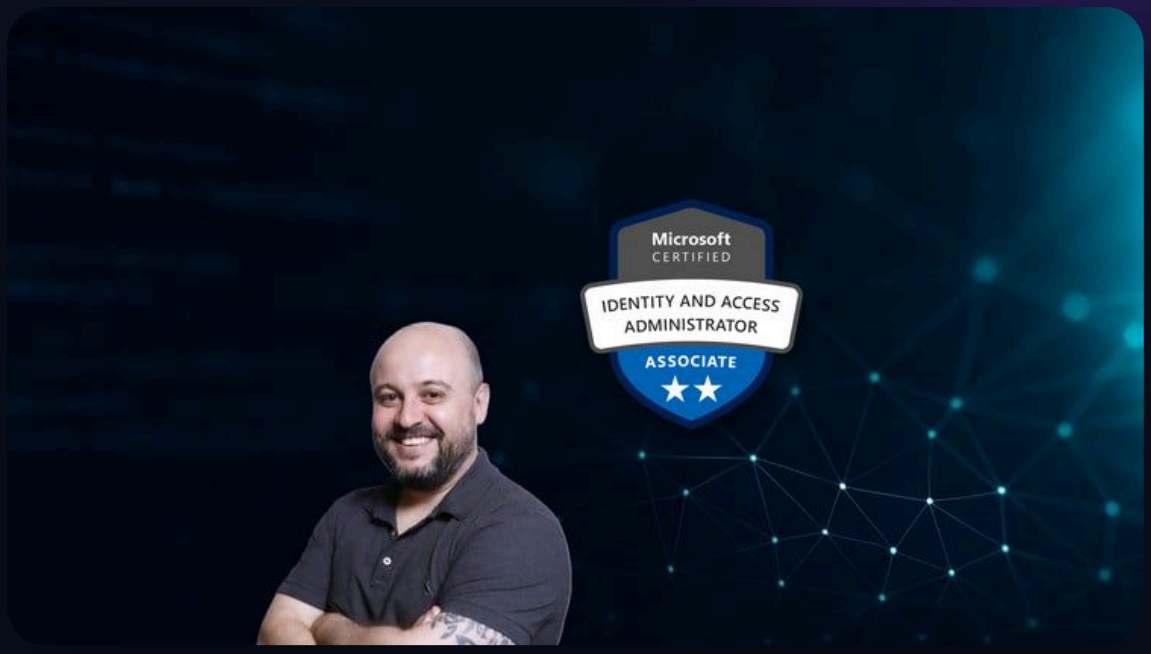
Strecht Simulados · Guia de preparação



Guia de preparação SC-300

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-300: o guia explica o que cai e onde estão as armadilhas; as provas treinam o ritmo e mostram o que você ainda não domina.

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

Mapa do exame

Cada prova do curso tem 50 questões e 100 minutos, no formato do exame. Referência de aprovação: 70%.

Domínio (capítulo)	Peso	Neste guia
1. Implementar e gerenciar identidades de usuários	20-25%	20 conceitos · 14 pegadinhas
2. Implementar o gerenciamento de autenticação e acesso	25-30%	19 conceitos · 14 pegadinhas
3. Planejar e automatizar a governança de identidade	20-25%	18 conceitos · 14 pegadinhas
4. Planejar e implementar identidades de carga de trabalho	20-25%	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 · Implementar e gerenciar identidades de usuários

A equipe de automação da Transportadora Rodovia Livre quer atribuir funções do Microsoft Entra por script nos pipelines e cogita usar a CLI do Azure, que já usa para recursos do Azure. O que a documentação informa?

A. A CLI do Azure não é suportada para atribuições de funções do Microsoft Entra
B. A CLI do Azure é o único método suportado para funções do Microsoft Entra
C. A CLI do Azure atribui funções do Entra desde que o usuário seja Owner da assinatura
D. A CLI do Azure atribui funções do Entra só no escopo de unidades administrativas

D2 · Implementar e gerenciar identidades de usuários

A equipe de identidade da Companhia Hidrelétrica Rio Forte usa o SSO contínuo e recebeu da auditoria a recomendação de reforçar a segurança da conta de computador que representa o Microsoft Entra ID no AD local. O que a documentação orienta?

A. Excluir a conta AZUREADSSOACC e recriá-la manualmente uma vez por ano no controlador de domínio local
B. Renovar a chave de descriptografia Kerberos com Update-AzureADSSOForest ao menos a cada 30 dias
C. Habilitar MFA por usuário na conta AZUREADSSOACC para proteger os tíquetes emitidos pelo AD
D. Mover a conta AZUREADSSOACC para uma unidade administrativa de gerenciamento restrito do Entra

D3 · Implementar e gerenciar identidades de usuários

A Seguradora Proteção Familiar quer que convites B2B só possam ser enviados para os domínios de três corretoras parceiras, bloqueando qualquer outro, inclusive provedores de e-mail pessoal. O que está correto ao configurar as restrições de colaboração?

A. Usar lista de permissão e lista de bloqueio ao mesmo tempo na mesma política
B. Usar lista de permissão com os três domínios; os demais ficam bloqueados
C. Usar lista de permissão no SharePoint, que vale também para convites do Microsoft Entra
D. Usar lista de bloqueio, que também remove convidados que já resgataram o convite

D4 · Implementar o gerenciamento de autenticação e acesso

A Transportadora Via Expressa quer migrar usuários que fazem MFA por SMS para notificações por push do Microsoft Authenticator, incentivando o registro durante a entrada. Qual pré-requisito a campanha de registro do Authenticator exige?

A. Política de registro de MFA do ID Protection habilitada para os usuários
B. Authenticator habilitado com modo Any ou Push e usuários no escopo do método
C. Licença P2 para cada usuário incluído na campanha de registro do Authenticator
D. Authenticator habilitado com modo Passwordless para todos os usuários-alvo

D5 · Implementar o gerenciamento de autenticação e acesso

A Universidade Estadual Campo Largo usa domínios federados com um IdP de terceiros. Um aluno perdeu o celular e precisa registrar uma passkey com um Temporary Access Pass. Como o TAP se comporta para domínios federados?

A. O TAP não funciona com domínios federados e exige converter o domínio para gerenciado
B. O TAP tem preferência sobre a federação, e o aluno autentica no Microsoft Entra ID
C. O TAP é redirecionado ao IdP federado, que valida o código antes de liberar o acesso
D. O TAP substitui a senha do aluno no IdP federado até o fim da validade definida

D6 · Implementar o gerenciamento de autenticação e acesso

Na Autarquia Previdenciária Futuro Seguro, os certificados dos cartões trazem no campo Principal Name o mesmo valor do UPN dos servidores. Ao configurar a CBA, como o Microsoft Entra ID identifica o usuário a partir do certificado por padrão?

A. Mapeando a data de validade do certificado para o employeeId do usuário
B. Mapeando o emissor do certificado para o atributo department do usuário
C. Mapeando o número de série do certificado para o objectId do usuário
D. Mapeando Principal Name para o userPrincipalName do usuário

D7 · Planejar e automatizar a governança de identidade

A equipe de segurança da Indústria Naval Proa quer investigar chamadas feitas ao Microsoft Graph por aplicativos no locatário, mas descobriu que não há dados desses logs no portal. A empresa tem P1. O que está correto sobre os logs de atividade do Microsoft Graph?

A. Estão disponíveis na edição Free por sete dias e na edição P1 por um ano no centro de administração
B. Só são retidos se integrados a armazenamento ou análise pelas configurações de diagnóstico
C. Ficam no log de auditoria do PIM, na aba Resource audit, junto com as ativações das funções privilegiadas
D. São retidos por 30 dias no portal com P1, sem nenhuma configuração adicional no locatário da empresa

D8 · Planejar e automatizar a governança de identidade

A analista da Construtora Eixo Norte quer, no Log Analytics, listar os aplicativos com mais entradas na última semana a partir dos logs do Microsoft Entra ID. Qual consulta KQL atende?

A. AuditLogs | where TimeGenerated >= ago(7d) | summarize auditCount = count() by OperationName | sort by auditCount desc
B. SigninLogs | where RiskState contains "atRisk" | project UserPrincipalName, AppDisplayName, RiskState
C. SigninLogs | where CreatedDateTime >= ago(7d) | summarize signInCount = count() by AppDisplayName | sort by signInCount desc
D. AADProvisioningLogs | where TimeGenerated > ago(7d) | summarize count() by Action, bin(TimeGenerated, 1d)

D9 · Planejar e automatizar a governança de identidade

O Banco Regional Campo Forte tem duas contas de acesso de emergência com chaves FIDO2. A auditoria quer saber como mantê-las confiáveis ao longo do tempo. Qual prática faz parte da orientação da Microsoft?

A. Registrar o MFA das contas no dispositivo de um único administrador de plantão
B. Incluir as contas em todas as políticas que exigem dispositivo compatível
C. Vincular cada conta ao celular pessoal do diretor de TI para receber códigos por SMS
D. Testar periodicamente se as contas entram e guardar as chaves em cofres separados

D10 · Planejar e implementar identidades de carga de trabalho

Na Cooperativa de Crédito Laço Forte, a equipe criou uma API de consulta de cooperados e quer que outros aplicativos clientes peçam a permissão delegada Cooperados.Read. O que configurar no registro da API?

A. Em Certificates & secrets, criar um segredo chamado Cooperados.Read na API
B. Em API permissions, adicionar Cooperados.Read como permissão do Microsoft Graph
C. Em App roles, criar a função Cooperados.Read com tipo de membro Applications
D. Em Expose an API, definir o URI de ID do aplicativo e adicionar o escopo

D11 · Planejar e implementar identidades de carga de trabalho

A Plataforma de Dados Clínicos Saúde Conectada expõe uma API com o escopo Prontuarios.ReadWrite.All, que dá acesso amplo a dados sensíveis. Como configurar quem pode consentir com esse escopo?

A. Definir Who can consent = Admins and users ao adicionar o escopo
B. Ativar Assignment required = No na entidade de serviço da API
C. Definir Who can consent = Admins only ao adicionar o escopo
D. Criar uma função de aplicativo com membros do tipo Users/Groups

D12 · Planejar e implementar identidades de carga de trabalho

A Universidade Integrada Novo Saber quer que alunos descubram no My Apps o aplicativo de biblioteca digital e solicitem acesso, com aprovação de um bibliotecário e não da TI. O que configurar e qual licença é necessária?

A. Self-service application access no aplicativo, com aprovadores de negócio, e P1 ou P2
B. Admin consent workflow com bibliotecários como revisores, e Workload Identities Premium
C. Assignment required = No no aplicativo, com coleção no My Apps, e licença Free
D. Pacote de acesso sem aprovação para todos os alunos, e licença do Defender for Cloud Apps

01

CAPÍTULO 1 · 20-25% DA PROVA

Implementar e gerenciar identidades de usuários

Aqui preciso dominar funções do Microsoft Entra (internas e personalizadas), unidades administrativas, domínios e configurações do locatário, usuários, grupos, licenças, dispositivos, colaboração externa B2B, acesso entre locatários e identidade híbrida (Connect Sync, Cloud Sync, PHS, PTA, SSO contínuo, Connect Health). A prova cobra limites e comportamentos padrão: 30 dias para restaurar, 50 dispositivos por usuário, 500 exclusões no Connect Sync, dois minutos da sincronização de hash. Erro bastante em entrada x saída nas configurações entre locatários, em B2B direct connect x sincronização entre locatários e em qual função redefine senha ou método de quem. Outra armadilha frequente é unidade administrativa: não aninha, e grupo dentro dela não traz os membros para o escopo.

Neste capítulo

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

Tópicos-chave

Funções do Entra x funções do Azure

São sistemas separados: função do Entra não dá acesso ao Azure e vice-versa. A exceção é a elevação de acesso: Global Administrator ativa Access management for Azure resources e recebe User Access Administrator na raiz. Atribuição = entidade de segurança + definição + escopo; por script, use centro de administração, Graph PowerShell ou API (a CLI do Azure não é suportada).

Funções personalizadas

Criadas a partir de permissões (registros de aplicativo, aplicativos empresariais, consentimento, dispositivos, usuários, grupos) por ao menos Privileged Role Administrator. Funções internas não podem ser clonadas nem editadas, e permissões do Entra não entram em funções personalizadas do Azure. Podem ser atribuídas no diretório ou num registro de aplicativo específico.

Funções de senha e autenticação

Helpdesk Administrator redefine senhas de não administradores e de algumas funções limitadas (e vê chaves do BitLocker). Authentication Administrator gerencia métodos de alguns usuários; Privileged Authentication Administrator de todos, inclusive administradores e membros de grupos atribuíveis a funções; Authentication Policy Administrator gerencia a política de métodos.

Grupos atribuíveis a funções

A propriedade isAssignableToRole só é definida na criação e não muda depois; grupo antigo precisa ser recriado. Exigem associação Assigned (sem dinâmica), não aceitam aninhamento e são criados por ao menos Privileged Role Administrator. Podem ser de segurança ou do Microsoft 365.

Unidades administrativas

Restringem o escopo de uma função a usuários, grupos e dispositivos; não podem ser aninhadas, mas um usuário pode estar em várias. Grupo na unidade permite gerenciar o grupo (nome e associação), não as propriedades dos membros; adicione os usuários diretamente. Unidades dinâmicas aceitam um só tipo (usuários ou dispositivos), nunca grupos, e exigem P1 por usuário membro.

Unidade administrativa de gerenciamento restrito

Só administradores atribuídos explicitamente no escopo dela alteram os objetos, até Global Administrators precisam se atribuir (auditável). Aceita usuários, dispositivos e grupos de segurança; não aceita grupos do Microsoft 365, de distribuição ou de segurança habilitados para e-mail. Não bloqueia operações em serviços como Exchange.

Permissões efetivas e inventário

Users > usuário > Assigned roles mostra todas as funções, inclusive via grupos atribuíveis e em outros escopos. Roles and administrators > All roles > Download assignments gera CSV de todas as atribuições ativas (operação em massa de até uma hora). Your Role mostra só as funções de quem está conectado.

Domínios personalizados

Verificação por registro TXT ou MX com os valores exibidos (TTL sugerido 3600); subdomínios do domínio verificado são verificados automaticamente. O domínio principal precisa ser verificado e não federado, e trocar o principal não muda UPNs existentes (Domain Name Administrator). A exclusão é bloqueada por usuários, grupos ou apps (app ID URI) que referenciam o domínio.

Configurações do locatário

Users can register applications = No + Application Developer libera registros só a alguns. Restrict non-admin users from creating tenants = Yes + Tenant Creator controla criação de locatários. Restrict access to Microsoft Entra admin center não é controle de segurança (PowerShell e Graph continuam). Em Group settings define-se se usuários criam grupos de segurança. Company branding (P1, Organizational Branding Administrator) aceita personalização por idioma do navegador.

Grupos dinâmicos e políticas de grupos do Microsoft 365

Grupo dinâmico calcula membros pela regra (sem inclusão manual), não mistura usuários e dispositivos e exige P1 por usuário único membro; dispositivos não exigem licença. Expiração: uma política para todos os grupos do Microsoft 365, renovação automática por atividade e restauração em até 30 dias. Política de nomenclatura: prefixo/sufixo como GRP_[Department], palavras bloqueadas, até 63 caracteres.

Atributos de segurança personalizados

Pares chave-valor em conjuntos, tipos booleano, inteiro ou cadeia, atribuídos a usuários e aplicativos empresariais e usados no ABAC do Azure. Attribute Definition Administrator define, Attribute Assignment Administrator atribui; Global Administrator não lê nem altera por padrão. Não são emitidos em tokens; no filtro para aplicativos do AC só funcionam atributos do tipo cadeia.

Operações em massa e restauração

Bulk create exige no CSV Name [displayName], User name [userPrincipalName] e Initial password [passwordProfile]; Bulk invite exige e-mail a convidar e URL de redirecionamento (ao menos User Administrator). Usuário excluído fica 30 dias em Deleted users; depois a exclusão é permanente e nem o suporte restaura.

Licenciamento baseado em grupo

Feito no Microsoft 365 admin center; não suporta grupos aninhados. Erros comuns: planos conflitantes (desabilite um plano ou remova a licença direta) e localização de uso ausente ou não suportada (corrija no usuário e reprocesse). Para mover entre grupos licenciados, adicione ao destino antes de remover da origem; desligue serviços com Turn apps and services on or off. Por script: Set-MgGroupLicense; licença herdada não sai com Set-MgUserLicense.

Identidades de dispositivo

Joined dispensa AD local; hybrid joined fica no domínio e registrado no Entra, precisa de linha de visão com DCs e descobre o locatário pelo SCP (Connect ou Cloud Sync); registered é BYOD. Limite padrão de 50 dispositivos joined ou registered por usuário. Se o MFA de registro for por Acesso Condicional (Register or join devices), deixe a opção de Device settings em No.

Administração de dispositivos

Microsoft Entra Joined Device Local Administrator vira admin local de todos os joined. Windows LAPS guarda a senha do admin local no Entra para joined e hybrid joined (não registered nem macOS), desde a edição Free, com recuperação delegável por função personalizada e unidade administrativa. Ver chave do BitLocker gera auditoria KeyManagement. Obsoletos: desabilitar antes de excluir; híbridos se tratam no AD local.

Colaboração externa B2B

Guest user access tem três níveis (igual a membro, limitado padrão, restrito ao próprio objeto). Guest invite settings define quem convida (Only users assigned to specific admin roles + Guest Inviter). Collaboration restrictions usa lista de permissão ou de bloqueio, nunca as duas (25 KB). Código de acesso único por e-mail atende quem não tem conta compatível; federação com Google atende Gmail; IdP SAML/WS-Fed atende parceiros sem Entra (domínio diferente exige TXT DirectFedAuthUrl).

Ciclo de vida de convidados

Redefinir o status de resgate troca o e-mail de entrada sem perder acessos (menor privilégio Helpdesk Administrator); o UPN não muda. Contas internas de parceiros viram B2B convidando a conta existente pela API de convite. UserType (Member ou Guest) é independente da origem: membro externo é B2B com UserType Member. External user leave settings exige informações de privacidade no locatário.

Acesso entre locatários e multilocatário

Entrada controla quem vem ao seu locatário; saída controla aonde seus usuários vão; configurações por organização prevalecem sobre as padrão. Trust settings de entrada aceitam MFA e dispositivo compatível do parceiro. B2B direct connect (canais compartilhados do Teams) vem bloqueado e precisa ser habilitado nos dois lados. Sincronização entre locatários é push da origem, com entrada permitida e resgate automático nos dois locatários, e só leva membros internos.

Identidade híbrida

PHS sincroniza a cada dois minutos, habilita detecção de credenciais vazadas (só vazamentos novos) e serve de backup da federação. PTA aplica políticas do AD na hora, sem senha na nuvem, com agentes só de saída. SSO contínuo usa a conta AZUREADSSOACC, cuja chave Kerberos se renova com Update-AzureADSSOForest ao menos a cada 30 dias. Staged rollout testa autenticação na nuvem com até 10 grupos por recurso, sem dinâmicos nem aninhados, temporariamente.

Connect Sync, Cloud Sync e Connect Health

Connect Sync combina filtros de domínio, UO e atributo com lógica E; a prevenção de exclusões acidentais para a exportação acima de 500 exclusões (ajustável por PowerShell); servidor em staging importa e sincroniza, mas não exporta nem sincroniza senhas. Cloud Sync atende florestas desconectadas com vários agentes, provisiona grupos da nuvem para o AD e sincroniza computadores. Connect Health exige agente em cada servidor (AD FS e WAP) e P1 ou P2.

Macetes para memorizar

Entra x Azure

Dois reinos, uma ponte: só o Global Administrator eleva para User Access Administrator na raiz.

Unidades administrativas

UA não tem filho; grupo dentro não traz os membros junto.

Entrada x saída

Entrada é quem chega na minha casa; saída é aonde minha gente vai.

Google

Gmail = federação Google; Workspace com domínio = SAML/WS-Fed.

Números da identidade híbrida

Hash a cada 2 minutos, exclusão trava em 500, chave do SSO contínuo a cada 30 dias, staged rollout com 10 grupos.

Licença por grupo

Entra no novo, depois sai do velho; licença herdada sai saindo do grupo.

Restaurações

Usuário, registro de aplicativo e grupo do Microsoft 365: 30 dias para voltar.

Tabela de memorização: não confunda

Quando é...	...e quando é
Configurações de entrada Controlar usuários externos que acessam o seu locatário (e confiar no MFA ou dispositivo deles).	**Configurações de saída** Impedir seus usuários de colaborar no locatário de outra organização.
B2B direct connect Canais compartilhados do Teams sem criar convidados; habilitado nos dois lados.	**Sincronização entre locatários** Criar, atualizar e remover automaticamente usuários B2B no locatário de destino, sem convites.
Federação com Google Convidados com contas do Gmail.	**Federação com IdP SAML/WS-Fed** Parceiros com IdP próprio sem Microsoft Entra ID, inclusive Google Workspace com domínio próprio.
Sincronização de hash de senha Autenticação na nuvem simples, detecção de credenciais vazadas e backup da federação.	**Autenticação de passagem** Políticas de senha e bloqueio do AD aplicadas a cada entrada, sem hash na nuvem.
Connect Sync Sincronizador completo com filtros por domínio, UO e atributo e servidor em staging.	**Cloud Sync** Florestas desconectadas, infraestrutura mínima com vários agentes e provisionamento de grupos para o AD.
Unidade administrativa comum Delegar administração de um recorte da organização.	**Unidade de gerenciamento restrito** Blindar objetos até de administradores com escopo de locatário.
Authentication Administrator Gerenciar métodos de usuários comuns e alguns administradores.	**Privileged Authentication Administrator** Gerenciar métodos de todos, inclusive Global Administrators.

Números que caem

Item	Valor
Dispositivos por usuário (joined ou registered)	**Padrão 50, ajustável até 100 ou ilimitado**
Prevenção de exclusões acidentais no Connect Sync	**500 exclusões pendentes, ajustável**
Ciclo da sincronização de hash de senha	**A cada dois minutos**

Renovação da chave Kerberos do SSO contínuo	**Ao menos a cada 30 dias**
Staged rollout	**Até 10 grupos por recurso; 200 usuários ao adicionar um grupo pela primeira vez**
Restauração de usuário excluído	**30 dias em Deleted users**
Grupos do Microsoft 365 expirados	**Restauração em até 30 dias; renovação por atividade cerca de 35 dias antes**
Política de nomenclatura de grupos	**Prefixo, nome e sufixo até 63 caracteres**
Política de restrição de colaboração	**Uma por organização, até 25 KB**
Painel de migração de apps do AD FS	**Só apps com logins nos últimos 30 dias**
TTL sugerido no registro de verificação de domínio	**3600 segundos**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Dar Privileged Role Administrator para o Global Administrator recuperar uma assinatura do Azure.
Como não cair: Funções do Entra não concedem acesso ao Azure; use a elevação de acesso (User Access Administrator na raiz).

⚠ **Alerta de prova:** Clonar a função interna Application Administrator e remover permissões.
Como não cair: Funções internas não são clonadas nem editadas; crie função personalizada a partir das permissões.

⚠ **Alerta de prova:** Criar unidade administrativa filha ou incluir unidades como membros de outra.
Como não cair: Unidades administrativas não aninham; crie uma por recorte e atribua os escopos.

⚠ **Alerta de prova:** Colocar só o grupo na unidade e esperar gerenciar a senha dos membros.
Como não cair: Grupo na unidade só permite gerenciar o grupo; adicione os usuários diretamente.

⚠ **Alerta de prova:** Converter um grupo existente em atribuível a funções ou torná-lo dinâmico.
Como não cair: isAssignableToRole só na criação e exige associação Assigned; crie um grupo novo.

⚠ **Alerta de prova:** Considerar Restrict access to Microsoft Entra admin center um bloqueio de leitura do diretório.
Como não cair: Ela só esconde páginas do portal; PowerShell, Graph e links diretos continuam.

⚠ **Alerta de prova:** Bloquear a colaboração com uma concorrente nas configurações de entrada ou na lista de domínios.
Como não cair: Para impedir seus usuários de irem até ela, use configurações de saída da colaboração B2B para a organização.

⚠ **Alerta de prova:** Usar federação SAML/WS-Fed entre locatários do Microsoft Entra.
Como não cair: Não é suportada nem recomendada; entre locatários Entra use B2B, direct connect, sincronização ou organização multilocatário.

⚠ **Alerta de prova:** Achar que a sincronização entre locatários é pull do destino e leva os convidados da origem.
Como não cair: É push configurado na origem, com resgate automático nos dois lados, e não sincroniza usuários externos.

⚠ **Alerta de prova:** Remover do grupo licenciado de origem antes de adicionar ao de destino.
Como não cair: Adicione ao destino, confirme a licença e só então remova, para não perder acesso.

⚠ **Alerta de prova:** Remover licença herdada de grupo com Set-MgUserLicense.
Como não cair: Licença herdada só sai removendo o usuário do grupo licenciado.

⚠ **Alerta de prova:** Usar federação com Google para domínios do Google Workspace.
Como não cair: A federação com Google é para Gmail; domínio próprio usa federação SAML/WS-Fed.

⚠ **Alerta de prova:** Manter o staged rollout permanente com grupos dinâmicos ou aninhados.
Como não cair: O recurso é temporário, até 10 grupos por recurso, sem dinâmicos nem aninhados, e o AD FS fica ativo nos testes.

⚠ **Alerta de prova:** Achar que o servidor em staging assume sozinho ou exporta em paralelo.
Como não cair: Ele importa e sincroniza, mas não exporta nem sincroniza senhas; a troca é manual, desabilitando o modo de preparo.

Como cai na prova

📝 **Como cai:** Delegar administração com menor privilégio a um recorte da organização.
Como resolver: Use unidade administrativa com a função no escopo; se o objetivo é proteger contra admins de locatário, gerenciamento restrito. Verifique se os objetos certos estão na unidade (usuários diretamente, não só o grupo).

📝 **Como cai:** Cenário B2B ou multilocatário com parceiro e quatro mecanismos parecidos.
Como resolver: Pergunte se o parceiro tem Entra ID (sim: B2B, direct connect, trust settings, sincronização; não: OTP, Google, SAML/WS-Fed) e qual direção do fluxo (entrada ou saída).

📝 **Como cai:** Escolher método de autenticação ou sincronizador híbrido por requisitos.
Como resolver: Políticas do AD a cada entrada sem senha na nuvem = PTA; credenciais vazadas ou simplicidade = PHS; florestas desconectadas = Cloud Sync; testar antes de converter = staged rollout.

📝 **Como cai:** Erro de licença por grupo ou script de licenciamento.
Como resolver: Identifique o erro (planos conflitantes, localização de uso) e aplique a correção documentada; em scripts, grupo é Set-MgGroupLicense e licença herdada sai pelo grupo.

📝 **Como cai:** Escolha DUAS sobre domínios, dispositivos ou unidades administrativas.
Como resolver: Confronte cada afirmação com a regra fixa: principal verificado e não federado sem renomear UPNs; hybrid join com linha de visão; gerenciamento restrito sem grupos do Microsoft 365.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Único Owner da assinatura saiu e o Global Administrator não consegue atribuir funções	**Elevar acesso: Access management for Azure resources**
Blindar objetos até de administradores de locatário	**Unidade administrativa de gerenciamento restrito**
Todas as funções de um usuário, inclusive via grupos e escopos	**Users > usuário > Assigned roles**
Convidado sem Entra ID e sem conta Microsoft sendo levado a criar conta pessoal	**Código de acesso único por e-mail**
Convidado trocou de empresa ou e-mail mantendo os acessos	**Redefinir o status de resgate**
Funcionários de empresas irmãs com acesso de membro	**Membro externo (B2B com UserType Member) e sincronização entre locatários**
Canais compartilhados do Teams sem adicionar convidados	**B2B direct connect habilitado nos dois locatários**
Parceiro já exige MFA e dispositivo compatível; evitar registro duplicado	**Trust settings de entrada no acesso entre locatários**
Vários locatários como uma só organização no Teams	**Organização multilocatário**

Exportação do Connect Sync parou após desmarcar uma UO	**Prevenção de exclusões acidentais (limite de 500)**
Duas florestas sem conectividade, infraestrutura mínima	**Cloud Sync com vários agentes**
Grupo criado na nuvem precisa existir no AD local	**Provisionamento de grupos do Cloud Sync**
Credenciais vazadas em ambiente federado com AD FS	**Habilitar sincronização de hash de senha**
Help desk como admin local de todos os notebooks Entra joined	**Microsoft Entra Joined Device Local Administrator**

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

- Funções do Entra e do Azure são separadas; a ponte é a elevação de acesso do Global Administrator.
- Unidades administrativas não aninham, e grupo na unidade não coloca os membros no escopo.
- Entrada controla quem chega; saída controla aonde seus usuários vão; por organização prevalece sobre padrão.
- Grupo atribuível a funções só nasce assim, com associação Assigned e sem aninhamento.
- Licenciamento por grupo não suporta aninhamento: adicione ao novo grupo antes de remover do antigo.

Essenciais para a prova (checklist)

- ☐ Sei a diferença entre funções do Entra e do Azure e como um Global Administrator eleva acesso.
- ☐ Sei criar funções personalizadas e quais funções redefinem senhas e métodos de quem.
- ☐ Sei as regras de unidades administrativas comuns, dinâmicas e de gerenciamento restrito.
- ☐ Sei verificar, tornar principal e excluir um domínio personalizado.
- ☐ Sei as regras de grupos dinâmicos, atribuíveis a funções, expiração e nomenclatura.
- ☐ Sei corrigir erros de licenciamento por grupo e usar Set-MgGroupLicense.
- ☐ Sei os tipos de ingresso de dispositivo, o limite por usuário, LAPS e administradores locais.
- ☐ Sei escolher entre OTP por e-mail, federação com Google e federação SAML/WS-Fed para convidados.
- ☐ Sei configurar entrada, saída, trust settings, B2B direct connect e sincronização entre locatários.
- ☐ Sei escolher entre PHS, PTA, SSO contínuo, staged rollout, Connect Sync e Cloud Sync.

Questões de revisão do capítulo

R1.1 · Implementar e gerenciar identidades de usuários

Um engenheiro da Indústria Aeronáutica Alto Voo não consegue registrar um novo notebook no Microsoft Entra ID e recebe mensagem de que atingiu o limite de dispositivos. Ele tem dezenas de dispositivos antigos registrados. O que a documentação informa sobre esse limite?

A. Padrão de 10 dispositivos por usuário, incluindo os dispositivos hybrid joined do domínio local
B. Padrão de 5 dispositivos registrados por usuário, ajustável pela política de Intune
C. Padrão de 50 dispositivos joined ou registered por usuário, ajustável até 100 ou ilimitado
D. Limite fixo de 20 dispositivos por usuário, alterável só pelo suporte da Microsoft

R1.2 · Implementar e gerenciar identidades de usuários

Na Distribuidora Elétrica Faísca, os técnicos do help desk precisam ser administradores locais de todos os notebooks Microsoft Entra joined, sem receber Global Administrator e sem mexer manualmente em cada dispositivo. O que configurar?

A. Atribuir aos técnicos a função Cloud Device Administrator com escopo de locatário
B. Atribuir aos técnicos a função Intune Administrator nas unidades administrativas
C. Atribuir os técnicos à função Microsoft Entra Joined Device Local Administrator
D. Incluir os técnicos no grupo Administradores do domínio do Active Directory local

R1.3 · Implementar e gerenciar identidades de usuários

A Cooperativa Educacional Ensinar tem milhares de grupos do Microsoft 365 abandonados. A equipe quer que grupos sem uso expirem, mas sem incomodar donos de grupos ativos. O que considerar ao configurar a política de expiração?

A. Cada grupo pode ter uma política própria, e os excluídos não podem ser restaurados depois
B. A política vale para grupos de segurança e distribuição, renovados pelo administrador
C. Grupos com atividade são renovados automaticamente, e os excluídos voltam em até 30 dias
D. Os donos precisam renovar todo grupo manualmente, mesmo havendo atividade recente nele

R1.4 · Implementar e gerenciar identidades de usuários

Na Associação Comercial Bairro Novo, convidados de pequenas empresas sem Microsoft Entra ID e sem conta Microsoft relatam que, ao aceitar o convite, são levados a criar uma conta Microsoft pessoal. A associação quer que eles entrem com um código enviado por e-mail. O que habilitar?

A. A federação com Google para todos os convidados das empresas parceiras
B. A sincronização entre locatários com cada pequena empresa convidada
C. O código de acesso único por e-mail para os convidados
D. O B2B direct connect com as pequenas empresas nas configurações de entrada

Respostas comentadas

R1.1. C) Padrão de 50 dispositivos joined ou registered por usuário, ajustável até 100 ou ilimitado

Por quê: Em Device settings ficam, entre outras opções, quem pode ingressar dispositivos (padrão All), quem pode registrar, a exigência de MFA para registrar ou ingressar (recomenda-se usar a ação de usuário no Acesso Condicional) e o número máximo de dispositivos por usuário.

✗ A) Incorreta. O padrão é 50, e o limite não se aplica a dispositivos hybrid joined.
✗ B) Incorreta. O padrão não é 5, e o limite é configurado nas configurações de dispositivo do Microsoft Entra ID.
✗ D) Incorreta. O limite é configurável pelo administrador em Device settings.

> **Dica de prova:** Limite de dispositivos por usuário: padrão 50 (joined/registered).

R1.2. C) Atribuir os técnicos à função Microsoft Entra Joined Device Local Administrator

Por quê: No ingresso, entram no grupo de administradores locais a função Microsoft Entra Joined Device Local Administrator, a função Global Administrator e o usuário que fez o ingresso. A função é gerenciada em Device settings > Manage Additional local administrators on all Microsoft Entra joined devices.

✗ A) Incorreta. Cloud Device Administrator gerencia dispositivos no Microsoft Entra ID, como habilitar ou desabilitar, sem dar direito de administrador local.
✗ B) Incorreta. Intune Administrator gerencia o Intune; não é o mecanismo descrito para administradores locais.
✗ D) Incorreta. Dispositivos Microsoft Entra joined não dependem do AD local para administradores locais.

> **Dica de prova:** Admin local em todos os Entra joined: Microsoft Entra Joined Device Local Administrator.

R1.3. C) Grupos com atividade são renovados automaticamente, e os excluídos voltam em até 30 dias

Por quê: Grupos com atividade são renovados cerca de 35 dias antes de expirar, sem notificação aos donos. A política exige possuir licenças P1 ou P2 para os membros dos grupos abrangidos.

✗ A) Incorreta. Só existe uma política de expiração para todos os grupos do Microsoft 365 do locatário, e a restauração é possível em 30 dias.
✗ B) Incorreta. A política de expiração vale apenas para grupos do Microsoft 365.
✗ D) Incorreta. A renovação baseada em atividade dispensa ação manual dos donos de grupos ativos.

> **Dica de prova:** Expiração de grupos do Microsoft 365: renovação por atividade, restauração em 30 dias.

R1.4. C) O código de acesso único por e-mail para os convidados

Por quê: No resgate, o Microsoft Entra ID verifica se o usuário existe em um locatário gerenciado, se há federação SAML/WS-Fed para o domínio, entre outras etapas, e usa o código de acesso único quando aplicável.

✗ A) Incorreta. A federação com Google atende usuários do Gmail, não qualquer e-mail.
✗ B) Incorreta. A sincronização entre locatários exige locatários do Microsoft Entra.
✗ D) Incorreta. O B2B direct connect exige que as duas organizações usem Microsoft Entra ID.

> **Dica de prova:** Convidado sem conta compatível: habilite o código de acesso único por e-mail.

02

CAPÍTULO 2 · 25-30% DA PROVA

Implementar o gerenciamento de autenticação e acesso

É o domínio de maior peso (25-30%) e o mais cheio de detalhe fino: métodos de autenticação (TAP, CBA, passkeys, Authenticator), SSPR, proteção de senha, Acesso Condicional, ID Protection e Global Secure Access. A prova descreve uma empresa com um problema concreto e pede a configuração exata, quase sempre com o nome da opção em inglês (Require risk remediation, Sign-in frequency, Report-only, Enabled). As alternativas erradas são recursos reais colocados no lugar errado, então preciso saber o que cada um faz e o que ele NÃO faz. Onde mais erro: força de autenticação x Require MFA, CAE x Sign-in frequency, perfil de segurança x perfil de linha de base no GSA e os estados das configurações (Microsoft managed x Enabled). Recursos aposentados (fraud alert, approved client app, tempo de vida configurável de token) aparecem como distratores.

Neste capítulo

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

Tópicos-chave

Temporary Access Pass (TAP)

Senha de acesso com tempo limitado, de uso único ou múltiplo, para registrar métodos sem senha na primeira entrada ou recuperar o acesso quando o usuário perde o método forte. Quem cria com menor privilégio é o Authentication Administrator (o Authentication Policy Administrator só edita a política). Em domínio federado o TAP tem preferência: o usuário autentica no Microsoft Entra ID sem ir ao IdP. Não substitui a senha; é credencial temporária adicional.

Política do TAP

Em Authentication methods > Policies > Temporary Access Pass > Configure ficam tempo de vida mínimo (padrão 1 hora), máximo (padrão 8 horas, podendo chegar a 30 dias) e padrão, uso único e tamanho (8 a 48 caracteres). Para um passe valer três dias, aumenta-se o máximo para 4.320 minutos. SSPR, frequência de entrada e política de senhas não controlam a validade do TAP.

Autenticação baseada em certificado (CBA)

Associações de autenticação (binding) definem se o certificado vale como fator único ou MFA, mapeando OID de política ou emissor ao nível de proteção. Associações de nome de usuário identificam a conta; por padrão o Principal Name do certificado é mapeado para o userPrincipalName. Cada AC configurada precisa de CRL acessível pela internet, senão não há verificação de revogação.

Passkeys (FIDO2) e perfis de passkey

Perfis de passkey substituem a configuração única do locatário por regras por grupo: tipos permitidos (vinculada ao dispositivo ou sincronizada), atestado e autenticadores-alvo por AAGUID. Para passkey só no Microsoft Authenticator, use perfil device-bound com o AAGUID do Authenticator (Android 14+ ou iOS 17+). Passkeys estão em todas as edições do Microsoft Entra ID, sem licença extra.

Forças de autenticação

As internas são Multifactor authentication strength, Passwordless MFA strength e Phishing-resistant MFA strength; não podem ser modificadas. A Phishing-resistant aceita Windows Hello for Business ou credencial de plataforma, chave FIDO2 e CBA multifator. Para uma combinação exata de métodos, crie força personalizada; os métodos precisam estar habilitados na política de métodos.

Microsoft Authenticator: correspondência de número e denúncia

A correspondência de número vale para todas as notificações por push (MFA, SSPR, registro combinado, adaptador do AD FS e extensão NPS); vestíveis não são suportados. Report suspicious activity substitui o fraud alert, removido em 1º de março de 2025 junto com Block/unblock users e notificações herdadas. Com P2, políticas baseadas em risco remedeiam automaticamente o denunciante marcado com risco alto (usuários sem senha não são marcados); com P1, use os eventos User Reported Suspicious Activity.

Campanha de registro e autenticação preferencial do sistema

A campanha incentiva, após o MFA, o registro de passkey ou Authenticator, um método por vez (estados Microsoft managed, Enabled, Disabled). Authenticator exige modo Any ou Push (Passwordless fica inelegível); passkey exige Allow self-service setup. Na preferencial do sistema, Microsoft managed atua no primeiro e no segundo fator e Enabled só no segundo.

SSPR e registro combinado

Require users to register when signing in força o cadastro e o número de dias para reconfirmar mantém os contatos atualizados (sugestão de 180 dias). Para usuários sincronizados, a senha redefinida só funciona no AD com write-back (Connect Sync ou Cloud Sync). Administradores seguem política fixa de duas etapas, sem perguntas de segurança. O registro combinado é um cadastro único para MFA e SSPR e é pré-requisito da ação Register security information.

Proteção de senha

A lista global é mantida pela Microsoft, aplicada automaticamente e não pode ser editada; a lista personalizada aceita até 1.000 termos e exige P1 ou P2. A senha é normalizada (minúsculas, 0 por o, 1 por l, $ por s, @ por a) e há correspondência de substring para termos de quatro ou mais caracteres. No AD local: proxy + agente de DC, começando em Audit e depois Enforced, sem PHS, sem mudança de esquema e sem portas de entrada.

Bloqueio inteligente

Por padrão bloqueia após 10 tentativas, por um minuto inicialmente e mais tempo depois, sempre ativo; personalizar exige P1. Com autenticação de passagem, o limite do Entra deve ser menor que o do AD (o do AD duas a três vezes maior) e a duração do Entra maior, para a nuvem filtrar o ataque antes de bloquear a conta no AD.

Avaliação do Acesso Condicional

Todas as políticas aplicáveis precisam ser atendidas (lógica E entre políticas) e um bloqueio encerra a avaliação. Dentro de uma política, o padrão é Require all the selected controls; Require one of the selected controls cria o OU. Políticas são aplicadas depois do primeiro fator, e autenticação herdada não faz MFA, sendo bloqueada por políticas que exigem MFA.

Report-only, What If e solução de problemas

Report-only testa a maioria das políticas sem impor (exceto as de User actions) e o resultado aparece nas abas Conditional Access e Report-only do log de entradas. What If simula uma entrada, avalia só políticas On e Report-only e ignora dependências de serviço. Para saber por que uma entrada real foi bloqueada, abra o evento no log de entradas. Insights and reporting mostra o impacto ao longo do tempo (4 horas a 90 dias) e exige logs no Log Analytics.

Condições do Acesso Condicional

Network é a antiga Location (país pelo IP ou GPS do Authenticator, locais nomeados, rede compatível). Device platforms vem do user agent, não verificado; combine com conformidade. Client apps separa modernos e herdados; Authentication Flows bloqueia device code flow e transferência de autenticação; Filter for devices mira atributos como extensionAttribute1 (operadores negativos alcançam não registrados); Guest or external users escolhe tipo de externo e locatário.

Controles de concessão

Require device to be marked as compliant exige dispositivo registrado e inscrito no Intune (Edge InPrivate conta como não compatível). Require Microsoft Entra hybrid joined device só serve para Windows ingressado no domínio. Require app protection policy substitui o aposentado Require approved client app. Windows Hello for Business satisfaz Require multifactor authentication.

Controles de sessão

Sign-in frequency pode ser periódica (horas ou dias) ou Every time; a orientação é desabilitar Remember MFA on trusted devices antes de usá-la. Token protection aceita só tokens vinculados ao dispositivo em apps nativos (Exchange Online, SharePoint Online, Teams) em Windows 10 ou mais recente joined, hybrid joined ou registered. Use app enforced restrictions limita Outlook na Web e SharePoint em dispositivo não gerenciado. Persistent browser session só decide se o navegador guarda a sessão.

Avaliação contínua de acesso (CAE)

Serviços compatíveis rejeitam o token antes de expirar em eventos críticos: conta excluída ou desabilitada, senha alterada, MFA habilitado, revogação explícita e risco de usuário alto, sem depender de política (latência de até 15 minutos). Strictly enforce location policies bloqueia quando o IP visto pelo recurso está fora da lista; exige rede bem conhecida e teste com poucos usuários antes.

Contexto de autenticação e ações protegidas

Contexto de autenticação (até 99, c1 a c99) aplica exigência extra a parte de um app, como um site do SharePoint, ou à ativação de função no PIM. Ações protegidas aplicam Acesso Condicional a permissões (políticas de AC, acesso entre locatários, exclusão definitiva, locais nomeados) independentemente da função e só no momento da ação. Ordem: criar contexto e política primeiro, depois atribuir às permissões.

ID Protection: risco de usuário e de entrada

Risco de entrada se remedeia com autenticação forte: recomendação é médio e alto exigindo MFA com frequência de entrada. Risco de usuário alto usa Require risk remediation, que cobre usuários com e sem senha e aplica sozinho força de autenticação + Sign-in frequency Every time; Block prevalece sobre ela, e ela sobre Require password change. Não combine risco de entrada e de usuário na mesma política.

Global Secure Access

Perfis avaliados na ordem Microsoft, Private Access, Internet Access. Private Access usa conectores (só saída 80/443, dois ou mais por grupo) e Quick Access para trocar a VPN rápido. Internet Access filtra web por política > perfil de segurança > Acesso Condicional; redes remotas (IPsec, sem cliente) usam o perfil de linha de base. Em dispositivo só registrado, o cliente suporta apenas Private Access.

Macetes para memorizar

💡 Ordem dos perfis do GSA

M-P-I: Microsoft primeiro, Private no meio, Internet por último.

💡 Remediação de risco

Entrada se cura com MFA; usuário se cura com senha ou remediação.

💡 Bindings da CBA

Binding de autenticação diz QUANTO vale (único ou MFA); binding de usuário diz QUEM é.

💡 Feedback de risco

Dismiss = era real, mas do bem; Confirm safe = nunca foi risco.

💡 Ações protegidas

Contexto antes, ação depois: primeiro a regra, depois a porta.

💡 Bloqueio inteligente com PTA

Nuvem bloqueia antes e segura por mais tempo.

💡 Forças internas

Três internas e intocáveis: MFA, Passwordless, Phishing-resistant. Quer sob medida? Personalizada.

Tabela de memorização: não confunda

Quando é...	...e quando é
Require password change Risco de usuário só para quem tem senha: exige troca segura de senha após MFA.	**Require risk remediation** Risco de usuário alto cobrindo usuários com e sem senha (passkey); recomendação atual, aplica força de autenticação e Every time automaticamente.
Força de autenticação interna Exigir MFA, Passwordless MFA ou Phishing-resistant MFA como a Microsoft define (sem edição; a resistente a phishing aceita WHfB).	**Força de autenticação personalizada** Aceitar só uma combinação exata, como FIDO2 ou CBA multifator sem Windows Hello for Business.
Avaliação contínua de acesso (CAE) Cortar o acesso antes de o token expirar por evento crítico (conta desabilitada, senha trocada) ou IP fora da lista visto pelo recurso.	**Sign-in frequency** Forçar reautenticação periódica ou a cada acesso (Every time); não compara IP nem reage a eventos.
Report-only Medir o impacto real de uma política nas entradas por dias ou semanas, sem impor.	**What If** Simular uma entrada escolhida para ver quais políticas On ou Report-only se aplicariam.

Perfil de segurança ligado ao Acesso Condicional Filtragem web por usuário ou grupo (ex.: só estudantes), pela identidade no cliente GSA.	**Perfil de segurança de linha de base** Tráfego de redes remotas sem cliente ou regra para todo o tráfego, com a menor prioridade.
Dismiss sign-in risk Risco real mas benigno (teste de intrusão autorizado); entradas parecidas continuam avaliadas.	**Confirm sign-in safe** Falso positivo; entradas semelhantes deixam de ser consideradas arriscadas.
Universal Tenant Restrictions Impedir que usuários entrem em locatários externos não autorizados (exige TRv2 e Entra ID em Tunnel no perfil Microsoft).	**Verificação de rede compatível** Exigir que o acesso aos apps do próprio locatário venha pelo GSA do locatário, sem listas de IP (excluir All Compliant Network locations).

Números que caem

Item	Valor
Tempo de vida do TAP	**Mínimo padrão 1 hora; máximo padrão 8 horas; pode chegar a 30 dias (3 dias = 4.320 minutos)**
Tamanho do TAP	**8 a 48 caracteres**
Lista personalizada de senhas proibidas	**Até 1.000 termos (P1 ou P2); substring a partir de 4 caracteres**
Bloqueio inteligente padrão	**10 tentativas, bloqueio inicial de 1 minuto**
Política de registro de MFA do ID Protection	**14 dias para registrar**
Reconfirmação de métodos do SSPR (sugestão do tutorial)	**180 dias**
Contextos de autenticação	**Até 99 (c1 a c99)**
Latência da CAE em eventos críticos	**Até 15 minutos (token de acesso vale cerca de 1 hora)**
Conectores de rede privada	**Só saída nas portas 80 e 443; dois ou mais por grupo**
Fim de fraud alert e Block/unblock users	**1º de março de 2025**
Insights and reporting do Acesso Condicional	**Intervalo de 4 horas a 90 dias**
Requisitos de plataforma	**Passkey no Authenticator: Android 14+ ou iOS 17+; cliente GSA Android: 11.0+; macOS: 14+**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Editar a força interna Phishing-resistant MFA strength para tirar o Windows Hello for Business.
Como não cair: Forças internas não podem ser modificadas; crie força personalizada com só as combinações aceitas.

⚠ **Alerta de prova:** Habilitar fraud alert, Block/unblock users ou notificações no portal herdado de MFA.
Como não cair: Foram removidos em 1º de março de 2025; a denúncia de prompt suspeito é Report suspicious activity nos métodos de autenticação.

⚠ **Alerta de prova:** Usar o tempo de vida configurável de tokens para resolver prompts inesperados com Sign-in frequency.
Como não cair: Esse recurso foi aposentado; a orientação é desligar Remember MFA on trusted devices antes de usar Sign-in frequency.

⚠ **Alerta de prova:** Dar Authentication Policy Administrator para o suporte emitir o TAP.
Como não cair: Authentication Policy Administrator edita a política de métodos; quem cria o TAP com menor privilégio é o Authentication Administrator.

⚠ **Alerta de prova:** Achar que o TAP não funciona em domínio federado ou que é validado pelo IdP.
Como não cair: O TAP funciona em domínio federado, tem preferência sobre a federação e autentica direto no Microsoft Entra ID.

⚠ **Alerta de prova:** Habilitar write-back para que a troca de senha no Ctrl+Alt+Del remedeie o risco.
Como não cair: Write-back grava senha da nuvem no AD (sentido inverso). Use Allow on-premises password change to reset user risk, com sincronização de hash de senha.

⚠ **Alerta de prova:** Deixar a política em Off e ver no log de auditoria o que teria sido bloqueado.
Como não cair: Políticas Off não são avaliadas e o log de auditoria registra mudanças de configuração; use Report-only e o log de entradas.

⚠ **Alerta de prova:** Adicionar as permissões em protected actions e depois criar o contexto de autenticação.
Como não cair: A ordem invertida causa pedidos repetidos de reautenticação; primeiro contexto + política, depois atribuir às permissões.

⚠ **Alerta de prova:** Manter Require approved client app nas políticas móveis.
Como não cair: Aplicativo cliente aprovado está aposentado; a concessão indicada é Require app protection policy.

⚠ **Alerta de prova:** Exigir dispositivo hybrid joined para iPads ou para qualquer plataforma inscrita no Intune.
Como não cair: Hybrid joined só atende Windows ingressado no domínio; Intune atende o controle de dispositivo compatível.

⚠ **Alerta de prova:** Escolher Microsoft managed na autenticação preferencial do sistema para mudar só o segundo fator.
Como não cair: Microsoft managed aplica ao primeiro e ao segundo fator; só segundo fator é Enabled.

⚠ **Alerta de prova:** Igualar os limites do bloqueio inteligente aos do AD com autenticação de passagem.
Como não cair: Valores iguais não garantem bloqueio na nuvem antes; limite do Entra menor e duração do Entra maior.

⚠ **Alerta de prova:** Vincular a filtragem web ao perfil de linha de base para afetar só os estudantes.
Como não cair: A linha de base vale para todo o tráfego; por grupo, use perfil de segurança ligado a política de Acesso Condicional.

⚠ **Alerta de prova:** Excluir as contas de emergência também das políticas em Report-only.
Como não cair: Report-only não impõe controles; a exclusão é das políticas impostas que bloqueiam ou restringem.

Como cai na prova

📝 **Como cai:** Cenário de suporte que pede a ação com o menor privilégio (TAP, MFA de administrador, SSPR).
Como resolver: Identifique o objeto da ação: emitir TAP é Authentication Administrator; editar política é Authentication Policy Administrator. Descarte Global Administrator e alternativas que desabilitam MFA ou trocam senha, pois enfraquecem a conta.

📝 **Como cai:** Qual estado ou opção configurar, com alternativas em inglês muito parecidas.
Como resolver: Leia o efeito exato pedido (só segundo fator, medir sem impor, nunca persistir) e associe ao estado: Enabled x Microsoft managed, Report-only x Off. Report-only nunca é estado de configurações de método.

📝 **Como cai:** Escolha DUAS ou TRÊS sobre controles de concessão ou forças de autenticação.
Como resolver: Teste cada afirmação contra a regra fixa: compliant = registrado + Intune; InPrivate não é compatível; forças internas são três; padrão é exigir todos os controles.

📝 **Como cai:** Global Secure Access com notebooks que saem da empresa ou filiais sem cliente.
Como resolver: Se o requisito é pela identidade do usuário, vá de perfil de segurança + Acesso Condicional; se é rede remota sem cliente, perfil de linha de base. Descarte local nomeado por IP e restauração do IP de origem quando o pedido é filtrar ou restringir.

📝 **Como cai:** Política de risco com detalhes de licença, senha e combinação de condições.
Como resolver: Separe risco de entrada (MFA, médio e alto) de risco de usuário (Require risk remediation, alto). Nunca combine os dois na mesma política e lembre que Block prevalece sobre as demais.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Perdeu o celular e precisa registrar uma passkey hoje	**Temporary Access Pass criado por Authentication Administrator**
Cartão inteligente como multifator e certificado de software como fator único	**Regras de associação de autenticação da CBA por OID de política**
Regras de passkey diferentes por grupo (atestado, modelos aprovados)	**Perfis de passkey com tipo, atestado e AAGUID**
Usuários aprovam notificações por engano (fadiga de MFA)	**Correspondência de número, sempre ativa em todo push**
Usuários com e sem senha, risco de usuário alto	**Require risk remediation**
Token roubado reutilizado em outro dispositivo	**Token protection (controle de sessão)**
Conta desabilitada, mas token ainda válido por uma hora	**CAE: eventos críticos sem precisar de política**
Exigência extra só para um site do SharePoint	**Contexto de autenticação + política + marcar o site**
MFA resistente a phishing para alterar políticas de AC, qualquer que seja a função	**Ações protegidas (protected actions)**
Phishing que abusa do código de dispositivo	**Condição Authentication Flows com Device code flow + Block**
Medir impacto por duas semanas sem bloquear ninguém	**Report-only + log de entradas**
Substituir a VPN rapidamente liberando faixas de IP e FQDNs	**Quick Access do Private Access**
Políticas por IP pararam porque o serviço vê o IP do proxy GSA	**Restauração do IP de origem (Enable Conditional Access Signaling, Adaptive Access)**

Pulverização de senha por clientes de e-mail antigos	**Política que bloqueia autenticação herdada (Client apps + Block)**

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

- Entre políticas de Acesso Condicional vale E e o bloqueio vence; Require one of the selected controls é o único OU.
- Recursos aposentados são distratores: fraud alert, Require approved client app, tempo de vida configurável de token.
- Risco de usuário alto: Require risk remediation; risco de entrada médio e alto: MFA + frequência de entrada; nunca na mesma política.
- Windows Hello for Business satisfaz Require MFA; para métodos específicos use força de autenticação.
- Contas de emergência ficam fora das políticas impostas que bloqueiam ou restringem.

Essenciais para a prova (checklist)

☐ Sei quem cria um TAP com menor privilégio e como ele se comporta em domínio federado.

☐ Sei diferenciar associação de autenticação e associação de nome de usuário na CBA.

☐ Sei montar perfis de passkey por grupo com tipo, atestado e AAGUID.

☐ Sei quais são as três forças internas e quando criar uma personalizada.

☐ Sei a diferença entre Require password change e Require risk remediation e o que esta aplica automaticamente.

☐ Sei quando usar Report-only, What If, log de entradas e Insights and reporting.

☐ Sei quais eventos a CAE trata sem política e o que faz Strictly enforce location policies.

☐ Sei a sequência correta para configurar ações protegidas.

☐ Sei a ordem dos perfis do GSA e quando usar perfil ligado ao AC ou perfil de linha de base.

☐ Sei configurar a proteção de senha local e o bloqueio inteligente com autenticação de passagem.

Questões de revisão do capítulo

R2.1 · Implementar o gerenciamento de autenticação e acesso

A Rede de Padarias Trigo Bom habilitou o SSPR para todos os funcionários, mas muitos só descobrem que não cadastraram métodos quando esquecem a senha, e outros mudaram de telefone. Quais configurações de registro do SSPR resolvem os dois problemas?

A. Write-back de senha e desbloqueio de contas sem redefinir a senha local
B. Número de métodos exigidos para redefinir igual a dois e perguntas de segurança
C. Require users to register when signing in e dias para reconfirmar
D. Notificar usuários sobre redefinições e notificar todos os administradores

R2.2 · Implementar o gerenciamento de autenticação e acesso

A Rede de Lojas Preço Bom tem uma política que exige MFA para todos os usuários, e algumas contas de impressoras multifuncionais que usam protocolos antigos passaram a ser bloqueadas. O que a documentação informa sobre esse comportamento?

A. Clientes de autenticação herdada passam a usar autenticação moderna
B. Clientes de autenticação herdada não são avaliados pelo Acesso Condicional em nenhum caso
C. Clientes de autenticação herdada não suportam MFA e são bloqueados por esses controles
D. Clientes de autenticação herdada recebem MFA por SMS automaticamente na primeira entrada

R2.3 · Implementar o gerenciamento de autenticação e acesso

A Seguradora Vida Plena criou uma política com Sign-in frequency de 8 horas para aplicativos financeiros, mas usuários relatam pedidos de reautenticação inesperados. O locatário também tem habilitado Remember MFA on trusted devices. O que a documentação orienta?

A. Habilitar a configuração de tempo de vida de tokens de atualização e sessão
B. Trocar Sign-in frequency por Persistent browser session em cada aplicativo
C. Desabilitar Remember MFA on trusted devices antes de usar Sign-in frequency
D. Manter as duas opções ativas e aumentar a frequência de entrada para 90 dias

R2.4 · Implementar o gerenciamento de autenticação e acesso

Um gerente da Seguradora Porto Firme perdeu o celular com o Microsoft Authenticator e precisa registrar hoje uma passkey em uma chave de segurança nova, sem passar por um fluxo de recuperação demorado. O método Temporary Access Pass já está habilitado para todos os usuários na política de métodos de autenticação. Como a equipe de suporte deve proceder com o menor privilégio?

A. Com a função Global Administrator, desabilitar o MFA do gerente até que ele registre um novo método
B. Com a função Authentication Administrator, criar um Temporary Access Pass para o gerente usar em Security info
C. Com a função Password Administrator, gerar uma senha temporária e exigir a troca no próximo acesso
D. Com a função Authentication Policy Administrator, excluir o gerente da política e redefinir a senha dele

Respostas comentadas

R2.1. C) Require users to register when signing in e dias para reconfirmar

Por quê: A interrupção para registro só ocorre para usuários habilitados no SSPR e aparece uma vez por sessão interativa. O tutorial sugere reconfirmação a cada 180 dias, para evitar contatos desatualizados no momento da redefinição.

✗ A) Incorreta. Write-back grava a senha no AD local; não trata do registro dos métodos.
✗ B) Incorreta. Exigir dois métodos aumenta a segurança da redefinição, mas não força o registro nem a atualização.
✗ D) Incorreta. Notificações avisam sobre redefinições; não garantem registro de métodos.

> **Dica de prova:** Forçar e atualizar registro do SSPR: registro na entrada + dias para reconfirmar.

R2.2. C) Clientes de autenticação herdada não suportam MFA e são bloqueados por esses controles

Por quê: A condição Client apps separa clientes modernos (navegador, aplicativos móveis e desktop) e herdados (Exchange ActiveSync e outros clientes). Por padrão, políticas novas se aplicam a todos os tipos de cliente.

✗ A) Incorreta. A política não converte o protocolo usado pelo cliente.
✗ B) Incorreta. A condição de aplicativos cliente permite mirar clientes herdados, como Exchange ActiveSync e Other clients.
✗ D) Incorreta. Esses clientes não conseguem concluir MFA.

> **Dica de prova:** Autenticação herdada não faz MFA: é bloqueada por políticas que exigem MFA.

R2.3. C) Desabilitar Remember MFA on trusted devices antes de usar Sign-in frequency

Por quê: Sign-in frequency pode ser periódica (horas ou dias) ou Every time. Recomenda-se frequência igual para aplicativos-chave do Microsoft 365, como Exchange Online e SharePoint Online, e a sessão persistente do Acesso Condicional sobrepõe a opção Stay signed in? da identidade visual.

✗ A) Incorreta. O tempo de vida configurável para tokens de atualização e sessão foi aposentado e substituído pelo gerenciamento de sessão do Acesso Condicional.

✗ B) Incorreta. A sessão persistente do navegador exige selecionar todos os aplicativos de nuvem e controla outra coisa.

✗ D) Incorreta. Manter as duas configurações juntas é justamente o que causa prompts inesperados.

> **Dica de prova:** Usar Sign-in frequency: desligue Remember MFA on trusted devices.

R2.4. B) Com a função Authentication Administrator, criar um Temporary Access Pass para o gerente usar em Security info

Por quê: O Temporary Access Pass é uma senha de acesso com tempo limitado, de uso único ou múltiplo, usada para integrar métodos sem senha ou recuperar o acesso quando o usuário perde um método forte. Só usuários incluídos na política podem entrar com ele.

✗ A) Incorreta. Desabilitar MFA enfraquece a conta e usa um privilégio muito acima do necessário.

✗ C) Incorreta. Uma senha temporária não substitui um método forte e não permite concluir o registro sem o MFA perdido.

✗ D) Incorreta. O Authentication Policy Administrator edita a política de métodos, mas não é o papel que cria o TAP; e redefinir a senha não ajuda a registrar a passkey com segurança.

> **Dica de prova:** Perdeu o método forte e precisa registrar outro: Temporary Access Pass.

03

CAPÍTULO 3 · 20-25% DA PROVA

Planejar e automatizar a governança de identidade

Aqui eu preciso dominar entitlement management, revisões de acesso, PIM (funções do Entra, recursos do Azure e grupos), contas de emergência e monitoramento (logs, retenção, diagnóstico, KQL, workbooks e Identity Secure Score). A prova cobra o nome exato da opção (Auto apply results to resource, If reviewers don't respond, Allow users to extend access) e o comportamento padrão do recurso. Erro muito quando misturo revisores alternativos da revisão com aprovadores alternativos do pacote, ou o requisito de função entre revisões de funções do Entra e do Azure. Também é comum a pegadinha de licença: PIM e revisões não vêm no P1. Nos logs, preciso saber qual log responde qual pergunta e quanto tempo cada um fica guardado.

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

Tópicos-chave

Catálogo e pacote de acesso

Catálogo é o contêiner de recursos e pacotes; recursos típicos são grupos (incluindo do Microsoft 365), aplicativos integrados ao Entra e sites do SharePoint Online, além de funções do Microsoft Entra. Políticas de AC e unidades administrativas não são recursos de catálogo. Para externos pedirem pelo autoatendimento, o catálogo precisa de Enabled for external users = Yes e a política precisa permitir organizações conectadas.

Políticas de pacote de acesso

Para usuários fora do diretório: Specific connected organizations, All configured connected organizations ou All users (All connected organizations + any new external users). Atribuição direta pelo administrador só aparece se uma política a permitir. Política de atribuição automática concede por regra de atributo (ex.: department), exige ID Governance ou Suite e é criada por Identity Governance Administrator; recomenda-se uma por pacote.

Organizações conectadas: configured x proposed

Organizações criadas pelo administrador ou pela API nascem configured. As criadas automaticamente quando alguém de fora pede um pacote aberto a qualquer externo nascem proposed e ficam fora do escopo de políticas para organizações configuradas até um administrador mudar o estado. Usuários de organizações propostas só veem pacotes abertos a qualquer usuário externo.

Aprovação em pacotes de acesso

Em várias etapas, basta um aprovador por etapa; se um nega antes de outro aprovar, a solicitação é encerrada; sem decisão no prazo, é negada automaticamente. Aprovadores não aprovam as próprias solicitações. Aprovadores alternativos (Show advanced request settings) recebem o pedido encaminhado quando não há ação.

Dados e comprovantes na solicitação

Perguntas em Requestor information (texto livre e múltipla escolha) são exibidas ao aprovador, junto com Require requestor justification. Requisito de Verified ID exige credencial de emissor confiável e licença ID Governance ou Suite. Termos de uso registram aceite de documento, não coletam dados.

Lifecycle, separação de funções e extensões

Na aba Lifecycle define-se expiração (Number of days, Number of hours, On date ou Never) e Allow users to extend access; mudar a expiração não altera atribuições já aprovadas. Separation of duties marca pacotes incompatíveis e impede o pedido. Extensão personalizada com Logic Apps executa ações em outros sistemas quando a atribuição é concedida (aba Rules).

Ciclo de vida de usuários externos

Em Control Configurations, Lifecycle of external users define o que acontece com o convidado quando a última atribuição termina: o padrão é bloquear a entrada e remover após 30 dias. Só vale para convidados trazidos pelo entitlement management; convidados que já existiam permanecem.

Funções do entitlement management

Por catálogo: Catalog owner (gerencia pacotes e recursos), Catalog reader, Access package manager (cria e edita pacotes) e Access package assignment manager (só atribui e remove usuários). Gerais: Catalog creator (donos de recursos criam catálogos sem função administrativa do Entra) e Connected Organization Administrator. Aprovador e solicitante são direitos de política, não funções.

Termos de uso

Exigem P1, documento em PDF (com versões por idioma) e são impostos como controle de concessão do Acesso Condicional; até 40 termos por locatário. Opções: Require users to expand, Require users to consent on every device (dispositivo precisa estar registrado no Entra) e Expire consents. Contas de serviço devem ser excluídas das políticas.

Criação de revisões de acesso

Revisores: proprietários do grupo, usuários selecionados, autorrevisão ou Managers of users, com fallback reviewers quando faltar dono ou gerente. Escopos especiais: Guest users only, Inactive users (on tenant level) com Days inactive (até 730 dias) e All Microsoft 365 groups with guest users. Recorrência: frequência, Duration (in days) e fim por data ou número de ocorrências. Exigem ID Governance ou Suite.

Conclusão de revisões

Auto apply results to resource remove os negados ao fim; If reviewers don't respond pode ser No change, Remove access, Approve access ou Take recommendations. Sem aplicação automática, aplique em Review History > instância > Apply. Para convidados negados em revisão só de convidados, Block user from signing-in for 30 days, then remove user from the tenant. Don't know mantém o acesso e fica no log de auditoria.

Auxiliares e preparação

No sign-in within 30 days recomenda negar a quem não entrou (em apps, conta a última entrada no app); User-to-Group Affiliation usa a distância na hierarquia. Para revisar um aplicativo, ele precisa de Assignment required = Yes. Review History > New report gera CSV com as decisões de todas as revisões.

PIM: funções do Microsoft Entra

Atribuição elegível exige ativação em PIM > My roles (atribuição ativa criada em segundos); ativa fica disponível o tempo todo. Configurações: duração máxima da ativação (1 a 24 horas), MFA ou contexto de autenticação na ativação, justificativa, aprovação e Allow permanent eligible/active assignment. A aprovação tem 24 horas fixas e fica em Approve requests. Licença: P2 ou ID Governance.

PIM: extensão, notificações e risco de bloqueio

Atribuição que expira em até 14 dias pode ser estendida em My roles; Global Administrator ou Privileged Role Administrator decide. E-mails saem de MSSecurity-noreply@microsoft.com com prefixo PIM no assunto. Se a ativação exige aprovação sem aprovadores, aprovam os administradores ativos; sem nenhum ativo, ninguém aprova e o locatário pode ficar bloqueado.

PIM para recursos do Azure e PIM for Groups

PIM para Azure exige Owner ou User Access Administrator no recurso (Global Administrator não basta) e atribui funções em grupo de gerenciamento, assinatura, grupo de recursos ou recurso. PIM for Groups dá associação e propriedade just-in-time, cada uma com sua política; serve a grupos de segurança e do Microsoft 365 e controla acesso a apps de terceiros autorizados por grupo.

Alertas, auditoria e descoberta no PIM

Alerta de severidade alta: Roles are being assigned outside of Privileged Identity Management. Resource audit mostra ativações, mudanças de atribuição e de configuração (30 dias); My audit só a atividade de quem consulta. Discovery and insights lista quem tem funções privilegiadas permanentes e ajuda a converter para just-in-time.

Contas de acesso de emergência

Duas ou mais contas somente nuvem no domínio onmicrosoft.com, com Global Administrator permanente e passkey (FIDO2), sem dispositivos pessoais nem SMS. Crie um grupo dedicado excluído das políticas que bloqueiam ou restringem, teste periodicamente, guarde as chaves em cofres separados e alerte cada entrada com regra do Azure Monitor em SigninLogs.

Logs, retenção e diagnóstico

Entradas e auditoria: 7 dias na Free e 30 dias com P1/P2; logs de atividade do Microsoft Graph só existem se exportados. Configurações de diagnóstico enviam a Log Analytics (KQL), conta de armazenamento (arquivo) ou hub de eventos (SIEM quase em tempo real) e exigem ao menos Security Administrator. Logs de auditoria são gerados pelo sistema e não podem ser editados.

Macetes para memorizar

Revisor x aprovador alternativo

Revisão tem fallback REVISOR; pacote tem APROVADOR alternativo.

Quem cria revisão no PIM

Entra = PRA; Azure = Owner ou UAA.

Retenção de logs

Free 7, pago 30; mais que isso, exporte.

Destinos de diagnóstico

LAH: Log Analytics consulta, Armazenamento arquiva, Hub transmite.

Organização conectada

Criou sozinha = proposta; só o admin a deixa configurada.

Aprovação no PIM

24 horas fixas, ninguém aprova o próprio pedido.

Contas de emergência

2+, nuvem, onmicrosoft, GA, FIDO2, fora das políticas, testadas e vigiadas.

Tabela de memorização: não confunda

Quando é...	...e quando é
If reviewers don't respond = No change Manter o acesso de quem não foi revisado, evitando revogação em massa se gerentes não responderem.	**If reviewers don't respond = Take recommendations** Seguir as recomendações do sistema para não revisados; com Auto apply pode revogar acessos.
Fallback reviewers Revisão de acesso quando o grupo não tem dono ou o usuário não tem gerente.	**Aprovadores alternativos** Fluxo de aprovação de pacote de acesso quando o aprovador não decide no prazo.

Revisão em PIM > Microsoft Entra roles Revisar funções do Entra (Global Administrator, Exchange Administrator); exige Privileged Role Administrator.	**Revisão em PIM > Azure resources** Revisar funções do Azure (Owner em assinatura); exige Owner ou User Access Administrator no recurso.
Atribuição elegível (Eligible) Usar a função só quando precisar, com ativação, MFA, justificativa e aprovação.	**Atribuição ativa (Active)** Função disponível o tempo todo, sem ativação (contas de emergência).
Access package assignment manager Só atribuir e remover usuários de pacotes existentes.	**Access package manager / Catalog owner** Criar e editar pacotes (Access package manager) ou gerenciar pacotes e recursos do catálogo (Catalog owner).
Hub de eventos Enviar logs a um SIEM de terceiros quase em tempo real.	**Conta de armazenamento / Log Analytics** Arquivar por longo prazo (armazenamento) ou consultar com KQL e workbooks (Log Analytics).
Resource audit do PIM Histórico de ativações, mudanças de atribuição e de configuração de funções no PIM.	**Review History** Relatório CSV com as decisões dos revisores em revisões de acesso.

Números que caem

Item	Valor
Retenção de entradas e auditoria	**Free: 7 dias; P1/P2: 30 dias**
Entradas arriscadas com P2	**90 dias**
Log de auditoria do PIM	**30 dias**
Duração da ativação no PIM	**1 a 24 horas**
Janela de aprovação no PIM	**24 horas, não configurável**
Aviso e extensão de atribuições do PIM	**Expirando em até 14 dias; expiradas visíveis por até 30 dias**
Duração mínima de atribuição no PIM para Azure	**5 minutos**
Ciclo de vida padrão de convidados sem pacotes	**Bloqueio e remoção após 30 dias**
Ação para convidado negado	**Bloquear por 30 dias e depois remover**
Inatividade em revisões de grupos	**Até 730 dias**
Termos de uso por locatário	**Até 40**
E-mails do PIM por evento	**Até 1.000; remetente MSSecurity-noreply@microsoft.com**
Janela sugerida para conta inativa	**90 a 180 dias**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que Global Administrator no Entra basta para gerenciar o PIM das assinaturas do Azure.
Como não cair: PIM para recursos do Azure exige Owner ou User Access Administrator no recurso.

⚠ **Alerta de prova:** Criar a revisão de funções do Azure no PIM com Privileged Role Administrator.
Como não cair: PRA é requisito para funções do Entra; para Azure resources é Owner ou User Access Administrator.

⚠ **Alerta de prova:** Selecionar Stop ou excluir a revisão para aplicar as decisões.
Como não cair: Sem aplicação automática, as decisões só valem com Apply em Review History; excluir não aplica e Reset apaga decisões.

⚠ **Alerta de prova:** Usar fallback reviewers para resolver aprovador ausente no pacote de acesso.
Como não cair: Revisores alternativos pertencem às revisões; no pacote, configure aprovadores alternativos com encaminhamento.

⚠ **Alerta de prova:** Exigir que todos os aprovadores de uma etapa aprovem ou mandar para desempate na etapa seguinte.
Como não cair: Um aprovador por etapa basta; uma negação encerra a solicitação.

⚠ **Alerta de prova:** Ligar só On activation, require multifactor authentication para garantir autenticação nova e forte.
Como não cair: O MFA simples pode ser satisfeito pela entrada com Windows Hello for Business; use contexto de autenticação com força de autenticação.

⚠ **Alerta de prova:** Definir Activation maximum duration de seis meses para expirar atribuições.
Como não cair: A ativação vai de 1 a 24 horas; para expirar atribuições, desmarque Allow permanent e defina a expiração.

⚠ **Alerta de prova:** Exigir aprovação no PIM com a lista de aprovadores vazia esperando que o PIM escolha alguém.
Como não cair: Sem aprovadores, aprovam os administradores ativos; sem nenhum ativo e sem contas de emergência, há risco de bloqueio.

⚠ **Alerta de prova:** Esperar que a aprovação no PIM possa durar sete dias ou seja automática após o prazo.
Como não cair: A janela é de 24 horas fixas; sem aprovação, o pedido não é concedido.

⚠ **Alerta de prova:** Achar que o PIM ou as revisões de acesso estão incluídos no P1.
Como não cair: O P1 não inclui PIM nem revisões de acesso: PIM exige P2 ou ID Governance; revisões exigem ID Governance ou Suite, e revisões de inativos e afinidade usuário-grupo exigem ID Governance.

⚠ **Alerta de prova:** Procurar os logs de atividade do Microsoft Graph no portal com P1.
Como não cair: Esses logs só existem se integrados a armazenamento ou análise pelas configurações de diagnóstico.

⚠ **Alerta de prova:** Supor que com P1 os logs de entrada ficam 90 dias.
Como não cair: Com P1/P2 são 30 dias; 90 dias é o período de entradas arriscadas com P2; para mais tempo, exporte.

⚠ **Alerta de prova:** Ajustar a remoção de convidados em Guest invite settings ou External user leave settings.
Como não cair: O ciclo de vida após o fim dos pacotes fica em Control Configurations > Lifecycle of external users.

⚠ **Alerta de prova:** Usar o auxiliar No sign-in within 30 days para restringir a revisão a inativos.
Como não cair: Auxiliares só recomendam; para revisar só inativos use Inactive users (on tenant level) + Days inactive.

Como cai na prova

📝 **Como cai:** Requisito de negócio sobre revisões (quem revisa, o que fazer com não revisados, quando aplicar).
Como resolver: Separe em três decisões: revisores (+ fallback), Upon completion (Auto apply + If reviewers don't respond) e escopo (convidados, inativos). Se o enunciado teme revogação em massa, a resposta é No change.

📝 **Como cai:** Externos não conseguem pedir um pacote de acesso.
Como resolver: Verifique, nesta ordem: catálogo com Enabled for external users, política aceitando organizações conectadas e estado da organização (proposed precisa virar configured).

📝 **Como cai:** Configurar uma função no PIM com prazo, autenticação forte e aprovação.
Como resolver: Mapeie cada exigência à opção: duração da ativação (até 24 horas), contexto de autenticação para autenticação nova, aprovação com aprovadores definidos e expiração para eliminar permanentes.

📝 **Como cai:** Qual log, workbook ou relatório responde a uma pergunta de investigação.
Como resolver: Autenticação é log de entradas; mudança de configuração é auditoria; criação de conta em app é provisionamento; impacto de políticas é Insights and reporting; decisões de revisão é Review History.

📝 **Como cai:** Consulta KQL entre quatro opções parecidas.
Como resolver: Olhe a tabela e o campo agrupado: SigninLogs por AppDisplayName para apps com mais entradas; AuditLogs por OperationName para operações; AADProvisioningLogs para provisionamento.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Excesso de prompts de MFA ao longo do dia	**Workbook Authentication Prompts Analysis**
Entradas não cobertas por nenhuma política de AC	**Workbook Conditional Access Gap Analyzer**
Abuso de aplicativos e credenciais adicionadas a entidades de serviço	**Workbook Sensitive Operations Report**
Indicador percentual de postura de identidade, até na edição Free	**Identity Secure Score (recalculado a cada 24 horas)**
Quem já está apto a MFA, passwordless e SSPR	**Authentication methods > Activity (Registration e Usage)**
Logs no SIEM quase em tempo real	**Configuração de diagnóstico com Stream to an event hub**
Usuário não chegou ao app com provisionamento automático	**Logs de provisionamento**
Quem mudou proprietários de grupo ou licenças	**Logs de auditoria (imutáveis)**
Falha de entrada com recomendação de correção, sem abrir chamado	**Sign-in diagnostic**
Conta inativa por entrada interativa bem-sucedida via Graph	**signInActivity/lastSuccessfulSignInDateTime (P1 ou P2)**
Acesso just-in-time a app autorizado por grupo	**PIM for Groups com membros elegíveis**
Começando no PIM, achar quem tem função permanente	**Discovery and insights**

Vendedor não pode ter dois pacotes ao mesmo tempo	**Separation of duties (pacotes incompatíveis)**
Externos de instituições ainda não cadastradas pedindo pacote	**All users (All connected organizations + any new external users); organização nasce proposed**

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

- PIM exige P2 ou ID Governance; revisões e recursos avançados de pacote exigem ID Governance ou Suite.
- Revisão sem Auto apply não muda nada até alguém clicar Apply em Review History.
- Organização conectada criada automaticamente é proposed e não entra em políticas para organizações configuradas.
- Funções do Azure no PIM dependem de Owner ou User Access Administrator, não de funções do Entra.
- Logs de atividade do Graph só existem se exportados por configurações de diagnóstico.

Essenciais para a prova (checklist)

- ☐ Sei quais recursos entram em um catálogo e o que é preciso para externos pedirem pacotes.
- ☐ Sei diferenciar organização conectada configured e proposed e as opções de política para externos.
- ☐ Sei configurar expiração, extensão, separação de funções e extensões personalizadas de um pacote.
- ☐ Sei como funciona a aprovação em várias etapas e o papel dos aprovadores alternativos.
- ☐ Sei escolher revisores, escopo, recorrência e configurações de conclusão de uma revisão de acesso.
- ☐ Sei ativar, estender e configurar funções no PIM, incluindo aprovação e contexto de autenticação.
- ☐ Sei qual função é exigida para PIM e revisões em funções do Entra e em recursos do Azure.
- ☐ Sei montar e monitorar contas de acesso de emergência conforme a orientação da Microsoft.
- ☐ Sei a retenção de cada log e os três destinos das configurações de diagnóstico.
- ☐ Sei qual workbook ou relatório usar para prompts, lacunas de AC, operações sensíveis e postura.

Questões de revisão do capítulo

R3.1 · Planejar e automatizar a governança de identidade

A Agência de Eventos Palco Livre quer que atribuições do pacote de acesso Produção de Shows expirem 60 dias após a aprovação e que o usuário possa pedir prorrogação antes de perder o acesso. O que configurar na aba Lifecycle da política?

A. Expiração por On date e Users can request specific timeline desativado
B. Expiração por Number of days igual a 60 e Allow users to extend access = Yes
C. Expiração por Number of hours igual a 60 e Require approval to extend = No
D. Expiração por Never e uma revisão de acesso anual com aplicação automática dos resultados

R3.2 · Planejar e automatizar a governança de identidade

O analista da Rede de Clínicas Saúde Plena quer encontrar entradas que não foram cobertas por nenhuma política de Acesso Condicional, como entradas por autenticação herdada ou de locais não protegidos. Os logs já estão no Log Analytics. Qual pasta de trabalho usar?

A. Sensitive Operations Report
B. Conditional Access Gap Analyzer
C. Usage and insights de métodos de autenticação
D. Authentication Prompts Analysis

R3.3 · Planejar e automatizar a governança de identidade

O painel do PIM da Editora Brisa mostra um alerta de severidade alta para funções do Microsoft Entra. Qual destes alertas do PIM tem severidade alta por indicar possível ataque em andamento?

A. Roles are being assigned outside of Privileged Identity Management
B. Roles don't require multifactor authentication for activation
C. There are too many Global Administrators in the organization
D. Administrators aren't using their privileged roles regularly

R3.4 · Planejar e automatizar a governança de identidade

A Editora Saber Vivo quer revisar, no grupo Licenças-Adobe, apenas os membros que não entram no locatário há mais de 120 dias, interativa ou não interativamente. Como configurar o escopo da revisão de acesso?

A. Usar o auxiliar No sign-in within 30 days e repetir a revisão por quatro meses
B. Criar uma regra dinâmica no grupo com o atributo lastSignInDateTime
C. Marcar Inactive users (on tenant level) e informar 120 em Days inactive
D. Escolher Guest users only, que já inclui só os membros inativos do grupo

Respostas comentadas

R3.1. B) Expiração por Number of days igual a 60 e Allow users to extend access = Yes

Por quê: Ao pedir extensão, o usuário precisa continuar no escopo da política. Mudar a expiração em uma política não altera a expiração de solicitações já pendentes ou aprovadas. Revisões de acesso das atribuições também podem ser habilitadas na política.

✗ A) Incorreta. Uma data fixa não equivale a 60 dias após cada aprovação, e o pedido é permitir prorrogação.
✗ C) Incorreta. 60 horas não correspondem a 60 dias.
✗ D) Incorreta. Never mantém o acesso sem prazo, contrariando o pedido.

> **Dica de prova:** Expirar em X dias e permitir prorrogar: Number of days + Allow users to extend access.

R3.2. B) Conditional Access Gap Analyzer

Por quê: A pasta de trabalho apoia boas práticas como bloquear autenticação herdada, aplicar ao menos uma política a cada aplicativo, bloquear entradas de alto risco e bloquear entradas de locais não confiáveis.

✗ A) Incorreta. Sensitive Operations Report trata de operações sensíveis de aplicativos e entidades de serviço.
✗ C) Incorreta. O relatório de uso de métodos mostra registro e uso de métodos de autenticação.
✗ D) Incorreta. Authentication Prompts Analysis investiga excesso de prompts.

> **Dica de prova:** Entradas sem nenhuma política de AC: Conditional Access Gap Analyzer.

R3.3. A) Roles are being assigned outside of Privileged Identity Management

Por quê: Os alertas de segurança do PIM aparecem no painel e podem ser lidos por Global Administrator, Privileged Role Administrator, Global Reader, Security Administrator e Security Reader. Cada alerta traz correção, prevenção e ação de mitigação no portal.

✗ B) Incorreta. O alerta de funções sem MFA na ativação tem severidade baixa.
✗ C) Incorreta. O alerta de excesso de Global Administrators tem severidade baixa.
✗ D) Incorreta. O alerta de administradores que não usam as funções tem severidade baixa.

> **Dica de prova:** Alerta alto do PIM: funções atribuídas fora do PIM.

R3.4. C) Marcar Inactive users (on tenant level) e informar 120 em Days inactive

Por quê: Usuários criados ou convidados dentro do período de inatividade configurado ficam fora do escopo, para que possam entrar ao menos uma vez antes de serem removidos.

✗ A) Incorreta. O auxiliar de decisão só recomenda aprovar ou negar; não restringe o escopo aos inativos.
✗ B) Incorreta. A revisão tem opção própria para inativos; regras dinâmicas definem membros do grupo.
✗ D) Incorreta. Guest users only limita a convidados, não a inativos.

> **Dica de prova:** Revisar só inativos: Inactive users (on tenant level) + Days inactive.

04

CAPÍTULO 4 · 20-25% DA PROVA

Planejar e implementar identidades de carga de trabalho

Este domínio junta identidades gerenciadas, entidades de serviço, registros de aplicativo, aplicativos empresariais, consentimento, SSO, application proxy, provisionamento e Defender for Cloud Apps. A prova pede o tipo certo de identidade ou credencial para um workload, a função mínima para uma ação e a opção de SSO ou de política que resolve o cenário. Meu ponto fraco é confundir permissões delegadas (escopos) com funções de aplicativo, e as três propriedades do aplicativo empresarial (Enabled for users to sign-in, Assignment required, Visible to users). No Defender for Cloud Apps, a confusão clássica é entre política de acesso, de sessão, de atividade, de descoberta e de OAuth. Também cai quem concede consentimento para permissões de aplicativo do Microsoft Graph.

Neste capítulo

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

Tópicos-chave

Identidade gerenciada atribuída pelo sistema

Criada como entidade de serviço especial do próprio recurso, só ele a usa e ela é excluída junto com ele. Indicada quando cada recurso precisa de identidade e permissões próprias. Habilitar numa VM existente exige Virtual Machine Contributor (VM > Security > Identity, aba System assigned, Status On), sem função de diretório.

Identidade gerenciada atribuída pelo usuário

Recurso autônomo do Azure, criado antes da computação, associável a vários recursos e excluído explicitamente. Ideal para muitos recursos com a mesma permissão ou para recursos efêmeros em massa (evita HTTP 429). Criar exige Managed Identity Contributor; associar a um recurso exige Managed Identity Operator.

Uso de identidade gerenciada

As credenciais não ficam acessíveis a ninguém e são gerenciadas pela plataforma. A identidade autentica, mas quem autoriza é uma atribuição de função do Azure no recurso (ex.: Storage Blob Data Reader). Na VM, o token vem do IMDS com o cabeçalho Metadata: true e o parâmetro resource.

Workloads fora do Azure

Serviço local em vários servidores: gMSA, com senha trocada pelo Windows (sMSA é para um único servidor). Servidor fora do Azure chamando o Graph: registro de aplicativo com entidade de serviço e certificado de AC confiável. Pipelines como GitHub Actions ou Kubernetes: federação de identidade de workload, sem segredo.

Objeto de aplicativo x entidade de serviço

O objeto de aplicativo existe só no locatário de origem e define propriedades estáticas, como uma classe. Cada locatário que usa o app tem uma entidade de serviço, onde recebe consentimentos e atribuições. Registrar pelo portal cria os dois no locatário de origem; clientes não registram de novo.

Registro de aplicativo

Tipo de conta vira signInAudience: AzureADMyOrg (locatário único), AzureADMultipleOrgs (qualquer organização, sem contas pessoais), AzureADandPersonalMicrosoftAccount e PersonalMicrosoftAccount. App React no navegador usa plataforma Single-page application. Registro excluído volta em Deleted applications por até 30 dias; App instance property lock vem habilitado por padrão em apps novos desde junho de 2026.

Credenciais de aplicativo confidencial

Certificado de AC conhecida (recomendado, gerenciado no Key Vault, .cer, .pem ou .crt) e credencial de identidade federada são indicados para produção. Segredo do cliente é menos seguro, só para desenvolvimento local; certificado autoassinado é para testes.

Permissões delegadas x de aplicativo

Delegadas (escopos) agem em nome do usuário conectado; são publicadas em Expose an API (URI de ID do aplicativo + escopo, com Who can consent). Funções de aplicativo com Allowed member types = Applications dão acesso somente de aplicativo e aparecem na declaração roles. No fluxo de credenciais do cliente, scope = recurso/.default.

Consentimento do administrador

Permissões de aplicativo sempre exigem consentimento do administrador. Cloud Application Administrator e Application Administrator consentem, exceto permissões de aplicativo do Microsoft Graph, que exigem Privileged Role Administrator. Para revogar, Enterprise apps > Permissions > Admin consent; consentimentos de usuário se revogam por Graph ou PowerShell.

Consentimento do usuário

Recomendação: permitir só para editores verificados e permissões classificadas como baixo impacto (Permission classifications, aba Low). Fluxo de consentimento do administrador encaminha pedidos a revisores, mas a designação não eleva privilégios. Verificação do editor usa PartnerID do AI Cloud Partner Program e mostra o selo azul.

Propriedades do aplicativo empresarial

Enabled for users to sign-in = No bloqueia tudo, inclusive tokens com permissões de aplicativo. Assignment required = Yes restringe quem obtém token aos atribuídos. Visible to users = No só tira do My Apps e do iniciador do Microsoft 365. Proprietário (usuário, nunca grupo) gerencia um app sem função administrativa.

Atribuição e My Apps

Atribuição por grupo exige P1 ou P2 e não suporta aninhamento: atribua os subgrupos diretamente. Funções de aplicativo são atribuídas a usuários e grupos em Users and groups do app empresarial. Coleções (App launchers) só organizam abas do My Apps; Self-service application access permite pedir o app com aprovação de negócio (P1 ou P2).

Tipos de SSO

SAML: Identifier (Entity ID) e Reply URL (ACS), certificado autoassinado de três anos (troca: criar novo, enviar ao app, ativar, cadastrar e-mails). Password-based: login HTML sem SAML. Linked: só um link no My Apps. Header-based e KCD: apps locais pelo application proxy que leem cabeçalhos ou usam Autenticação Integrada do Windows.

Application proxy

Pré-autenticação Microsoft Entra ID permite MFA e Acesso Condicional; Passthrough não. Conectores só saída 80/443, organizados em grupos por local, com o grupo padrão para ociosos. Domínio personalizado exige domínio verificado, certificado e CNAME. Application Administrator gerencia o proxy; Cloud Application Administrator não.

Provisionamento automático

Usa SCIM para criar e atualizar contas no SaaS; escopo por atribuições e filtros de escopo por atributo. Mapeamentos: Direct, Constant, Expression (até 10.000 caracteres, concatena e transforma) e None. Em quarentena os ciclos caem até um por dia e o trabalho é desabilitado após quatro semanas; teste a correção com Provision on demand.

Declarações no token

Add groups claim com Groups assigned to the application evita estourar o limite (150 grupos em SAML e 200 em JWT, incluindo aninhados). Funções de aplicativo vêm na declaração roles, não em groups.

Cloud Discovery do Defender for Cloud Apps

Compara logs com o catálogo de mais de 31.000 apps e mais de 90 fatores de risco; a pontuação é média ponderada de General, Security, Compliance e Legal. Snapshot é upload manual pontual; contínuo vem do coletor de logs Docker, do Defender for Endpoint (inclusive fora da rede) ou de gateways. Unsanctioned + Defender for Endpoint bloqueia; anonimização criptografa nomes com resolução auditada.

Políticas do Defender for Cloud Apps

Acesso bloqueia a entrada inteira; sessão permite e controla (Monitor only, Block activities, Control file download/upload), ambas exigem política de AC roteando ao app control. Atividade alerta e suspende por volume; OAuth alerta e bane permissões; descoberta avisa sobre apps novos (snapshot não dispara); anomalias vêm habilitadas com sete dias de aprendizado. Conectores de aplicativo dão visibilidade por API.

Macetes para memorizar

💡 Tipos de identidade gerenciada

Sistema nasce e morre com o recurso; usuário é avulsa e compartilhável.

💡 Funções de identidade gerenciada

Contributor Cria, Operator Ope-ra a associação.

💡 Delegada x aplicativo

Com usuário: escopo (Expose an API). Sem usuário: app role (Applications) e .default.

💡 Três propriedades do app

Enabled desliga tudo; Assignment escolhe quem; Visible só esconde.

💡 Políticas do Defender for Cloud Apps

Acesso fecha a porta; sessão vigia a sala; atividade conta ações; OAuth olha permissões; descoberta olha apps novos.

💡 SSO de app local pelo proxy

Lê cabeçalho = Header-based; usa Windows integrado = KCD.

Tabela de memorização: não confunda

Quando é...	...e quando é
Identidade gerenciada atribuída pelo sistema Identidade própria que deve morrer junto com o recurso.	**Identidade gerenciada atribuída pelo usuário** Mesma identidade e permissão para vários recursos, criada antes, mantida quando o recurso é recriado ou em recursos efêmeros em massa.
Managed Identity Contributor Criar e gerenciar identidades atribuídas pelo usuário.	**Managed Identity Operator** Associar uma identidade existente a um recurso (junto com Virtual Machine Contributor na VM).
Expose an API (escopo) Permissão delegada usada por cliente com usuário conectado.	**App roles com Applications** Permissão para serviço sem usuário, entregue na declaração roles.

Assignment required = Yes Restringir quem consegue obter token para o app.	**Visible to users = No** Só esconder o app do My Apps e do iniciador, sem bloquear.
Application Administrator Administrar apps e registros incluindo o application proxy.	**Cloud Application Administrator** Mesmas permissões, exceto gerenciar o application proxy.
Política de acesso (app control) Bloquear por completo o acesso de dispositivos não gerenciados.	**Política de sessão (app control)** Permitir o acesso e só bloquear download, upload ou atividades.
Header-based sign-on App local que identifica o usuário por cabeçalhos HTTP.	**Kerberos Constrained Delegation** App local com Autenticação Integrada do Windows e SPN registrado.

Números que caem

Item	Valor
Restauração de registro de aplicativo excluído	**Até 30 dias em Deleted applications**
Certificado SAML gerado automaticamente	**Válido por três anos**
Limite de grupos no token	**150 em SAML e 200 em JWT, incluindo aninhados**
Expressões de mapeamento de atributos	**Até 10.000 caracteres**
Quarentena do provisionamento	**Ciclos até um por dia; desabilitado após mais de quatro semanas**
Catálogo do Cloud Discovery	**Mais de 31.000 apps e mais de 90 fatores de risco; notas de 0 a 10**
Detecção de anomalias	**Aprendizado inicial de sete dias; mais de 30 indicadores**
Política de atividade	**Pode levar até 15 minutos para entrar em vigor**
Políticas de descoberta	**Alerta uma vez a cada 90 dias por app por relatório contínuo**
Coletor de logs Docker	**250 GB de disco, 2 núcleos, 4 GB de RAM; alerta após 48 horas sem dados**
Property lock padrão	**Habilitado em apps novos desde junho de 2026**
Versão da API do IMDS	**2018-02-01 ou superior**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Dar Application Administrator ou Cloud Application Administrator para consentir Mail.Read de aplicativo do Graph.
Como não cair: Essas funções não consentem permissões de aplicativo do Microsoft Graph; é preciso Privileged Role Administrator.

⚠ **Alerta de prova:** Criar a permissão delegada em App roles ou em API permissions.
Como não cair: Escopo delegado é criado em Expose an API; API permissions lista o que o app pede a outras APIs.

⚠ **Alerta de prova:** Atribuir a função de app ao grupo pai esperando que os grupos aninhados herdem.
Como não cair: Atribuição de grupo a aplicativo não suporta aninhamento; atribua os subgrupos diretamente.

⚠ **Alerta de prova:** Usar Managed Identity Operator para criar a identidade, ou Contributor para associar.
Como não cair: Contributor cria e gerencia; Operator associa a recursos.

⚠ **Alerta de prova:** Habilitar identidade gerenciada no servidor local ou no executor do GitHub.
Como não cair: Identidades gerenciadas só existem em recursos de computação do Azure; use gMSA, entidade de serviço com certificado ou federação de identidade de workload.

⚠ **Alerta de prova:** Conceder User.Read à identidade gerenciada para ler blobs.
Como não cair: Acesso a dados vem de função do Azure no recurso, como Storage Blob Data Reader.

⚠ **Alerta de prova:** Usar Passthrough no application proxy mantendo Acesso Condicional.
Como não cair: Com Passthrough o usuário não autentica no Entra, então não há MFA nem Acesso Condicional.

⚠ **Alerta de prova:** Revogar consentimentos de usuário pela aba User consent do portal.
Como não cair: Pelo portal só se revoga Admin consent; consentimento de usuário se revoga com Graph ou PowerShell.

⚠ **Alerta de prova:** Editar a data de expiração do certificado SAML ou excluí-lo esperando outro automático.
Como não cair: A data não pode ser alterada e excluir o ativo interrompe o SSO; crie novo, envie ao app e ative.

⚠ **Alerta de prova:** Adicionar um grupo como proprietário do aplicativo empresarial.
Como não cair: Grupos não podem ser proprietários de aplicativos empresariais; adicione o usuário.

⚠ **Alerta de prova:** Marcar o app como Unsanctioned achando que isso sozinho bloqueia.
Como não cair: O bloqueio automático depende do Defender for Endpoint ou de gateways integrados.

⚠ **Alerta de prova:** Esperar que relatórios snapshot disparem políticas de descoberta.
Como não cair: Só relatórios contínuos disparam, uma vez a cada 90 dias por app por relatório contínuo.

⚠ **Alerta de prova:** Achar que o designado como revisor no fluxo de consentimento já pode aprovar.
Como não cair: A designação não eleva privilégios; o revisor precisa de função que conceda o consentimento.

⚠ **Alerta de prova:** Usar mapeamento Constant para limitar quem é provisionado.
Como não cair: Constant grava valor fixo; quem entra no provisionamento é definido por filtro de escopo.

Como cai na prova

📝 **Como cai:** Workload precisa acessar recurso sem segredos; escolha a identidade.
Como resolver: Pergunte: está no Azure? Se não, gMSA (local Windows) ou entidade de serviço com certificado ou federação. Se sim, ciclo de vida junto do recurso = sistema; compartilhada ou criada antes = usuário.

📝 **Como cai:** Função mínima para criar, associar ou habilitar identidade gerenciada.
Como resolver: Criar = Managed Identity Contributor; associar = Managed Identity Operator (+ Virtual Machine Contributor); habilitar a de sistema = Virtual Machine Contributor. Descarte funções do Entra.

📝 **Como cai:** Usuários não conseguem consentir ou quem consente uma permissão.
Como resolver: Defina o tipo de permissão: aplicativo exige administrador; Graph de aplicativo exige PRA; com o consentimento com elevação baseado em risco, usuários não consentem a maioria dos apps multilocatário sem editor verificado que pedem permissões além das básicas (resolva com verificação do editor).

📝 **Como cai:** Escolher o tipo de SSO ou a pré-autenticação do proxy a partir da descrição do app.
Como resolver: Mapeie a característica: SAML suportado, login HTML, só link, cabeçalhos, Windows integrado. Se pede MFA e AC antes do app publicado, pré-autenticação Microsoft Entra ID.

📝 **Como cai:** Requisito no Defender for Cloud Apps com quatro tipos de política.
Como resolver: Bloquear tudo = acesso; limitar ações = sessão; volume de atividade = atividade; permissões concedidas = OAuth; app novo nos logs = descoberta.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Centenas de VMs criadas e destruídas por hora, erro HTTP 429	**Identidade gerenciada atribuída pelo usuário compartilhada**
Identidade deve deixar de existir junto com a VM	**Identidade gerenciada atribuída pelo sistema**
GitHub Actions com segredo que expira	**Federação de identidade de workload**
Serviço Windows em três servidores locais com balanceamento	**gMSA**
Serviço sem usuário conectado chamando o Graph com credenciais do cliente	**Permissão de aplicativo, scope recurso/.default, consentimento de administrador**
Esconder o app do My Apps sem parar o funcionamento	**Visible to users = No**
Parar a emissão de tokens de um app comprometido sem excluir	**Enabled for users to sign-in = No**
Portal com login HTML, sem SAML	**SSO baseado em senha**
App já com SSO no AD FS que só precisa aparecer no My Apps	**Linked sign-on**
Combinar sobrenome e nome no displayName de destino	**Mapeamento Expression**
Provisionamento parado por credenciais inválidas	**Quarentena; corrigir e testar com Provision on demand**
Bloquear download em dispositivo não gerenciado, mantendo o acesso	**Política de sessão + AC roteando ao app control**
Alerta quando muitos usuários autorizam app OAuth de permissão alta	**Política de aplicativo OAuth**
Selo azul de editor no aviso de consentimento	**Verificação do editor com PartnerID do AI Cloud Partner Program**

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

- Identidade gerenciada autentica; a autorização vem de função do Azure no recurso.
- Permissão de aplicativo do Microsoft Graph só é consentida por Privileged Role Administrator.
- Assignment required controla token; Visible to users só exibição; Enabled for users to sign-in desliga tudo.
- Atribuição de grupo a aplicativo não aceita aninhamento.
- Política de acesso bloqueia; política de sessão permite e controla.

Essenciais para a prova (checklist)

☐ Sei escolher entre identidade gerenciada de sistema, de usuário, gMSA, entidade de serviço com certificado e federação de identidade de workload.

☐ Sei as funções do Azure para criar, associar e habilitar identidades gerenciadas.

☐ Sei a diferença entre objeto de aplicativo e entidade de serviço em apps multilocatário.

☐ Sei publicar escopos em Expose an API e criar funções de aplicativo para serviços sem usuário.

☐ Sei quem concede consentimento de administrador e qual é a configuração recomendada de consentimento do usuário.

☐ Sei o efeito de Enabled for users to sign-in, Assignment required e Visible to users.

☐ Sei escolher entre SAML, senha, vinculado, cabeçalho e KCD e configurar o certificado SAML.

☐ Sei configurar o application proxy com pré-autenticação, grupos de conectores e domínio personalizado.

☐ Sei configurar provisionamento com SCIM, filtros de escopo, mapeamentos e tratar quarentena.

☐ Sei qual política do Defender for Cloud Apps atende cada requisito e como o Cloud Discovery coleta dados.

Questões de revisão do capítulo

R4.1 · Planejar e implementar identidades de carga de trabalho

A equipe de desenvolvimento do Clube de Vantagens Mais Pontos está registrando um aplicativo React executado inteiramente no navegador e quer configurar onde os tokens serão entregues após a autenticação. Qual plataforma selecionar em Authentication?

A. Mobile and desktop applications, escolhendo um URI de redirecionamento sugerido
B. iOS / macOS, informando o Bundle ID que gera o URI de redirecionamento
C. Single-page application, informando o URI de redirecionamento manualmente
D. Android, informando o nome do pacote e o hash de assinatura do aplicativo

R4.2 · Planejar e implementar identidades de carga de trabalho

O auditor da Companhia de Gás Brasa Viva quer garantir que nenhuma pessoa da equipe consiga copiar a credencial usada pela identidade gerenciada de uma VM. O que a documentação informa sobre credenciais de identidades gerenciadas?

A. As credenciais não ficam acessíveis a ninguém e são gerenciadas pela plataforma
B. As credenciais ficam no Key Vault da assinatura e podem ser lidas pelo Owner dela
C. As credenciais são um segredo exibido uma única vez ao habilitar a identidade
D. As credenciais são um certificado que o administrador renova a cada ano

R4.3 · Planejar e implementar identidades de carga de trabalho

A Prefeitura de Vila Serena publicou pelo Microsoft Entra application proxy um sistema local antigo que identifica o usuário por cabeçalhos HTTP enviados por um produto de acesso legado. A equipe quer pré-autenticação no Microsoft Entra ID e SSO sem mudar o sistema. Qual método de SSO escolher?

A. Linked sign-on, criando no My Apps um link para a página do produto legado de acesso
B. Password-based sign-on, guardando no cofre a senha que o sistema local espera receber
C. Header-based sign-on, com os valores dos cabeçalhos definidos com base nas declarações
D. Kerberos Constrained Delegation, com os conectores autorizados a representar usuários

R4.4 · Planejar e implementar identidades de carga de trabalho

A Universidade Aberta do Sul quer provisionar contas para um SaaS de biblioteca que segue o padrão SCIM. Qual é a base do provisionamento automático do Microsoft Entra ID para esse tipo de aplicativo?

A. O protocolo LDAP, usado pelo agente do Connect Sync local
B. O protocolo SAML, usado para enviar as contas no momento da primeira entrada do aluno
C. O protocolo WS-Federation, usado para replicar as contas a cada ciclo de sincronização
D. O padrão SCIM, usado pelo serviço de provisionamento para criar e atualizar contas

Respostas comentadas

R4.1. C) Single-page application, informando o URI de redirecionamento manualmente

Por quê: O URI de redirecionamento é para onde a plataforma de identidade envia os tokens; ele é configurado na página Authentication do registro. Para Web e SPA, informa-se o URI; para plataformas móveis, ele é gerado a partir de dados do aplicativo.

✗ A) Incorreta. Essa plataforma serve a aplicativos desktop ou móveis que não usam MSAL ou um agente.
✗ B) Incorreta. A plataforma iOS / macOS é para aplicativos Apple nativos.
✗ D) Incorreta. A plataforma Android é para aplicativos Android nativos.

> **Dica de prova:** App React no navegador: plataforma Single-page application.

R4.2. A) As credenciais não ficam acessíveis a ninguém e são gerenciadas pela plataforma

Por quê: Identidades gerenciadas permitem obter tokens do Microsoft Entra sem gerenciar credenciais e podem substituir segredos, chaves de acesso e certificados entre serviços, sem custo adicional.

✗ B) Incorreta. As credenciais não são guardadas em um cofre acessível ao cliente.
✗ C) Incorreta. Não há segredo exibido para a identidade gerenciada.
✗ D) Incorreta. O administrador não renova certificados de identidades gerenciadas.

> **Dica de prova:** Identidade gerenciada: credencial inacessível, gerida pela plataforma.

R4.3. C) Header-based sign-on, com os valores dos cabeçalhos definidos com base nas declarações

Por quê: O SSO baseado em cabeçalho do application proxy usa os conectores de rede privada existentes, sem software adicional, e aceita os mesmos atributos e transformações disponíveis para declarações SAML ou OIDC.

✗ A) Incorreta. Linked sign-on só cria um link e não adiciona SSO ao aplicativo.
✗ B) Incorreta. SSO por senha preenche formulários de login; o sistema descrito espera cabeçalhos.
✗ D) Incorreta. KCD atende aplicativos com Autenticação Integrada do Windows, não aplicativos que leem cabeçalhos HTTP.

> **Dica de prova:** App local que lê cabeçalhos HTTP: application proxy com header-based sign-on.

R4.4. D) O padrão SCIM, usado pelo serviço de provisionamento para criar e atualizar contas

Por quê: O provisionamento automático pode usar atribuições de usuários e grupos e filtros de escopo para definir quem é provisionado, além de mapeamentos de atributos para transformar dados.

✗ A) Incorreta. O Connect Sync sincroniza o AD com o Microsoft Entra ID, não provisiona SaaS.
✗ B) Incorreta. SAML trata de SSO; o provisionamento usa SCIM.
✗ C) Incorreta. WS-Federation é protocolo de federação, não de provisionamento.

> **Dica de prova:** Provisionamento automático para SaaS: padrão SCIM.

DIA DA PROVA

Estratégia de prova

O SC-300 tem 100 minutos e a Microsoft não divulga o número exato de questões (conte com cerca de 50), de múltipla escolha e múltipla resposta, com nota de 1 a 1000 e mínimo de 700. Quase todo enunciado é um cenário de empresa com um requisito de negócio e pede a configuração, a função ou o recurso exato no Microsoft Entra, muitas vezes com o nome da opção em inglês. As alternativas erradas são recursos reais usados no contexto errado, recursos aposentados ou opções que exigem mais privilégio que o necessário. Autenticação e acesso pesa mais (25-30%); os outros três domínios ficam em 20-25% cada. O guia vigente é o de 28 de outubro de 2026, com mudanças em autenticação de usuários, Global Secure Access e acesso privilegiado.

Como responder

✓ Leia a última frase primeiro para saber se pede recurso, função mínima, sequência ou comportamento padrão, e só então volte aos detalhes do cenário.

✓ Sublinhe as restrições do enunciado (menor privilégio, sem excluir, sem listas de IP, sem convidados, por grupo); cada uma costuma eliminar uma alternativa.

✓ Quando o enunciado diz menor privilégio, descarte Global Administrator e funções de escopo de locatário se houver opção mais estreita (função específica, unidade administrativa, proprietário).

✓ Desconfie de alternativas com recursos aposentados ou removidos (fraud alert, Require approved client app, tempo de vida configurável de token, módulo AzureAD).

✓ Em múltipla resposta (Escolha DUAS ou TRÊS), avalie cada afirmação isoladamente como verdadeira ou falsa contra a regra fixa do recurso.

✓ Em perguntas de licença, lembre o mapa: Acesso Condicional, proteção de senha personalizada e termos de uso em P1; ID Protection completo e PIM em P2; revisões e pacotes avançados em ID Governance; controles por risco de identidades de workload em Workload Identities Premium.

✓ Para sequências (ações protegidas, troca de grupo licenciado, certificado SAML), confira a ordem: a alternativa com os passos certos na ordem errada é distrator comum.

✓ Gerencie o tempo: com cerca de dois minutos por item, marque cenários longos para revisão e não deixe nenhum em branco.

Erros que derrubam candidatos

✗ Confundir Report-only, What If e log de entradas na hora de medir impacto ou diagnosticar bloqueio.

✗ Trocar configurações de entrada por saída no acesso entre locatários.

✗ Achar que funções do Microsoft Entra dão acesso a recursos do Azure (e vice-versa).

✗ Escolher a função mais poderosa em vez da mínima que atende (Application Administrator onde basta Application Developer, Global Administrator onde basta Authentication Administrator).

✗ Ignorar o comportamento padrão do recurso: forças internas não editáveis, unidades administrativas sem aninhamento, aprovação do PIM de 24 horas fixas.

✗ Confundir revisores alternativos de revisões com aprovadores alternativos de pacotes de acesso.

✗ Usar Visible to users ou coleções para restringir acesso, quando o controle real é Assignment required.

Na semana da prova

- ☐ Volte aos temas em que mais errou e explique com suas palavras por que cada recurso parecido não atende ao requisito.
- ☐ Revise as tabelas de números de cada capítulo (retenção de logs, limites do TAP, 50 dispositivos, 500 exclusões, 30 dias de restauração).
- ☐ Monte uma folha com pares que a prova confunde: entrada x saída, sistema x usuário, acesso x sessão, Dismiss x Confirm safe, Enabled x Microsoft managed.
- ☐ Dedique um dia extra a autenticação e acesso, que tem o maior peso.
- ☐ Na véspera, revise só os tópicos marcados em lembrar e os macetes; não comece assunto novo.
- ☐ No dia, confirme o agendamento e chegue (ou conecte-se) com antecedência para não perder minutos dos 100 disponíveis.

REVISÃO FINAL

Folha de cola

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

1. Implementar e gerenciar identidades de usuários

‣ Único Owner da assinatura saiu e o Global Administrator não consegue atribuir funções → **Elevar acesso: Access management for Azure resources**

‣ Blindar objetos até de administradores de locatário → **Unidade administrativa de gerenciamento restrito**

‣ Todas as funções de um usuário, inclusive via grupos e escopos → **Users > usuário > Assigned roles**

‣ Convidado sem Entra ID e sem conta Microsoft sendo levado a criar conta pessoal → **Código de acesso único por e-mail**

‣ Convidado trocou de empresa ou e-mail mantendo os acessos → **Redefinir o status de resgate**

⚠ Funções do Entra não concedem acesso ao Azure; use a elevação de acesso (User Access Administrator na raiz).

⚠ Funções internas não são clonadas nem editadas; crie função personalizada a partir das permissões.

⚠ Unidades administrativas não aninham; crie uma por recorte e atribua os escopos.

2. Implementar o gerenciamento de autenticação e acesso

‣ Perdeu o celular e precisa registrar uma passkey hoje → **Temporary Access Pass criado por Authentication Administrator**

‣ Cartão inteligente como multifator e certificado de software como fator único → **Regras de associação de autenticação da CBA por OID de política**

‣ Regras de passkey diferentes por grupo (atestado, modelos aprovados) → **Perfis de passkey com tipo, atestado e AAGUID**

‣ Usuários aprovam notificações por engano (fadiga de MFA) → **Correspondência de número, sempre ativa em todo push**

‣ Usuários com e sem senha, risco de usuário alto → **Require risk remediation**

⚠ Forças internas não podem ser modificadas; crie força personalizada com só as combinações aceitas.

⚠ Foram removidos em 1º de março de 2025; a denúncia de prompt suspeito é Report suspicious activity nos métodos de autenticação.

⚠ Esse recurso foi aposentado; a orientação é desligar Remember MFA on trusted devices antes de usar Sign-in frequency.

3. Planejar e automatizar a governança de identidade

‣ Excesso de prompts de MFA ao longo do dia → **Workbook Authentication Prompts Analysis**

‣ Entradas não cobertas por nenhuma política de AC → **Workbook Conditional Access Gap Analyzer**

‣ Abuso de aplicativos e credenciais adicionadas a entidades de serviço → **Workbook Sensitive Operations Report**

‣ Indicador percentual de postura de identidade, até na edição Free → **Identity Secure Score (recalculado a cada 24 horas)**

‣ Quem já está apto a MFA, passwordless e SSPR → **Authentication methods > Activity (Registration e Usage)**

⚠ PIM para recursos do Azure exige Owner ou User Access Administrator no recurso.

⚠ PRA é requisito para funções do Entra; para Azure resources é Owner ou User Access Administrator.

⚠ Sem aplicação automática, as decisões só valem com Apply em Review History; excluir não aplica e Reset apaga decisões.

4. Planejar e implementar identidades de carga de trabalho

‣ Centenas de VMs criadas e destruídas por hora, erro HTTP 429 → **Identidade gerenciada atribuída pelo usuário compartilhada**

‣ Identidade deve deixar de existir junto com a VM → **Identidade gerenciada atribuída pelo sistema**

‣ GitHub Actions com segredo que expira → **Federação de identidade de workload**

‣ Serviço Windows em três servidores locais com balanceamento → **gMSA**

‣ Serviço sem usuário conectado chamando o Graph com credenciais do cliente → **Permissão de aplicativo, scope recurso/.default, consentimento de administrador**

⚠ Essas funções não consentem permissões de aplicativo do Microsoft Graph; é preciso Privileged Role Administrator.

⚠ Escopo delegado é criado em Expose an API; API permissions lista o que o app pede a outras APIs.

⚠ Atribuição de grupo a aplicativo não suporta aninhamento; atribua os subgrupos diretamente.

GABARITO

Respostas do diagnóstico

D1. A) A CLI do Azure não é suportada para atribuições de funções do Microsoft Entra → revise o capítulo 1

Por quê: Uma atribuição de função é composta de entidade de segurança (usuário, grupo ou entidade de serviço), definição de função e escopo. Funções do Microsoft Entra e do Azure são sistemas separados.

✗ B) Incorreta. O centro de administração, o Graph PowerShell e a API do Graph são os métodos suportados.

✗ C) Incorreta. Owner é função do Azure e não habilita a CLI para funções do Microsoft Entra.

✗ D) Incorreta. Não há suporte da CLI do Azure em nenhum escopo para funções do Microsoft Entra.

> **Dica de prova:** Atribuir função do Entra por script: Graph PowerShell ou API, não CLI do Azure.

D2. B) Renovar a chave de descriptografia Kerberos com Update-AzureADSSOForest ao menos a cada 30 dias → revise o capítulo 1

Por quê: Executar Update-AzureADSSOForest mais de uma vez por floresta faz o recurso parar até os tíquetes Kerberos expirarem e serem reemitidos. São necessárias credenciais de administrador de domínio e de Hybrid Identity Administrator.

✗ A) Incorreta. Excluir e recriar a conta não é o procedimento documentado e interromperia o SSO.

✗ C) Incorreta. Contas de computador não usam MFA por usuário.

✗ D) Incorreta. A conta fica no AD local; unidades administrativas do Entra não a protegem.

> **Dica de prova:** SSO contínuo: renove a chave Kerberos da conta AZUREADSSOACC a cada 30 dias.

D3. B) Usar lista de permissão com os três domínios; os demais ficam bloqueados → revise o capítulo 1

Por quê: As restrições de colaboração ficam em External collaboration settings. Há uma política por organização, limitada a 25 KB. Listas e configurações de acesso entre locatários são verificadas no momento do convite; convites pendentes de domínios bloqueados falham no resgate.

✗ A) Incorreta. Não é possível configurar os dois tipos de lista ao mesmo tempo.

✗ C) Incorreta. A lista do Microsoft Entra funciona de forma independente das listas do OneDrive e do SharePoint.

✗ D) Incorreta. A lista não se aplica a usuários externos que já resgataram o convite.

> **Dica de prova:** Convites só para parceiros: lista de permissão (uma lista por vez).

D4. B) Authenticator habilitado com modo Any ou Push e usuários no escopo do método → revise o capítulo 2

Por quê: A campanha de registro incentiva, após o MFA, o registro de passkey ou do Authenticator (um método por vez). Pode ser Microsoft managed, Enabled ou Disabled; políticas de Acesso Condicional de registro de informações de segurança se aplicam antes do incentivo.

✗ A) Incorreta. A política de registro de MFA do ID Protection é outro recurso e não é pré-requisito da campanha.

✗ C) Incorreta. A documentação da campanha não exige licença P2 por usuário.

✗ D) Incorreta. Com o modo Passwordless, os usuários não são elegíveis para o incentivo.

> **Dica de prova:** Campanha do Authenticator: modo Any ou Push; Passwordless não recebe o incentivo.

D5. B) O TAP tem preferência sobre a federação, e o aluno autentica no Microsoft Entra ID → revise o capítulo 2

Por quê: O uso mais comum do TAP é registrar métodos de autenticação na primeira entrada ou na configuração do dispositivo. Quem atualizar métodos por perda do dispositivo deve remover os métodos antigos.

✗ A) Incorreta. O TAP funciona em domínios federados.

✗ C) Incorreta. O usuário com TAP não é redirecionado ao IdP federado.

✗ D) Incorreta. O TAP não substitui a senha do usuário; é uma credencial temporária adicional.

> **Dica de prova:** TAP em domínio federado: autentica no Entra, sem ir ao IdP.

D6. D) Mapeando Principal Name para o userPrincipalName do usuário → revise o capítulo 2

Por quê: As associações de nome de usuário têm ordem de prioridade: se o campo existe no certificado mas nenhum usuário corresponde, a autenticação falha e a próxima associação é tentada. Atributos sincronizados (como certificateUserIds e userPrincipalName) podem ser alterados por quem administra o AD local.

✗ A) Incorreta. A validade do certificado não identifica o usuário.

✗ B) Incorreta. O emissor é usado em regras de associação de autenticação, não para identificar o usuário pelo department.

✗ C) Incorreta. O mapeamento padrão não usa número de série com objectId.

> **Dica de prova:** CBA, identificação padrão: Principal Name do certificado = userPrincipalName.

D7. B) Só são retidos se integrados a armazenamento ou análise pelas configurações de diagnóstico → revise o capítulo 3

Por quê: Na tabela de retenção, auditoria e entradas ficam 7 dias na edição Free e 30 dias com P1 ou P2; uso de MFA fica 30 dias. Para reter mais, use conta de armazenamento ou Log Analytics.

✗ A) Incorreta. Esses logs não estão disponíveis na edição Free.

✗ C) Incorreta. O Resource audit do PIM não contém chamadas ao Microsoft Graph.

✗ D) Incorreta. Diferentemente dos logs de entrada e de auditoria, esses logs não ficam retidos no portal.

> **Dica de prova:** Logs de atividade do Graph: só existem se exportados (diagnóstico).

D8. C) SigninLogs | where CreatedDateTime >= ago(7d) | summarize signInCount = count() by AppDisplayName | sort by signInCount desc → revise o capítulo 3

Por quê: Depois de integrar os logs ao Log Analytics, as tabelas SigninLogs, AuditLogs e AADProvisioningLogs podem ser consultadas com KQL; também é possível agrupar registros por CorrelationId para ver o status final de uma entrada.

✗ A) Incorreta. Essa consulta lista os eventos de auditoria mais frequentes, não entradas por aplicativo.

✗ B) Incorreta. Essa consulta busca entradas arriscadas, sem contar por aplicativo.

✗ D) Incorreta. Essa consulta resume eventos de provisionamento por ação e por dia.

> **Dica de prova:** Top aplicativos por entradas: SigninLogs | summarize count() by AppDisplayName.

D9. D) Testar periodicamente se as contas entram e guardar as chaves em cofres separados → revise o capítulo 3

Por quê: Os testes devem avisar a equipe de monitoramento, revisar quem está autorizado, manter o processo documentado, treinar os responsáveis e confirmar que os alertas de uso são disparados.

✗ A) Incorreta. Os métodos não devem depender do dispositivo de uma só pessoa.
✗ B) Incorreta. As contas devem ser excluídas de políticas que bloqueiam ou restringem a entrada.
✗ C) Incorreta. As contas não devem ser associadas a dispositivos pessoais de funcionários.

> **Dica de prova:** Contas de emergência: testes periódicos e chaves em cofres separados.

D10. D) Em Expose an API, definir o URI de ID do aplicativo e adicionar o escopo → revise o capítulo 4

Por quê: Expor uma API cria escopos (permissões delegadas) que aplicativos clientes solicitam em API permissions. O campo Who can consent define se usuários e administradores ou somente administradores podem consentir.

✗ A) Incorreta. Segredos são credenciais do aplicativo e não definem permissões.
✗ B) Incorreta. API permissions lista as permissões que o próprio aplicativo solicita a outras APIs, e Cooperados.Read não é permissão do Microsoft Graph.
✗ C) Incorreta. Funções de aplicativo com tipo Applications representam permissões de aplicativo, não permissões delegadas.

> **Dica de prova:** Publicar permissão delegada da sua API: Expose an API + escopo.

D11. C) Definir Who can consent = Admins only ao adicionar o escopo → revise o capítulo 4

Por quê: Cada escopo tem nome (convenção recurso.operação.restrição), quem pode consentir, nomes e descrições para administradores e usuários e estado. O URI de ID do aplicativo é o prefixo dos escopos.

✗ A) Incorreta. Permitir que usuários consintam não é adequado para uma permissão de alto privilégio.
✗ B) Incorreta. Desligar a atribuição obrigatória amplia quem obtém token, sem controlar o consentimento.
✗ D) Incorreta. Funções de aplicativo para usuários aparecem na declaração roles; não definem quem consente com o escopo.

> **Dica de prova:** Escopo de alto privilégio: Who can consent = Admins only.

D12. A) Self-service application access no aplicativo, com aprovadores de negócio, e P1 ou P2 → revise o capítulo 4

Por quê: Usuários aprovados são adicionados a um grupo preconfigurado, e é possível atribuir automaticamente uma função de aplicativo. O recurso vale para aplicativos da galeria, do application proxy ou adicionados por consentimento.

✗ B) Incorreta. O fluxo de consentimento do administrador trata de permissões do aplicativo, não de acesso de usuários.
✗ C) Incorreta. Liberar o acesso a todos elimina a aprovação do bibliotecário.
✗ D) Incorreta. Um pacote sem aprovação não atende ao pedido de aprovação do bibliotecário.

> **Dica de prova:** Usuário pede app no My Apps com aprovação de negócio: Self-service application access.

Agora, treine no formato real

Faça as 6 provas completas do curso SC-300: 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.