede e na NIC.

☐ Sei o que cada SKU do Azure Firewall oferece e a ordem de processamento das regras.

☐ Sei configurar Virtual WAN com hub protegido, VPN ativo-ativo, NAT e P2S com Entra ID.

☐ Sei qual ferramenta do Network Watcher usar para cada diagnóstico.

Questões de revisão do capítulo

R4.1 · Proteger armazenamento, bancos de dados e redes

No data lake da Agro Analytics (ADLS Gen2), a equipe removeu da ACL do diretório /financeiro a permissão de leitura de um analista, mas ele continua lendo os arquivos. Ele tem a função Storage Blob Data Reader na conta. Qual é a causa?

A. A ACL padrão do diretório pai sobrescreve a ACL de acesso definida no diretório filho
B. As ACLs POSIX se aplicam a arquivos, e não a diretórios, no Data Lake Storage Gen2
C. As alterações de ACL levam 24 horas para propagar em contas com namespace hierárquico
D. A atribuição RBAC é avaliada antes e, quando concede o acesso, as ACLs não são consultadas

R4.2 · Proteger armazenamento, bancos de dados e redes

A Gráfica Ipiranga entrega SAS a parceiros para baixar arquivos de um contêiner. Depois que um SAS vazou, a equipe percebeu que só conseguiria invalidá-lo rotacionando a chave da conta, o que derrubou outros sistemas. Que abordagem permitiria revogar SAS emitidos sem trocar a chave?

A. SAS de conta vinculados a uma política de acesso armazenada na própria conta
B. SAS de conta com restrição de IP de origem e protocolo exigindo HTTPS
C. SAS de serviço vinculados a uma política de acesso armazenada no contêiner
D. SAS de serviço com permissão de leitura e validade de um ano inteiro

R4.3 · Proteger armazenamento, bancos de dados e redes

Uma indústria acessa, a partir do data center on-premises conectado por ExpressRoute, um Azure SQL Database com ponto de extremidade privado. A zona privatelink.database.windows.net está vinculada à VNet do hub, onde há um Azure DNS Private Resolver. Os servidores on-premises ainda resolvem o IP público. Qual configuração corrige?

A. Encaminhador condicional de privatelink.database.windows.net no DNS local para o IP 168.63.129.16
B. Configurar os servidores DNS da VNet do hub com o IP do ponto de extremidade de entrada
C. Encaminhador condicional de database.windows.net no DNS local para o ponto de extremidade de entrada do resolvedor
D. Ponto de extremidade de saída do resolvedor com conjunto de regras de encaminhamento para o DNS local

R4.4 · Proteger armazenamento, bancos de dados e redes

O e-commerce Mercado Fácil tem VMs das camadas web, aplicação e banco em uma mesma VNet, com escala automática que muda os IPs o tempo todo. A equipe quer regras de NSG que permitam a porta 443 da camada web para a de aplicação sem depender de endereços IP. Qual recurso usar?

A. Regras de administrador de segurança do Virtual Network Manager com os IPs de cada VM
B. Marca de serviço VirtualNetwork usada como origem e destino nas regras do NSG associado à sub-rede
C. Grupos de segurança de aplicativo por camada, usados como origem e destino nas regras do NSG
D. Um NSG separado por VM, com regras atualizadas por script a cada evento de escala automática

Respostas comentadas

R4.1. D) A atribuição RBAC é avaliada antes e, quando concede o acesso, as ACLs não são consultadas

Por quê: No Data Lake Storage Gen2, a ordem é RBAC, depois ABAC, depois ACL; para controle fino por diretório, a função RBAC não pode já conceder o acesso amplo.

✗ A) Incorreta. A ACL padrão só é herdada por itens criados depois; ela não sobrescreve a ACL de acesso.
✗ B) Incorreta. ACLs se aplicam a diretórios e arquivos.
✗ C) Incorreta. Não há esse prazo de propagação; a causa é a ordem de avaliação.

> **Dica de prova:** ADLS Gen2: RBAC vence antes da ACL; para granularidade por pasta, não dê função de dados ampla.

R4.2. C) SAS de serviço vinculados a uma política de acesso armazenada no contêiner

Por quê: A política de acesso armazenada fica no contêiner, fila, tabela ou compartilhamento (até cinco por recurso) e serve para SAS de serviço; mudar ou apagar a política revoga os SAS ligados a ela.

✗ A) Incorreta. Políticas de acesso armazenadas não são suportadas para SAS de conta (nem para SAS de delegação de usuário).
✗ B) Incorreta. Restrições de IP e HTTPS reduzem o uso indevido, mas não oferecem forma de revogar o SAS emitido.
✗ D) Incorreta. Restringir permissão ajuda, mas um SAS avulso de um ano continua válido e só seria revogado com troca de chave.

> **Dica de prova:** Revogar SAS sem trocar chave = política de acesso armazenada (vale para SAS de serviço).

R4.3. C) Encaminhador condicional de database.windows.net no DNS local para o ponto de extremidade de entrada do resolvedor

Por quê: Para clientes on-premises resolverem pontos de extremidade privados, o DNS local usa um encaminhador condicional da zona pública do serviço (por exemplo, database.windows.net) para o ponto de extremidade de entrada do Azure DNS Private Resolver, em uma VNet vinculada à zona privatelink.

✗ A) Incorreta. O IP 168.63.129.16 só é alcançável de dentro do Azure, e o encaminhamento deve ser da zona pública, não da privatelink.

✗ B) Incorreta. Alterar o DNS da VNet não ajuda os clientes on-premises, que continuam consultando o DNS local sem encaminhamento.

✗ D) Incorreta. O ponto de extremidade de saída atende consultas do Azure para o ambiente local, o sentido oposto ao necessário.

> **Dica de prova:** On-premises para ponto de extremidade privado: encaminhador condicional da zona pública para o endpoint de entrada do resolvedor.

R4.4. C) Grupos de segurança de aplicativo por camada, usados como origem e destino nas regras do NSG

Por quê: Grupos de segurança de aplicativo permitem escrever regras de NSG por função da carga (web, app, banco) em vez de endereços explícitos.

✗ A) Incorreta. Continuaria dependendo de IPs, que mudam a cada escala.

✗ B) Incorreta. VirtualNetwork abrange todo o espaço da VNet e pares, permitindo bem mais do que web para aplicação.

✗ D) Incorreta. Scripts por evento de escala são frágeis e não resolvem a dependência de IP.

> **Dica de prova:** Regra por camada sem IP fixo = ASG como origem/destino na regra de NSG (NICs na mesma VNet).

DIA DA PROVA

Estratégia de prova

O SC-500 tem 120 minutos, questões de múltipla escolha e de múltipla resposta (Escolha DUAS ou TRÊS) e aprova com 700 em uma escala de 1 a 1000; a Microsoft não divulga a quantidade exata de questões. Quase toda questão é um cenário de empresa com um requisito principal e uma restrição (menor privilégio, sem chave, sem agente, sem IP público, inclusive recursos futuros). As alternativas erradas costumam ser recursos reais que resolvem um problema vizinho, usam o SKU ou plano errado ou citam recursos aposentados ou com aposentadoria anunciada, como o agente do Log Analytics, o Qualys integrado, o Azure Disk Encryption (15/09/2028) e os logs de fluxo de NSG (30/09/2027). O exame substituiu o AZ-500 e cobra o portfólio atual, incluindo segurança de cargas de IA dentro do domínio de computação.

Como responder

✓ Sublinhe a restrição do enunciado (menor privilégio, sem trocar chave, inclusive futuros, sem agente, sem IP público) antes de ler as alternativas; ela elimina metade das opções.

✓ Em questões de múltipla resposta, avalie cada alternativa como verdadeira ou falsa isoladamente e marque exatamente a quantidade pedida.

✓ Quando duas alternativas usam o mesmo produto, compare plano e SKU: Plano 1 x Plano 2, Foundational x Defender CSPM, Basic x Standard x Premium.

✓ Descarte alternativas que dependem de recursos aposentados (agente do Log Analytics, Qualys integrado, monitor de conexão clássico, logs de fluxo de NSG novos).

✓ Para menor privilégio, escolha a função mais estreita que contém a ação e o menor escopo; desconfie de Owner, Contributor e funções Officer.

✓ Em cenários de bloqueio inesperado, aplique a ordem de avaliação (NSG, Azure Firewall, RBAC antes de ACL, regras de automação) antes de pensar em atrasos de propagação.

✓ Separe plano de controle de plano de dados: bloqueios, Contributor e log de atividades não alcançam blobs, segredos lidos nem dados do banco.

✓ Administre os 120 minutos: marque para revisão as questões longas de várias etapas e volte a elas depois de garantir as diretas.

Erros que derrubam candidatos

✗ Escolher o recurso que protege a entrada quando o requisito é a saída (ou o contrário), como ponto de extremidade privado para evitar exfiltração do SQL.

✗ Confundir plano gratuito com pago no Defender for Cloud e recursos do Plano 1 com os do Plano 2 do Defender for Servers.

✗ Achar que NotActions nega, que bloqueio protege dados e que exp de segredo impede a leitura.

✗ Ignorar a ordem de avaliação de NSG e Azure Firewall e cair na alternativa que inventa prazo de propagação.

✗ Esquecer que alguns ajustes só existem na criação do recurso (dupla criptografia do Storage, retenção do Key Vault, Bastion private-only, criptografia de disco confidencial).

✗ Usar MFA como controle para identidades de agente, que só podem ser bloqueadas no acesso condicional.

✗ Mandar eventos para a tabela errada no Sentinel e não perceber que as regras consultam outra tabela.

Na semana da prova

- ☐ Revise as listas de lembrar de cada domínio e as tabelas de SKUs (Azure Firewall, Bastion, Defender for Servers, CSPM).
- ☐ Dê prioridade ao domínio de maior peso, Proteger armazenamento, bancos de dados e redes (25-30%): SAS, firewall do Storage, DNS de ponto de extremidade privado, NSG e Azure Firewall.
- ☐ Monte de memória as ordens de avaliação (NSG, Azure Firewall, ADLS Gen2, regras de automação) e confira.
- ☐ Revise as funções de menor privilégio do Key Vault, do Sentinel, do Security Copilot e de identidades gerenciadas.
- ☐ Na véspera, revise só os números e prazos (retenções, limites e datas de aposentadoria) e descanse.
- ☐ No dia, leia cada enunciado até o fim antes de olhar as alternativas e guarde tempo para revisar as marcadas.

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 e monitorar a postura de segurança

‣ VM exposta + vulnerável + com permissão em Storage, consulta em grafo → **Explorador de segurança na nuvem (Defender CSPM)**

‣ rota explorável até dados confidenciais para priorizar correção → **Análise de caminho de ataque (Defender CSPM + varredura sem agente)**

‣ colunas de risco embaçadas nas recomendações → **Habilitar o Defender CSPM**

‣ dados do Defender for Cloud para SIEM externo → **Exportação contínua para Event Hubs (streaming e snapshots semanais)**

‣ dono e prazo automáticos para recomendações → **Regra de governança**

⚠ Governança, caminhos de ataque, explorador e nível de risco exigem Defender CSPM; o gratuito tem secure score, recomendações, automação e exportação.

⚠ Enforce usa DeployIfNotExists e corrige na criação; para barrar, defina o efeito Deny em Políticas de segurança.

⚠ Soluções trazem modelos; é preciso criar as regras de análise a partir deles. Atualizar a solução também não altera regras existentes.

2. Gerenciar identidade, acesso e governança

‣ primeiro acesso sem senha, registrar passkey no primeiro dia → **Temporary Access Pass emitido por Administrador de Autenticação**

‣ aprovação, justificativa e MFA na ativação de função → **Configurações da função no PIM (atribuição qualificada)**

‣ acesso revogado quase em tempo real após desabilitar conta → **Avaliação contínua de acesso (CAE)**

‣ medir impacto antes de impor e não perder acesso administrativo → **Somente relatório + What If + excluir contas de emergência**

‣ usuário pode consentir só apps de baixo risco → **Editores verificados + permissões delegadas classificadas como de baixo impacto**

⚠ Permissões são aditivas e NotActions só subtrai daquela função. Negar de verdade exige atribuição de negação, criada por deployment stack com deny settings ou aplicativo gerenciado.

⚠ Bloqueios atuam só no plano de controle; gravar e excluir blobs continua possível. Já o ReadOnly quebra listKeys e a criação de atribuições de função.

⚠ Para segredos, exp e nbf são informativos e o get continua funcionando. Use enabled = false para bloquear mantendo a versão.

3. Proteger a computação

‣ token do Microsoft Entra no APIM, só de aplicativos específicos → **validate-azure-ad-token com client-application-ids**

‣ uma equipe consumiu a cota de tokens do modelo → **llm-token-limit inbound com counter-key da assinatura**

‣ porta 3389 fechada por padrão e aberta sob demanda → **JIT do Defender for Servers Plano 2**

‣ proibido instalar agente, mas quer vulnerabilidades e segredos dos discos → **Varredura sem agente (instantâneos de disco)**

‣ EC2 não vira servidor do Arc / Compute Engine não vira servidor do Arc → **SSM Agent com AmazonSSMManagedInstanceCore / agente OS Config**

⚠ Os dois planos incluem a integração com o Defender for Endpoint, provisionada como extensão MDE. O Plano 2 só acrescenta FIM, JIT, varredura sem agente e recursos premium.

⚠ JIT é do Plano 2, usa NSG ou DNAT no Azure Firewall e não suporta firewalls gerenciados pelo Firewall Manager nem VMs clássicas.

⚠ Nada é instalado; ela analisa instantâneos dos discos. Discos com CMK são suportados com permissões de chave no Key Vault.

4. Proteger armazenamento, bancos de dados e redes

‣ revogar SAS sem trocar a chave da conta → **SAS de serviço vinculada a política de acesso armazenada**

‣ token ligado à identidade do Entra, sem chave da conta, validade curta → **SAS de delegação de usuário (máximo 7 dias)**

‣ esconder o dado do DBA / db_owner → **Always Encrypted (determinística se houver busca por igualdade)**

‣ um parceiro com IP fixo deve acessar só um banco do servidor → **Regra de firewall no nível do banco com sp_set_database_firewall_rule**

▸ auditoria do SQL para SIEM de terceiros em streaming → **Event Hubs**

⚠ No Azure Firewall o tipo vem antes do número: DNAT, depois rede, depois aplicativo. Uma regra de rede permissiva libera o tráfego antes de a regra de aplicativo ser avaliada.

⚠ Regras de IP não afetam requisições da mesma região da conta. Use regra de rede virtual com ponto de extremidade de serviço ou ponto de extremidade privado.

⚠ Política armazenada só vale para SAS de serviço e apagar o repositório não invalida o token copiado. SAS de conta vazada se resolve girando a chave que a assinou.

GABARITO

Respostas do diagnóstico

D1. B) Um owner define, nas configurações de plug-ins, a disponibilidade dos pré-instalados como só para owners → revise o capítulo 1

Por quê: Nas configurações de plug-ins do Security Copilot, owners decidem se os plug-ins pré-instalados ficam disponíveis a todos os usuários ou só a owners, e quem pode adicionar plug-ins personalizados. Quando restritos, novos plug-ins pré-instalados também passam a ser só para owners.

✗ A) Incorreta. A escolha individual de um contribuidor não impõe restrição para os outros usuários.
✗ C) Incorreta. Funções na capacidade do Azure tratam de gestão de cobrança e unidades, não da disponibilidade de plug-ins.
✗ D) Incorreta. Funções do Entra controlam acesso a dados dos serviços; não restringem quais plug-ins do Copilot ficam disponíveis.

> **Dica de prova:** Restringir plug-ins da Microsoft no Security Copilot = configuração de owner, disponibilidade só para owners.

D2. D) Workspaces separados em cada região exigida, já que o workspace fica ligado à região onde foi criado → revise o capítulo 1

Por quê: A recomendação é começar com um workspace e criar outros só quando houver motivo, como residência de dados, vários locatários, separação de cobrança ou controle granular.

✗ A) Incorreta. RBAC de contexto de recurso controla quem vê o quê, mas os dados brasileiros ficariam na Alemanha.
✗ B) Incorreta. Retenção por tabela muda o tempo de guarda, não a região onde os dados ficam.
✗ C) Incorreta. Dividir por equipe ignora o requisito de residência e multiplica workspaces sem necessidade.

> **Dica de prova:** Residência de dados por país = um workspace por região exigida.

D3. A) A pasta de trabalho Compliance Over Time da galeria do Defender for Cloud → revise o capítulo 1

Por quê: O Defender for Cloud traz pastas de trabalho prontas do Azure Monitor. A Compliance Over Time mostra a evolução da conformidade com os padrões escolhidos no painel de conformidade regulatória, permite descer até controles e recomendações e exportar cada painel para Excel.

✗ B) Incorreta. A página de conformidade do Azure Policy mostra o estado atual das atribuições, sem a evolução por padrão regulatório.
✗ C) Incorreta. Essa pasta de trabalho acompanha a pontuação de segurança, não a conformidade com padrões regulatórios.
✗ D) Incorreta. Relatórios de auditoria são certificações da própria Microsoft (SOC, ISO), não a conformidade dos recursos do cliente.

> **Dica de prova:** Evolução da conformidade = pasta de trabalho Compliance Over Time.

D4. B) Temporary Access Pass, emitido por um Administrador de Autenticação → revise o capítulo 2

Por quê: O Temporary Access Pass (TAP) é habilitado na política de métodos de autenticação e permite o primeiro login para registrar métodos sem senha, como passkeys. Tem vida útil configurável (de 10 minutos a 30 dias), pode ser de uso único e cada usuário tem um TAP por vez.

✗ A) Incorreta. O Administrador de Usuários não cria Temporary Access Pass; quem cria são o Administrador de Autenticação (para membros) e o Administrador de Autenticação Privilegiada.

✗ C) Incorreta. Uma senha temporária leva o colaborador a criar uma senha permanente, o contrário do objetivo de começar sem senha.

✗ D) Incorreta. Senha de aplicativo serve a clientes legados que não suportam MFA; não permite login no navegador nem registro de passkey.

> **Dica de prova:** Integrar usuário direto em sem senha = Temporary Access Pass.

D5. D) Uma entidade de serviço, em Aplicativos empresariais; o objeto de aplicativo fica no locatário da Nimbus → revise o capítulo 2

Por quê: Um aplicativo tem um objeto de aplicativo (o modelo global, em Registros de aplicativo) no locatário de origem e uma entidade de serviço em cada locatário em que é usado (Aplicativos empresariais). Políticas, consentimentos e atribuições locais ficam na entidade de serviço.

✗ A) Incorreta. O consentimento cria a entidade de serviço no locatário do cliente, onde ficam as permissões concedidas e as atribuições.

✗ B) Incorreta. Identidades gerenciadas representam recursos do Azure; aplicativos multilocatário são representados por entidades de serviço do tipo aplicativo.

✗ C) Incorreta. O objeto de aplicativo não é copiado para os locatários consumidores, e os segredos ficam no registro do locatário de origem.

> **Dica de prova:** Registro de aplicativo = objeto global no locatário de origem; aplicativo empresarial = entidade de serviço em cada locatário.

D6. C) Na opção Baixar relatório do painel de conformidade regulatória e na guia Relatórios de auditoria → revise o capítulo 2

Por quê: O painel de conformidade regulatória permite baixar o relatório de cada padrão atribuído e acessar relatórios de auditoria das certificações da Microsoft; padrões além do MCSB exigem ao menos um plano pago.

✗ A) Incorreta. Exportação contínua envia dados para análise, mas não gera o relatório formal nem os atestados da Microsoft.

✗ B) Incorreta. A pontuação segura e o Advisor não trazem o status por controle do PCI DSS nem os relatórios de certificação da Microsoft.

✗ D) Incorreta. Os relatórios de auditoria da Microsoft ficam disponíveis no próprio painel, sem chamado de suporte.

> **Dica de prova:** Evidência para auditor: Baixar relatório (status do padrão) + Relatórios de auditoria (certificações da Microsoft).

D7. A) Criptografia no host (encryption at host) → revise o capítulo 3

Por quê: A criptografia no host estende a criptografia do lado do servidor ao servidor físico que hospeda a VM: discos temporários e efêmeros são cifrados com chave da plataforma e os caches com a chave do disco (da plataforma ou do cliente). Exige registrar o recurso EncryptionAtHost e não pode ser ativada em VM que já usou Azure Disk Encryption.

✗ B) Incorreta. O Azure Disk Encryption usa dm-crypt dentro da VM, consome CPU e tem aposentadoria anunciada para 15/09/2028.

✗ C) Incorreta. A criptografia de disco confidencial exige VM confidencial; não está disponível para o tipo de segurança padrão.

✗ D) Incorreta. A SSE padrão criptografa os discos gerenciados em repouso no armazenamento, mas não cobre disco temporário nem cache no host.

> **Dica de prova:** Substituta do Azure Disk Encryption que cobre disco temporário e cache = criptografia no host.

D8. B) rate-limit-by-key por assinatura e ip-filter com action forbid → revise o capítulo 3

Por quê: rate-limit-by-key contém picos (excesso retorna 429), quota-by-key limita volume em períodos maiores (excesso retorna 403) e ip-filter permite ou bloqueia endereços em qualquer nível do APIM.

✗ A) Incorreta. quota-by-key controla volume total por período (mínimo de 300 segundos) e não está disponível nos níveis v2; allow liberaria o intervalo.

✗ C) Incorreta. Quota não serve para janelas curtas e validação de token não bloqueia o intervalo de IPs.

✗ D) Incorreta. validate-jwt valida tokens, não bloqueia IPs, e limitar pelo IP do gateway agruparia todos os chamadores.

> **Dica de prova:** Pico curto = rate-limit-by-key; volume no período = quota-by-key; bloquear IP = ip-filter forbid.

D9. A) Habilitar o Azure RBAC para autorização do Kubernetes e desabilitar as contas locais → revise o capítulo 3

Por quê: No AKS, a integração com o Microsoft Entra autentica usuários e o Azure RBAC para Kubernetes autoriza por funções do Azure, com escopo no cluster ou em namespaces. A opção disable-local-accounts remove o acesso por credenciais estáticas; em clusters existentes, convém girar os certificados depois.

✗ B) Incorreta. Intervalos de IP autorizados restringem a origem de rede das chamadas, mas não mudam o modelo de autorização nem removem credenciais locais.

✗ C) Incorreta. As credenciais --admin são estáticas e ignoram o Entra, exatamente o que a segurança quer impedir.

✗ D) Incorreta. RoleBindings manuais não usam atribuições do Azure, e manter contas locais preserva credenciais estáticas.

> **Dica de prova:** AKS sem credencial estática: Azure RBAC para Kubernetes + contas locais desabilitadas.

D10. B) Definir esses resultados como linha de base, que na configuração expressa vale na hora → revise o capítulo 4

Por quê: A linha de base da avaliação de vulnerabilidades é definida por regra e por banco; desvios futuros voltam a gerar achado. A configuração expressa suporta linha de base em lote e a partir do último resultado.

✗ A) Incorreta. Isentar o banco esconderia todos os achados, inclusive problemas reais.
✗ C) Incorreta. A configuração clássica também usa linha de base, só que ela vale a partir da próxima verificação.
✗ D) Incorreta. As regras da avaliação de vulnerabilidades não são gerenciadas por iniciativa do Azure Policy.

> **Dica de prova:** Achado aceito na VA do SQL = linha de base (expressa: efeito imediato).

D11. B) Uma regra de instância de recurso para esse workspace, mais uma função de dados para a identidade dele → revise o capítulo 4

Por quê: Regras de instância de recurso permitem que instâncias específicas de serviços do Azure atravessem o firewall do Armazenamento; a autorização aos dados continua vindo do RBAC da identidade gerenciada.

✗ A) Incorreta. A exceção de serviços confiáveis vale para o conjunto de serviços confiáveis, não para uma instância específica.
✗ C) Incorreta. As regras de IP do firewall do Armazenamento aceitam endereços e intervalos, não marcas de serviço.
✗ D) Incorreta. Política de acesso armazenada controla SAS de serviço; não é regra de rede nem identifica um workspace.

> **Dica de prova:** Firewall do Storage para um recurso específico de outro serviço = regra de instância de recurso + RBAC.

D12. A) Restringir a rede de saída do servidor e listar os FQDNs das contas de armazenamento permitidas → revise o capítulo 4

Por quê: A restrição de rede de saída do Azure SQL Database afeta recursos como auditoria, avaliação de vulnerabilidades, importação/exportação, OPENROWSET e BULK INSERT; não se aplica à SQL Managed Instance.

✗ B) Incorreta. Negar acesso público e usar ponto de extremidade privado protege a entrada, não a saída.
✗ C) Incorreta. Autenticação controla quem acessa, não os destinos de saída do servidor.
✗ D) Incorreta. Regras de entrada controlam quem conecta ao servidor, não para onde ele envia dados.

> **Dica de prova:** Evitar exfiltração pelo próprio servidor SQL = regras de firewall de saída com FQDNs permitidos.

Agora, treine no formato real

Faça as 6 provas completas do curso SC-500: 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.