Strecht Simulados · Guia de preparação



Guia de preparação AB-620

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

3 capítulos por domínio	**21** questões comentadas	**70%** nota de corte
6 provas completas no curso		

ANTES DE COMEÇAR

Como usar este guia

Este guia foi feito para ser estudado junto com as 6 provas completas do curso AB-620: o guia explica o que cai e onde estão as armadilhas; as provas treinam o ritmo e mostram o que você ainda não domina.

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

Mapa do exame

Cada prova do curso tem 50 questões e 120 minutos, no formato do exame. Referência de aprovação: 70%.

Domínio (capítulo)	Peso	Neste guia
1. Integrar e estender agentes no Copilot Studio	40-45%	18 conceitos · 14 pegadinhas
2. Planejar e configurar soluções de agente	30-35%	18 conceitos · 14 pegadinhas
3. Testar e gerenciar agentes	20-25%	17 conceitos · 14 pegadinhas

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

Estude um pouco todo dia, de graça

Instagram @strecht.simulados

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

Seguir no Instagram →

YouTube Strecht Simulados

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

Inscrever-se no canal →

DIAGNÓSTICO

Você já sabe isso?

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

D1 · Integrar e estender agentes no Copilot Studio

Um desenvolvedor da Fintech Moeda Certa vai conectar um servidor MCP remoto ao agente pelo assistente de ferramentas do Copilot Studio, o caminho recomendado pela Microsoft. Que informações o assistente pede antes de criar a conexão e adicionar o servidor ao agente?

A. Lista de ferramentas do servidor, com o esquema de cada entrada digitado à mão
B. Arquivo OpenAPI do servidor, com a extensão do protocolo e o caminho do endpoint
C. Comando de inicialização local do servidor e variáveis do processo em stdio
D. Nome, descrição e URL do servidor, além do tipo de autenticação exigido por ele

D2 · Integrar e estender agentes no Copilot Studio

O agente público da Concessionária Via Norte, sem login, tem uma ferramenta de conector que consulta a tabela de preços de revisão em uma API que exige conta. Os visitantes do site não têm conta nessa API, e o conteúdo é igual para todos. Como configurar a autenticação da ferramenta?

A. Usar Maker-provided credentials, com a conta da empresa na conexão
B. Pedir ao visitante a chave da API em uma pergunta do tópico de boas-vindas
C. Trocar a autenticação do agente para Authenticate with Microsoft
D. Usar End user credentials, para cada visitante entrar com a própria conta

D3 · Integrar e estender agentes no Copilot Studio

Depois que o administrador da Distribuidora Norte Frio aplicou uma política de dados ao ambiente, o botão Publish de um agente ficou indisponível, e um banner de erro com Details lista a fonte de conhecimento do SharePoint e os nós de respostas generativas que a usam. O que resolve?

A. Trocar a autenticação para Authenticate with Microsoft e publicar o agente de novo
B. Ajustar a política no Microsoft Purview, liberando o SharePoint para o Copilot Studio
C. Ajustar o conector de conhecimento do SharePoint na política de dados
D. Pedir ao suporte da Microsoft uma isenção da política para esse agente específico

D4 · Planejar e configurar soluções de agente

Na Fazenda Boa Safra, a ferramenta Registrar colheita, um conector, foi adicionada no nível do agente e às vezes é escolhida pelo orquestrador em conversas que não deveriam registrar nada. A equipe quer que ela rode só quando o tópico Fechamento do dia a chamar. O que configurar na ferramenta?

A. Apagar a descrição da ferramenta para o orquestrador não a ver
B. Desligar o controle Enabled da ferramenta na página Tools do agente
C. Definir Ask the end user before running como Yes nos detalhes
D. Desmarcar Allow agent to decide dynamically when to use the tool

D5 · Planejar e configurar soluções de agente

No agente da Farmacêutica Lumen, a moderação de conteúdo nas configurações de IA generativa está em High. No tópico de interações medicamentosas, o nó de respostas generativas deixa de responder perguntas legítimas sobre efeitos colaterais graves, e a equipe quer mais respostas só nesse tópico, sem mexer no resto do agente. Como configurar?

A. Reduzir a moderação nas propriedades do nó desse tópico, que prevalece sobre a do agente
B. Reduzir a moderação nas configurações de IA generativa do agente, que prevalece sobre a do nó
C. Trocar o agente para a orquestração clássica, que usa o nível de cada tópico
D. Mover o nó para o tópico Conversational boosting, que não aplica moderação

D6 · Planejar e configurar soluções de agente

No agente da Escola de Idiomas Fala Mais, o tópico Matrícula pergunta o nome do aluno e depois redireciona para o tópico Teste de nível, que também pergunta o nome. A equipe não quer repetir a pergunta nem criar variáveis globais. O que configurar?

A. Marcar a variável do nome no destino com Receive values from other topics e passá-la ao redirecionar
B. Converter a variável em global e, após o redirecionamento, voltar com ela ao escopo de tópico
C. Marcar a variável no tópico Matrícula com Return values to original topics
D. Criar uma entidade personalizada para o nome, que é compartilhada entre os tópicos

D7 · Testar e gerenciar agentes

Na Fertilizantes Solo Rico, os componentes dos agentes criados até agora têm nomes de esquema como cr8a3_pedido, e a governança quer o prefixo solo em tudo o que for criado daqui em diante. O que o desenvolvedor deve fazer?

A. Criar um publisher com prefixo solo e uma solução dele antes de novos itens
B. Editar o prefixo do publisher padrão do Dataverse para solo e salvar a solução
C. Exportar a solução como gerenciada, que aplica o prefixo do ambiente
D. Renomear os componentes existentes na solução, trocando cr8a3 por solo em cada um

D8 · Testar e gerenciar agentes

Os aprovadores das implantações da Indústria Química Ácido Leve pediram que cada solicitação venha com um resumo do que mudou na solução. No pipeline atual, o campo de notas de implantação aparece vazio para o maker. O que o administrador deve verificar?

A. Se o recurso Copilot do Power Platform admin center está ligado para todo o locatário
B. Se a pasta de notas foi criada na solução do agente e se o maker preencheu o arquivo
C. Se o pipeline usa implantação delegada, que é o requisito para gerar notas por IA
D. Se a opção AI deployment notes do pipeline está como Enabled no app Deployment Pipeline Configuration

D9 · Testar e gerenciar agentes

O maker da Autopeças Roda Firme vai criar um agente para o projeto Garantias e quer que o agente e todos os componentes que ele criar depois entrem sozinhos na solução Garantias. A solução preferencial dele aponta para a solução de outro projeto, que ele continua usando, e ele quer evitar o uso de Add required objects antes de cada exportação. O que ele deve fazer ao criar o agente?

A. Criar o agente e, antes de exportar, publicá-lo para levar os componentes à solução certa
B. Criar o agente na solução padrão e exportá-la depois como uma solução gerenciada
C. Abrir Agent settings na criação e escolher a solução Garantias em Advanced settings
D. Criar o agente e um patch da solução Garantias para cada componente novo do agente

01

CAPÍTULO 1 · 40-45% DA PROVA

Integrar e estender agentes no Copilot Studio

Este é o domínio de maior peso (40-45%) e o mais extenso: fontes de conhecimento corporativas, ferramentas (MCP, REST API, conectores personalizados, computer use), colaboração entre agentes (filhos, conectados, Foundry, Fabric, A2A, Agents SDK) e integração com Azure (Azure AI Search, modelos do Foundry nos prompts, Application Insights). Cai como cenário de integração com uma restrição forte: não copiar dados, respeitar permissão de cada usuário, sem servidor próprio, sem chave de API, rede privada. Muitas questões citam um erro literal, como HTTP 400 sobre Activity, 404 Version not found ou CuaInsertCredentialNotAllowedInInsecureWebsites, e eu preciso associar a mensagem à causa. Onde mais erro é trocar protocolos (MCP x A2A x Activity), confundir Copilot connector com conhecimento em tempo real e esquecer onde cada coisa é configurada (Microsoft 365 admin center, Azure, Fabric, Copilot Studio).

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

Tópicos-chave

Copilot connectors como conhecimento

São os antigos Microsoft Graph connectors: o administrador os configura no Microsoft 365 admin center e eles copiam e indexam o conteúdo externo no Microsoft Graph com as permissões da origem. No agente entram por Add knowledge, e se não aparecerem entre as opções em destaque é preciso abrir Advanced. Nos canais publicados com autenticação manual, inclua o escopo ExternalItem.Read.All. O rastreamento completo trata exclusões e permissões; o incremental só pega novos ou alterados, com frequência mínima de 15 minutos, e o tenant graph grounding com busca semântica melhora a recuperação, cobrado à parte em Copilot Credits.

Conhecimento em tempo real por conectores da Power Platform

Salesforce, ServiceNow, Snowflake, Zendesk e Azure SQL são consultados na fonte a cada pergunta com o token de cada usuário, sem copiar dados; só metadados como tabelas e colunas são indexados (status In progress até Ready). Sinônimos e glossário existem hoje só para ServiceNow e Zendesk. Passam na moderação as perguntas de recuperação de dados; falham alterações, buscas de texto dentro dos registros, perguntas de suporte e de como fazer, sem mensagem de erro detalhada. Artigos de base de conhecimento (como a tabela Knowledge Article) entram pela opção Your connections, como base não estruturada.

Azure AI Search como conhecimento

Use um índice vetorial com vetorização integrada, criado com Import and vectorize data, para que a pergunta seja vetorizada pelo mesmo modelo de embedding; cada fonte aceita um único índice vetorial. A conexão aceita Access Key (endpoint e Admin Key), Client Certificate Auth, Service principal e Microsoft Entra ID Integrated. O semantic ranker é configurado no próprio Azure AI Search, citações exigem metadata_storage_path ou um campo com a URL completa, e índice atrás de ponto de extremidade privado exige suporte a Virtual Network no ambiente. Conexão criada à mão fora do caminho suportado pode gravar uma conexão com defeito no ambiente, recuperada redefinindo o acesso externo ou recriando o agente com Entra ID.

Arquivos, Foundry IQ e On Your Data

Um agente aceita até 500 arquivos carregados, sem escolha de modelo de embedding nem de tamanho dos trechos, o que torna o Azure AI Search melhor para acervos grandes. Uma base do Foundry IQ empacota fontes com a configuração de recuperação e relevância, entra como ferramenta e cada agente aceita uma única conexão do Foundry IQ, ajustada no Foundry. O Azure OpenAI On Your Data (opção Classic data do nó de respostas generativas) será aposentado em 14 de outubro de 2026, com migração para o Foundry Agent Service com Foundry IQ.

Conectar um servidor MCP

O agente é cliente de servidores MCP remotos: o assistente, caminho recomendado, pede nome, descrição, URL e tipo de autenticação, e as ferramentas são lidas dinamicamente. A autenticação pode ser None, API key (cabeçalho ou query) ou OAuth 2.0 nos tipos Dynamic discovery, Dynamic (registro dinâmico sem descoberta, com Authorization URL e Token URL template) ou Manual. O transporte suportado é o Streamable; SSE deixou de ser aceito após agosto de 2025, e servidor stdio local precisa virar serviço remoto com URL. No caminho alternativo, o conector personalizado tem uma operação POST com x-ms-agentic-protocol igual a mcp-streamable-1.0.

Ferramentas e recursos MCP no agente

A página do servidor mostra Tools e Resources; os prompts publicados pelo servidor MCP não são suportados. Um recurso só chega ao agente quando uma ferramenta do servidor o devolve como saída. Desligando Allow all, cada ferramenta ganha um botão próprio e ferramentas novas chegam desligadas. Entradas definidas por referência a outro esquema são filtradas, tipos múltiplos num array truncam o esquema e enumerações viram texto; o Microsoft Dataverse MCP Server é um servidor pronto listado em Model Context Protocol.

Ferramenta REST API

Pede a especificação OpenAPI em arquivo JSON; a base é a versão 2.0 e uma 3.0 é traduzida para 2.0, mas YAML não é convertido. A autenticação é None, API key (Parameter label, Parameter name e Parameter location Header ou Query, com o usuário informando a chave) ou OAuth 2.0 (Client ID, Client secret, Authorization URL, Token URL, Refresh URL, Scope e a escolha My organization only). O desenvolvedor seleciona só as operações que quer expor; entradas e saídas vêm da especificação e só as descrições são editáveis e obrigatórias. Solution em branco cria uma solução com o nome da ação e o publisher padrão, e no fim cada ferramenta ainda precisa de conexão e de Add and configure no agente.

Conector personalizado como ferramenta

O conector existe no ambiente onde foi criado no Power Apps; para outros ambientes ele viaja em solução, junto com as referências de conexão. Em conectores de solução, variáveis de ambiente preenchem Host, Base URL, Client ID, Client Secret e URLs de login e refresh pela sintaxe @environmentVariables, e o valor é aplicado quando o conector é salvo, então mudar a variável exige salvá-lo de novo. A política de dados classifica conectores personalizados em Business, Non-business ou Blocked, e conectores de grupos diferentes não são usados juntos; host e basePath da definição OpenAPI 2.0 formam o endereço chamado.

Conclusão e credenciais da ferramenta

Em Completion, Don't respond (padrão) deixa o agente incorporar a saída na própria resposta; também há resposta gerada por IA, Send specific response com variáveis de saída e cartão adaptável. A autenticação da ferramenta é End user (padrão) ou Maker-provided credentials, esta para dado igual para todos quando os usuários não têm conta no serviço. Description em Additional details é o texto mostrado ao usuário quando a ferramenta pede para ele entrar. Em Settings, Connection Settings, uma conexão Expired que gera 401 precisa ser reautenticada.

Ferramenta computer use

Opera interfaces gráficas de sites e apps Windows com um modelo de visão, onde não há API ou conector; exige orquestração generativa e não pode ser chamada a partir de tópico. Nome, descrição, modelo e instruções são obrigatórios, e instruções com URL completa, passos em ordem e nomes exatos de botões aumentam a precisão; valores que mudam a cada execução entram como entradas da ferramenta. O modelo pode ser o CUA da OpenAI ou modelos da Anthropic, que exigem liberação de modelos externos no ambiente pelo administrador, e cada etapa executada consome Copilot Credits.

Execução, credenciais e controle do computer use

Roda em hosted browser (sem acesso corporativo), em Cloud PC pool do Windows 365 for Agents (Entra, Intune e escala automática) ou em máquinas próprias com Power Automate for desktop, registradas e com Enable for computer use ligado. Stored credentials ficam no armazenamento interno ou no Azure Key Vault e não são inseridas em sites sem HTTPS. O controle de acesso lista sites e apps permitidos, aceita curinga para subdomínios e bloqueia ações fora da lista, mas não impede abrir outros sites. Com Store logs in Dataverse (padrão), a retenção é de 7 dias por padrão e a verbosidade, como Data without screenshots, é ajustada nas configurações de Computer Use do ambiente; a supervisão humana envia pedido por e-mail do Outlook aos revisores e pausa até a resposta ou o tempo limite.

Agente filho

Vive dentro do agente principal, sem publicação, configuração nem ALM separados, e tem orquestração e limite de ferramentas próprios. Por padrão recebe a tarefa em linguagem natural e devolve um resumo; com entradas definidas, Should prompt user faz o próprio filho perguntar o valor ausente. When will this be used define o acionamento (The agent chooses pela descrição, It's redirected to, A custom client event occurs com Event name, The user is inactive for a while, entre outros). Quando filho e tópico respondem ao mesmo evento, Priority com número menor vai primeiro; sem Priority, vale a ordem de criação, do mais antigo para o mais novo.

Agente conectado do Copilot Studio

Exige mesmo ambiente, agente publicado, Let other agents connect to and use this one ligada e o maker como dono ou com o agente compartilhado; o principal precisa de orquestração generativa e usa a versão publicada. A descrição que orienta o orquestrador é local, não sincroniza e deve ser atualizada à mão; Pass conversation history decide se o histórico vai junto. Enabled pausa o agente sem perder configuração, Disconnect agent remove o vínculo, e um agente que já tem agentes conectados não pode ser conectado a outro. Em tempo de execução os usuários também precisam de acesso ao conectado, ferramentas ficam encapsuladas nele, Use general knowledge do principal vale para filhos e conectados e citações podem sumir no retorno, como limitação conhecida.

Agente do Microsoft Foundry conectado

Em versão prévia, só agentes do novo portal do Foundry são suportados, com o protocolo Activity habilitado pela API REST ou pelo SDK (por padrão o agente expõe Responses e A2A). A conexão usa a URL do endpoint do projeto, o Agent Id, e nome e descrição definidos no Copilot Studio; se o Agent Id mudar, edite-o na página de detalhes do agente. HTTP 400 dizendo que o endpoint não suporta Activity indica protocolo desligado, e 404 Version not found indica agente do portal anterior. O endpoint não aceita chave de API: usa Entra ID e RBAC (Foundry Agent Consumer ou superior), e fixar uma versão no lugar de Always use latest dá estabilidade.

Agente de dados do Microsoft Fabric

Precisa estar publicado no Fabric, no mesmo tenant, com capacidade paga F2 ou superior (ou Power BI Premium P1 ou superior) e a configuração que libera o Copilot e o Azure OpenAI; fora da EU Data Boundary e dos EUA, também o processamento e armazenamento entre regiões, e configurações do locatário podem levar até uma hora. Aceita até cinco fontes entre tabelas de lakehouse, warehouses, bancos KQL, modelos semânticos, bancos espelhados e ontologias, e regras de negócio vão nas instruções e consultas de exemplo no Fabric. Na conexão escolhe-se User authentication (permissões de cada pessoa) ou Agent author authentication. Não aceita redirecionamento a partir de tópico e não funciona com o principal no Microsoft Copilot.

A2A, Agents SDK e skills

Em Add agent, A2A agent, informa-se o endpoint de comunicação, não a URL do cartão; com cartão válido em .well-known, nome e descrição são preenchidos sozinhos. A autenticação é None, API key ou OAuth 2.0, cada mensagem leva metadados como contextId, localidade e o histórico completo, e por usar a base dos conectores personalizados a conexão alcança agentes on-premises ou em rede virtual; Dev Tunnels é só para teste e a avaliação de dados e segurança do agente externo é da empresa. Agentes do Microsoft 365 Agents SDK entram pela opção própria com o messaging endpoint em /api/messages. Skills do Azure Bot Service exigem passar o ID do agente ao desenvolvedor do skill para a lista de permissões, e o canal A2A client expõe o agente com registro no Entra e a permissão MCS.InvokeAsA2A.

Modelos do Foundry em prompts

São conectados pelo sinal de mais no campo Model do editor de prompt, com o nome da implantação e o Base model name iguais aos do Foundry e a URL do endpoint de chat completions; o endpoint Responses falha com Resource not found. Só modelos do tipo chat completion, sem a família GPT-5 e posteriores, e com entrada de imagem a lista mostra só modelos que aceitam imagem. O consumo é cobrado à parte, na assinatura do Azure, fora das tarifas de Copilot Credits; a moderação de conteúdo só existe para modelos gerenciados, e o uso pode ser bloqueado por ambiente na política de dados do conector.

Application Insights e telemetria

No nível do agente, a cadeia de conexão vai em Settings, Advanced, os eventos chegam à tabela customEvents (inclusive do painel de teste, separáveis por designMode igual a False) e channelId separa canais como msteams e webchat. Enable logging registra mensagens e eventos, Log conversation details acrescenta ID, nome e texto do usuário, Log sensitive Activity properties inclui propriedades sensíveis e Node execution events registra cada nó; o nó Log custom telemetry event grava eventos de negócio. A pasta de trabalho Copilot Studio Dashboard, em Monitoring, Workbooks, dá painel pronto, a retenção é de 90 dias sem custo e se amplia no workspace do Log Analytics com custo. No nível do ambiente, configurado por administradores, vêm traces alinhados ao OpenTelemetry e dependencies; a telemetria de voz em tempo real fica em traces, com Subject LlmInvocation e Duration_Ms.

Macetes para memorizar

💡 Copilot connector x tempo real

Copilot connector COPIA para o Graph (admin no Microsoft 365); tempo real CONSULTA na fonte com o token do usuário.

💡 A2A

Fala com o ENDPOINT, lê o CARTÃO sozinho; autenticação None, chave ou OAuth.

💡 Erros do Foundry

400 = falta Activity; 404 = portal velho; chave = nunca (Entra e RBAC).

💡 MCP no Copilot Studio

T e R sem P: Tools e Resources, sem Prompts; recurso só sai por ferramenta; transporte Streamable.

💡 Filho x conectado

Filho mora dentro de casa; conectado tem casa própria (publicação e ALM) e precisa estar publicado e aberto a conexões.

💡 Azure AI Search

Um índice vetorial por fonte, ranker configurado no Azure, link vem de campo no índice.

💡 Tabelas de telemetria

customEvents é do agente; traces é do ambiente e da voz em tempo real.

💡 Escolha de ferramenta

Tem API? Conector. Só tela? Computer use. Envolve dinheiro? Nunca computer use.

Tabela de memorização: não confunda

Quando é...	...e quando é
Copilot connector Reaproveitar o conteúdo já indexado no Microsoft Graph e usado pelo Microsoft 365 Copilot e pelo Microsoft Search, configurado pelo administrador.	**Conhecimento em tempo real (conector da Power Platform)** Os dados não podem ser copiados e a consulta deve ir à fonte com o token de cada usuário.
Agente filho Agrupar ferramentas e conhecimento dentro do agente, sem publicação, autenticação ou ALM próprios.	**Agente conectado** Outra equipe mantém o agente, com publicação, configurações e ALM próprios, e vários principais o reutilizam.
MCP Expor ferramentas e recursos de um sistema ao agente, que as escolhe dinamicamente.	**A2A** Delegar tarefas a outro agente com raciocínio próprio, em vários turnos e com metadados ricos.
Send HTTP request Chamada fixa em uma etapa definida do roteiro do tópico.	**Ferramenta REST API** O orquestrador escolhe entre operações da API pelas descrições, com conexão e OAuth 2.0 por usuário.
Ferramenta de conector O sistema tem API ou conector: chamadas estruturadas, rápidas, previsíveis e auditáveis.	**Computer use** O sistema só tem interface gráfica, sem API, e a tarefa não é transação financeira.
Telemetria no nível do agente O maker liga um agente com a cadeia de conexão; eventos em customEvents.	**Telemetria no nível do ambiente** O administrador quer todos os agentes do ambiente em um só lugar, com traces OpenTelemetry e dependencies.
End user credentials Cada usuário deve acessar só o que pode ver na origem.	**Maker-provided credentials** O conteúdo é igual para todos e os usuários não têm conta no serviço, como visitantes de um site público.

Números que caem

Item	Valor
Arquivos carregados como conhecimento por agente	**até 500**
Frequência mínima do rastreamento incremental de Copilot connector	**15 minutos**
Ferramentas por agente	**até 128, com recomendação de 25 a 30**
Capacidade exigida pelo agente de dados do Fabric	**F2 ou superior (ou Power BI Premium P1 ou superior)**

Fontes por agente de dados do Fabric	**até 5**
Retenção padrão dos logs do computer use no Dataverse	**7 dias**
Retenção sem custo das tabelas do Application Insights	**90 dias**
Aposentadoria do Azure OpenAI On Your Data	**14 de outubro de 2026**
Fim do suporte ao transporte SSE para MCP	**após agosto de 2025**
Tamanho máximo do manifesto de skill do Azure Bot Service	**500 KB**
Isenção de agentes da política de dados	**não é possível desde março de 2025**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Informar na conexão A2A a URL do cartão do agente em .well-known.
Como não cair: O campo pede o endpoint de comunicação; o cartão é lido sozinho a partir do caminho padrão.

⚠ **Alerta de prova:** Autenticar a chamada ao agente do Foundry com a chave do recurso copiada em Keys and endpoint.
Como não cair: Endpoints de agentes do Foundry não aceitam chave de API; a autorização é Entra ID com RBAC (Foundry Agent Consumer).

⚠ **Alerta de prova:** Ligar Log conversation details achando que é a opção das propriedades sensíveis, ou ligá-la quando a privacidade proíbe gravar nome e texto do usuário.
Como não cair: Log conversation details grava ID, nome e texto do usuário; propriedades sensíveis são Log sensitive Activity properties; para privacidade, só Enable logging.

⚠ **Alerta de prova:** Dizer que Copilot connectors consultam o sistema em tempo real sem copiar conteúdo.
Como não cair: Copilot connector copia e indexa no Microsoft Graph; consulta na fonte sem cópia é do conhecimento em tempo real por conector da Power Platform.

⚠ **Alerta de prova:** Reduzir o intervalo do rastreamento incremental para que exclusões e mudanças de permissão sumam das respostas.
Como não cair: O incremental não trata exclusões nem permissões; agende o rastreamento completo no Microsoft 365 admin center.

⚠ **Alerta de prova:** Ligar o semantic ranker na conexão do Copilot Studio depois de escolher o índice.
Como não cair: A conexão não tem essa opção; o semantic ranker é configurado no serviço e no índice do Azure AI Search antes de conectar.

⚠ **Alerta de prova:** Informar dois índices vetoriais na mesma fonte do Azure AI Search, achando que o tipo de autenticação ou campos iguais permitem.
Como não cair: Cada fonte do Azure AI Search aceita um único índice vetorial, sem exceção.

⚠ **Alerta de prova:** Trocar o transporte do servidor MCP para SSE para resolver ferramenta sumida, recurso não usado ou política de dados.
Como não cair: O Copilot Studio só suporta Streamable; SSE deixou de ser aceito, e o transporte não muda esquema nem política de dados.

⚠ **Alerta de prova:** Chamar a ferramenta computer use por um nó dentro do tópico para controlar a ordem dos passos.
Como não cair: Computer use não roda a partir de tópico; a orquestração generativa a chama e a ordem dos passos vai nas instruções da ferramenta.

⚠ **Alerta de prova:** Pedir nas instruções do agente que as respostas tragam o link do documento do Azure AI Search.
Como não cair: Sem campo de URL no índice não há link; inclua metadata_storage_path ou um campo com a URL completa.

⚠ **Alerta de prova:** Republicar o agente ou criar nova conexão depois de mudar a variável de ambiente usada no Host do conector personalizado.
Como não cair: O valor é aplicado quando o conector é salvo; abra o conector no ambiente e salve-o de novo.

⚠ **Alerta de prova:** Achar que basta salvar as novas instruções do agente conectado ou que a descrição sincroniza sozinha com o principal.
Como não cair: O principal usa a versão publicada do conectado e a descrição é local: publique o conectado e atualize a descrição à mão.

⚠ **Alerta de prova:** Dividir o agente em vários agentes conectados porque o orquestrador confunde duas ferramentas de descrição parecida.
Como não cair: Primeiro diferencie nomes e descrições e avalie; dividir aumenta latência, testes e governança e só se justifica com equipes, publicação ou reuso separados.

⚠ **Alerta de prova:** Pedir ao administrador isenção da política de dados para o agente ou recriar o MCP como fluxo para escapar dela.
Como não cair: Isenção não é mais suportada e fluxos também usam conectores; veja o relatório de violações em Channels e ajuste o conector na política.

Como cai na prova

📝 **Como cai:** Escolher a fonte de conhecimento para um sistema corporativo, com restrições de cópia, permissão e volume.
Como resolver: Verifique se o conteúdo já está indexado no Graph (Copilot connector), se não pode ser copiado e precisa do token do usuário (tempo real), se é acervo grande com controle de embedding (Azure AI Search) ou se é tabela do Dataverse (fonte própria).

📝 **Como cai:** Enunciado com mensagem de erro literal após configurar uma integração.
Como resolver: Associe o código à causa antes de ler as alternativas: 400 Activity, 404 Version not found, 401 com conexão Expired, CuaInsert... sem HTTPS, DataLossPreventionViolation com política de dados; descarte quem fala de autenticação quando o erro é de protocolo.

📝 **Como cai:** Que tipo de agente adicionar na página Agents para uma lógica que já existe em outro lugar.
Como resolver: Copilot Studio no mesmo ambiente vira conectado; lógica no Foundry usa Microsoft Foundry com endpoint do projeto e Agent Id; dados do Fabric usam Microsoft Fabric; outro framework com A2A usa A2A agent; Agents SDK usa /api/messages; agente declarativo do construtor do Microsoft 365 Copilot não entra.

📝 **Como cai:** Configurar a autenticação de uma conexão (MCP, REST API, A2A ou Azure AI Search).
Como resolver: Liste as opções de cada assistente: MCP com OAuth Dynamic discovery, Dynamic ou Manual; REST API com API key em Header ou Query e OAuth com My organization only; A2A com None, API key ou OAuth 2.0; Azure AI Search com Entra ID quando chave administrativa é proibida.

📝 **Como cai:** Onde ver ou configurar telemetria no Application Insights.
Como resolver: Cadeia de conexão em Settings, Advanced; consultas em customEvents com customDimensions; privacidade pelas quatro opções de log; painel pronto em Workbooks; retenção no Log Analytics; proibição pelo conector Application Insights in Copilot Studio numa política de dados.

📝 **Como cai:** Questão de múltipla resposta sobre requisitos de agente conectado, agente filho ou computer use.
Como resolver: Confira cada afirmação contra os requisitos exatos (mesmo ambiente, publicado, conexões permitidas, compartilhado) e desconfie de limites inventados, sincronizações automáticas e exigências de solução gerenciada ou orquestração clássica.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
HTTP 400 dizendo que o endpoint não suporta Activity	**Habilitar o protocolo Activity no agente do Foundry pela API REST ou pelo SDK.**
404 - Version not found ao conectar agente do Foundry	**Agente criado no portal anterior do Foundry, não suportado.**
CuaInsertCredentialNotAllowedInInsecureWebsites	**O site é acessado por http; o computer use não insere credenciais sem HTTPS.**
Botão Publish indisponível e banner com Details listando a fonte de conhecimento	**Política de dados no Power Platform admin center bloqueando o conector da fonte.**
DataLossPreventionViolation num agente com servidor MCP	**Relatório de violações na página Channels e liberação do conector na política.**
Dados que não podem ser copiados e permissões de cada usuário valendo nas respostas	**Conhecimento em tempo real por conector da Power Platform.**
Mesmo conteúdo indexado que já alimenta o Microsoft 365 Copilot	**Copilot connector configurado pelo administrador, adicionado em Add knowledge (Advanced).**
Tabela Knowledge Article fora da lista do assistente	**Adicionar como base de conhecimento não estruturada em Your connections.**
Milhares de PDFs grandes com controle de embedding e tamanho de trechos	**Azure AI Search com índice vetorial criado por Import and vectorize data.**
Resource not found ao conectar modelo do Foundry no editor de prompt	**Usar o endpoint de chat completions, não o de Responses.**
Relatórios inflados pelas conversas do painel de teste	**Filtrar customDimensions['designMode'] igual a False em customEvents.**
Todos os agentes do ambiente, sem configurar um a um, em traces OpenTelemetry	**Telemetria no nível do ambiente, configurada por administrador.**
Agente em C# ou Python feito com o Microsoft 365 Agents SDK	**Opção Microsoft 365 Agents SDK em Add an agent, com messaging endpoint em /api/messages.**

Orquestrador externo precisa enviar tarefas ao agente publicado por A2A	**Canal A2A client e registro de aplicativo no Entra com MCS.InvokeAsA2A.**

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

- Copilot connector copia para o Microsoft Graph; conhecimento em tempo real consulta a fonte com o token do usuário e só indexa metadados.
- Agente conectado: mesmo ambiente, publicado, conexões permitidas, compartilhado com o maker e com os usuários; descrição local atualizada à mão.
- Agente do Foundry: novo portal, protocolo Activity habilitado, endpoint do projeto mais Agent Id, Entra ID com RBAC.
- MCP no Copilot Studio é remoto, Streamable, com Tools e Resources e governado pelas políticas de dados.
- Computer use exige orquestração generativa, não roda por tópico e não insere credenciais em sites sem HTTPS.

Essenciais para a prova (checklist)

☐ Sei diferenciar Copilot connector, conhecimento em tempo real, Azure AI Search, arquivos carregados e Foundry IQ.

☐ Sei preparar o Azure AI Search: índice vetorial integrado, um por fonte, semantic ranker no Azure e campo de URL para citações.

☐ Sei conectar um servidor MCP pelo assistente, escolher o tipo de OAuth 2.0 e limitar ferramentas com Allow all.

☐ Sei criar uma ferramenta REST API: JSON, OpenAPI 2.0, seleção de operações, autenticação e Add and configure.

☐ Sei que variáveis de ambiente no Host de conector personalizado exigem salvar o conector de novo.

☐ Sei onde o computer use roda, como guarda credenciais, como funciona o controle de acesso e onde ajustar retenção dos logs.

☐ Sei os requisitos e as opções de agente conectado (Pass conversation history, Enabled, Disconnect) e de agente filho (When will this be used, Priority, Should prompt user).

☐ Sei associar os erros 400 e 404 do Foundry às causas e informar endpoint do projeto e Agent Id.

☐ Sei os pré-requisitos do agente de dados do Fabric e suas limitações de redirecionamento e de canal.

☐ Sei configurar o Application Insights do agente, consultar customEvents e escolher as opções de log conforme a privacidade.

Questões de revisão do capítulo

R1.1 · Integrar e estender agentes no Copilot Studio

O agente da Mineradora Vale Profundo usa como conhecimento um Copilot connector do Confluence configurado pelo administrador. As respostas trazem poucos trechos relevantes, mesmo para perguntas com termos que estão nas páginas. A empresa tem licenças do Microsoft 365 Copilot no mesmo locatário. O que a documentação recomenda ativar no agente?

A. A moderação de conteúdo no nível Lowest
B. A pesquisa na web, que complementa o índice
C. O tenant graph grounding com busca semântica
D. A orquestração clássica, com frases de gatilho

R1.2 · Integrar e estender agentes no Copilot Studio

A Consultoria Tributária Ápice tem um índice vetorial no Azure AI Search, criado com Import and vectorize data. O maker vai adicioná-lo como conhecimento de um agente pela opção Azure AI Search, com o tipo de autenticação Access Key. Quais dados ele precisa informar ao criar a conexão?

A. A string de conexão do Application Insights e o nome do índice vetorial
B. A URL do endpoint do serviço de pesquisa e a chave de administrador (Admin Key)
C. O ID do locatário, o ID do cliente e o segredo de um registro de aplicativo
D. O nome da implantação do modelo de embedding e a chave do recurso do Microsoft Foundry

R1.3 · Integrar e estender agentes no Copilot Studio

A Corretora de Seguros Elo Forte vai criar no Copilot Studio uma ferramenta REST API para a API de sinistros. O fornecedor entregou a especificação OpenAPI 2.0 só em um arquivo YAML, e o desenvolvedor quer seguir o assistente sem retrabalho. O que ele deve fazer antes de carregar a especificação?

A. Carregar o YAML como está, pois o assistente o converte para JSON na versão 2.0
B. Publicar o YAML num site e informar a URL da especificação no lugar do arquivo
C. Converter o arquivo YAML para JSON, formato de especificação que o assistente pede no envio
D. Converter a especificação para OpenAPI 3.0, versão que o assistente exige no envio

R1.4 · Integrar e estender agentes no Copilot Studio

A Indústria de Cosméticos Flor de Lis quer que um agente do Copilot Studio consulte e crie registros em tabelas do Dataverse por meio de MCP, sem desenvolver nem hospedar um servidor próprio. O que o desenvolvedor deve fazer?

A. Adicionar as tabelas do Dataverse como conhecimento, que também permite criar registros
B. Adicionar em Tools o Microsoft Dataverse MCP Server, listado em Model Context Protocol
C. Criar um servidor MCP no Azure Functions com as operações do Dataverse e registrá-lo pelo assistente
D. Criar um conector personalizado com o esquema OpenAPI da Web API do Dataverse e publicá-lo

Respostas comentadas

R1.1. C) O tenant graph grounding com busca semântica

Por quê: Copilot connectors indexam conteúdo de sistemas externos no Microsoft Graph, com as permissões da origem. A busca semântica do tenant graph grounding melhora a recuperação desse conteúdo e é cobrada à parte em Copilot Credits.

✗ A) Incorreta. Moderação mais baixa gera mais respostas com mais risco, mas não melhora a recuperação dos trechos.
✗ B) Incorreta. A pesquisa na web traz sites públicos, não o conteúdo do Confluence indexado no Microsoft Graph.
✗ D) Incorreta. A orquestração clássica não melhora a busca no conteúdo indexado e tira recursos da generativa.

> **Dica de prova:** Copilot connector com resultados fracos: tenant graph grounding com busca semântica.

R1.2. B) A URL do endpoint do serviço de pesquisa e a chave de administrador (Admin Key)

Por quê: A conexão do Azure AI Search aceita Access Key, Client Certificate Auth, Service principal e Microsoft Entra ID Integrated. Com chave, informam-se endpoint e Admin Key; o índice vetorial é escolhido no passo seguinte.

✗ A) Incorreta. A string de conexão do Application Insights serve para telemetria do agente, não para a conexão com o serviço de pesquisa.
✗ C) Incorreta. Esses dados correspondem à autenticação por entidade de serviço (Service principal), outra opção da lista, e não à chave de acesso.
✗ D) Incorreta. Com vetorização integrada, o próprio índice usa o modelo de embedding na consulta; a conexão do conhecimento não pede a implantação do modelo.

> **Dica de prova:** Azure AI Search por chave: endpoint + Admin Key, depois o índice.

R1.3. C) Converter o arquivo YAML para JSON, formato de especificação que o assistente pede no envio

Por quê: Para criar uma ferramenta REST API, o Copilot Studio pede a especificação OpenAPI, os dados de autenticação e as descrições. A página pede a especificação em arquivo JSON; se ela vier na versão 3, é traduzida para a versão 2 na criação.

✗ A) Incorreta. A conversão automática descrita na documentação é da versão 3.0 para a 2.0; a página pede a especificação em arquivo JSON e não prevê conversão de YAML.
✗ B) Incorreta. O assistente pede o envio do arquivo da especificação, arrastando-o ou procurando-o no computador.
✗ D) Incorreta. As ferramentas são criadas a partir da versão 2.0; uma 3.0 enviada é traduzida para a 2.0, então mudar de versão não resolve o formato do arquivo.

> **Dica de prova:** REST API no Copilot Studio: especificação OpenAPI em arquivo JSON.

R1.4. B) Adicionar em Tools o Microsoft Dataverse MCP Server, listado em Model Context Protocol

Por quê: Em Tools, Add a tool, Model Context Protocol, aparecem tanto os servidores MCP prontos da Microsoft quanto os servidores já conectados pelo maker. O Dataverse MCP Server expõe ferramentas para consultar, criar, atualizar e descrever tabelas e registros.

✗ A) Incorreta. Conhecimento serve para responder perguntas a partir dos dados; não executa operações de criação de registros.

✗ C) Incorreta. Desenvolver e hospedar um servidor próprio contraria o requisito, já que existe um servidor MCP pronto para o Dataverse.

✗ D) Incorreta. Um conector personalizado não é MCP e exigiria manter a definição da API, o que não é necessário.

> **Dica de prova:** Servidor MCP pronto da Microsoft para Dataverse: adicione pela lista de MCP em Tools.

02

CAPÍTULO 2 · 30-35% DA PROVA

Planejar e configurar soluções de agente

Aqui eu preciso dominar a construção do agente por dentro: autenticação, ferramentas e suas entradas, fluxos de agente, tópicos com Send HTTP request, variáveis, cartões adaptáveis, prompts, respostas generativas, canais e governança. É um domínio de 30-35% e quase sempre vem como cenário com uma restrição decisiva: sem login, só no Teams, sem segredo guardado, só neste tópico, sem criar nós novos. Onde mais erro é em opções de nome parecido, como Authenticate with Microsoft x Authenticate manually, Allow agent to decide dynamically x Ask the end user before running e Receive values x Return values. Também caio quando a alternativa resolve no agente inteiro e o enunciado pede só um tópico ou nó. A leitura certa é sublinhar a restrição e escolher o controle mais específico que a atende, nunca uma instrução em texto no lugar de uma configuração.

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

Tópicos-chave

Opções de autenticação do agente

No authentication só acessa informação pública, então um agente sem login fica limitado a fontes públicas, como sites; SharePoint e Dataverse exigem a identidade do usuário no Microsoft Entra ID. Authenticate with Microsoft configura o Entra ID sozinho, mas atende só ao canal Teams e Microsoft 365 (inclui o Microsoft 365 Copilot) e oferece User.Id e User.DisplayName. Authenticate manually é a opção para site próprio e demais canais; com qualquer variante dela (segredo, certificado ou credencial federada) o canal Teams e Microsoft 365 fica bloqueado.

Authenticate manually com Microsoft Entra ID

A Microsoft recomenda o Microsoft Entra ID V2 with federated credentials, que dispensa segredo de cliente guardado no registro de aplicativo. Os escopos incluem profile openid e, para o SharePoint como conhecimento, Sites.Read.All e Files.Read.All; User.DisplayName vazio com User.Id preenchido indica falta do escopo profile. Só a autenticação manual oferece User.AccessToken, que vai em cabeçalhos para destinos confiáveis e nunca em mensagens. Com Require users to sign in desmarcado e um nó Authenticate no tópico (caminhos por User.IsLoggedIn), o mesmo agente atende anônimos e autenticados.

Credenciais de ferramentas, fluxos e gatilhos

Uma ferramenta pode usar User authentication (credencial de quem conversa) ou Agent author authentication (conta de quem configurou). Quando o dado varia por pessoa, como uma lista do SharePoint com permissão por item, use a do usuário; instrução no agente não substitui controle de acesso. Gatilhos de evento usam sempre as credenciais do autor do agente, por isso a publicação mostra um aviso sobre credenciais. Em agente autenticado, as ações de um fluxo de agente rodam com a identidade do usuário configurando as conexões em Provided by run-only user.

Additional details da ferramenta

Allow agent to decide dynamically when to use the tool permite à orquestração generativa escolher a ferramenta; desmarcada, ela só roda quando um tópico a chama explicitamente. Ask the end user before running como Yes pede confirmação ao usuário antes de executar, o controle certo para ações de alto impacto, independente das instruções. Desligar Enabled na página Tools bloqueia a ferramenta para qualquer uso, inclusive pelo tópico.

Entradas de ferramentas e de tópicos

Fill using em Dynamically fill with AI (padrão) extrai o valor da conversa ou gera uma pergunta; quando falta o valor, o agente pergunta antes de chamar, sem enviar vazio. Custom value fixa um valor, variável ou fórmula Power Fx, e o agente para de perguntar. Em Customize da entrada ficam Identify as, nova tentativa e validação, para aceitar só formatos válidos como CEP. No tópico com orquestração generativa, entradas com boa descrição em Dynamically fill with the best option e Should prompt user dispensam o nó Question.

Fluxo de agente usado pelo agente

Precisa do gatilho When an agent calls the flow, da ação Respond to the agent e de estar numa solução no mesmo ambiente do agente; fluxo fora de solução não aparece em Add a tool. Save draft não muda a execução: só a versão publicada (Publish) roda quando o agente chama. Fluxos de agente também podem ser disparados por Recurrence ou por eventos, como arquivo novo no SharePoint, mas só os com When an agent calls the flow viram ferramenta. Para converter um fluxo da nuvem, ele precisa estar numa solução e ter o plano trocado para Copilot Studio em Edit, numa conversão de mão única.

Tempo de resposta do fluxo ao agente

O agente espera a resposta do fluxo por tempo limitado: o limite é de dois minutos. Asynchronous response em Respond to the agent, só em ambientes na nova infraestrutura, permite passar do limite e devolver o resultado no fim; o callback funciona no Teams, mas não no Microsoft Copilot nem na telefonia. Se o usuário precisa de algo logo, como um protocolo, coloque Respond to the agent cedo e deixe as etapas longas depois. O express mode acelera fluxos com muita lógica, mas tem limites de memória, de 1.024 caracteres por variável e de 64 KB por resposta de ação.

Tratamento de erros em fluxos

Configure run after faz uma ação rodar após sucesso, falha (has failed), tempo esgotado (has timed out) ou ação ignorada. No padrão try/catch com escopos, result('Try') com Filter array por status Failed mostra qual ação falhou e o corpo do erro; se o Catch terminar bem, a execução aparece como sucesso, a menos que se use Terminate com status Failed. Para o agente não mostrar erro genérico, o caminho de falha precisa de outro Respond to the agent com as mesmas saídas. Retry policy (Default, None, Exponential interval, Fixed interval) é o que repete chamadas com erro transitório, como 503.

Aprovações e Request for information

Start and wait for an approval serve para decidir: devolve Outcome (Approve ou Reject, com diferença entre maiúsculas e minúsculas) e Responses com aprovador e comentários; não escala sozinha, então use Timeout (como P3D) e uma ação com run after em has timed out. Request for information coleta dados tipados por e-mail no Outlook, vale só a primeira resposta e cada entrada vira conteúdo dinâmico. Em Run a multistage approval, o estágio de IA usa Next step based on decision (por padrão rejeição encerra), Analysis failed indica regras contraditórias e estágios manuais recebem dados por entradas criadas com barra.

Cobrança de fluxos de agente e do agente

Fluxos de agente são premium e consomem capacidade do Copilot Studio por ação executada, sem licença do Power Automate; testes no designer ou no chat de teste não consomem. Chamado por tópico, o fluxo soma uma Classic answer; escolhido pelo orquestrador, soma uma Autonomous action, e nos dois casos as ações também contam. A divisão de Copilot Credits por atividade fica na página Monitor do agente, em See billing, no gráfico Cost distribution.

Nó Send HTTP request

Define método, URL, cabeçalhos e corpo, que pode ser JSON Content (literal ou Formula com registro Power Fx usando variáveis) ou Raw content. Response data type, definido a partir de dados de exemplo da resposta de sucesso, tipa a resposta para usar os campos em condições. Error handling tem Raise an error (padrão, leva ao tópico On Error) ou Continue on error, que guarda código de status e corpo do erro em variáveis; o Request timeout é em milissegundos, com padrão de 30 segundos.

Variáveis no Copilot Studio

Os escopos são System, Global, Topic e Environment, e em Power Fx as de sistema levam o prefixo System. Activity.Text é a última mensagem do usuário, Recognizer.TriggeringMessage.Text é a frase que acionou o tópico e Conversation.Id só identifica a conversa. Receive values from other topics, no tópico de destino, recebe valores no redirecionamento e Return values to original topics devolve ao chamador; data e hora, duração, múltipla escolha e entidades personalizadas não são passadas. Globais podem ser preenchidas pela página com External sources can set values e limpas com Clear variable values; Table e Record nascem em Set variable value com fórmula, e Parse value converte JSON em texto num registro tipado.

Cartões adaptáveis

Ask with adaptive card exige ao menos um botão de envio e gera variáveis de saída, corrigidas em Edit Schema; para mostrar variáveis no conteúdo, troque o JSON por Formula. isRequired, regex e errorMessage no Input.Text validam antes do envio; um identificador em data de cada Action.Submit evita processar cliques em cartões antigos. Allow switching to another topic (ligada por padrão) deixa texto digitado trocar de tópico; desmarque e use How many reprompts e Retry prompt para insistir no cartão. O Copilot Studio suporta até a versão 1.6, mas Web Chat aceita 1.6 sem Action.Execute e Teams e chat ao vivo ficam na 1.5.

Nó Message

Variações de mensagem são sorteadas a cada execução, sem fórmula. Respostas rápidas podem ser Send a message, Open URL, Make a call ou Send a hidden message to the agent, que envia um comando sem aparecer no histórico. A versão Speech, com SSML opcional para pausas e ênfase, é usada nos canais de voz e mantém o texto do chat nos demais.

Nó de respostas generativas

O Input padrão é Activity.Text; monte-o com as variáveis do tópico quando a pergunta curta perde contexto. A moderação vai de Lowest a Highest (padrão High) e o nível do nó prevalece sobre o do agente; as instruções personalizadas do nó aceitam até 8.000 caracteres e valem só ali. Web search e Allow the AI to use its own general knowledge podem ser desligados no próprio nó. Desmarcar Send a message guarda a resposta numa variável, e no Teams quem personaliza precisa renderizar as citações por conta própria.

Prompts personalizados

O campo Model lista categorias Mini (tarifa basic, o padrão), General (standard) e Deep (premium, com raciocínio antes de responder); tarefa simples e volume alto pede Mini, e temperatura baixa deixa a saída mais estável. Prompts novos são privados: Share como User permite usar e Co-owner permite editar, compartilhar e excluir. No editor, o teste usa o Sample data das entradas; no tópico, a entrada precisa ser mapeada a uma variável pelo nó adicionado em Add a tool. Num prompt com tabelas do Dataverse como conhecimento, vêm 30 registros por padrão, ajustáveis até 1.000 nas configurações do prompt, e tabelas virtuais ainda não são suportadas como conhecimento do prompt.

Proteção, identidade e auditoria

Os agentes já bloqueiam por padrão injeção no prompt do usuário (UPIA) e injeção escondida em conteúdo lido, como e-mails e documentos (XPIA); um provedor externo é opcional. A coluna Protection status mostra Protected, Needs review ou Unknown, e Needs review vem de Authentication ou Policies; o Security analytics oferece 7, 14 e 30 dias. Desde maio de 2026 cada agente novo recebe um Microsoft Entra Agent ID, visto em Settings, Advanced, Metadata. No Purview, BotUpdateOperation-BotPublish e BotUpdateOperation-BotShare registram publicação e compartilhamento, e rótulos de confidencialidade aparecem como escudo com o rótulo mais alto e rótulo por citação.

Canais e publicação

Mudanças ficam em rascunho até Publish, que atualiza todos os canais em nova sessão; o site de demonstração serve para testes com colegas, com mensagem de boas-vindas e iniciadores de conversa. Com Require secured access, o acesso pelo Direct Line exige segredo ou token, e em navegador o back-end troca o segredo por um token. Agente já aprovado pelo administrador na loja do Teams precisa ser reenviado para aprovação quando muda ícone, cor ou descrição. Para vários idiomas, inclua idiomas secundários em Settings, Languages e traduza as mensagens dos tópicos pelo arquivo de localização (JSON ou ResX); para transferir ao Dynamics 365 Customer Service, o site usa o widget de chat dele.

Macetes para memorizar

💡 Autenticação por canal

Teams pede Microsoft; site com identidade pede manual; público pede nada (e só fonte pública).

💡 Precedência de configuração

Nó manda no tópico: moderação, fontes, web e conhecimento geral configurados no nó valem só ali e vencem o agente.

💡 Passar valores entre tópicos

Receive recebe no destino; Return retorna à origem.

💡 Detalhes da ferramenta

Allow decide QUEM chama; Ask pede LICENÇA ao usuário; Enabled desliga TUDO.

Pessoas no fluxo

Decidir = aprovação; Descobrir dado = Request for information (Outlook, vale o primeiro).

Erros em fluxos

Run after desvia, Retry repete, Terminate carimba Failed, Respond no erro avisa o agente.

Modelos de prompt

Mini, General, Deep = basic, standard, premium; simples e barato é Mini.

Versões de cartão

Teams e chat ao vivo 1.5; Web Chat 1.6 sem Action.Execute.

Tabela de memorização: não confunda

Quando é...	...e quando é
Authenticate with Microsoft Agente só no Teams e Microsoft 365 Copilot, com contas da organização e sem precisar de token nem de autenticação explícita em tópicos.	**Authenticate manually** Site próprio ou outros canais com identidade, quando precisa de User.AccessToken, de credencial federada ou de parte anônima com nó Authenticate em tópicos.
Desmarcar Allow agent to decide dynamically A ferramenta deve rodar só quando um tópico a chamar, sem o orquestrador escolhê-la.	**Ask the end user before running como Yes** O orquestrador continua escolhendo, mas o usuário precisa confirmar no chat antes de cada execução.
Dynamically fill with AI O valor vem da conversa, como o produto pedido, e o agente deve perguntar se faltar.	**Custom value** O valor é sempre o mesmo ou vem de variável ou fórmula, como canal de venda igual a Chat, e o agente não deve perguntar.
Conhecimento Responder com base em conteúdo, como artigos da base de conhecimento do ServiceNow.	**Ferramenta** Executar uma operação no sistema, como abrir um chamado ou lançar uma ordem.
Start and wait for an approval Uma pessoa precisa decidir aprovar ou rejeitar, com comentários.	**Request for information** Uma pessoa precisa informar dados tipados, como centro de custo e data, por e-mail no Outlook.
Instruções do agente (página Overview) Escopo de assuntos e formato, tom e tamanho das respostas do agente inteiro.	**Instruções personalizadas do nó de respostas generativas** Formato ou aviso só nas respostas geradas por aquele nó, sem afetar o resto do agente.

Números que caem

Item	Valor
Limite de espera do agente pela resposta de um fluxo de agente	**2 minutos (além disso, Asynchronous response na nova infraestrutura)**

Express mode: limite por variável e por resposta de ação	**1.024 caracteres por variável; 64 KB por resposta de ação**
Request timeout padrão do Send HTTP request	**30 segundos (configurado em milissegundos)**
Instruções personalizadas do nó de respostas generativas	**até 8.000 caracteres**
Custom data no nó de respostas generativas	**só os 3 primeiros registros; Content obrigatório**
Registros do Dataverse recuperados por um prompt	**30 por padrão, até 1.000**
Payload de conector	**5 MB na nuvem pública; 450 KB no GCC**
Pré-filtragem de fontes por descrição na orquestração generativa	**acima de 25 fontes (arquivos carregados não contam)**
Moderação de conteúdo	**Lowest a Highest, padrão High**
Security analytics	**intervalos de 7, 14 e 30 dias**
Microsoft Entra Agent ID automático	**agentes criados desde maio de 2026**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Achar que, sem um recurso de Prompt Shields criado no Azure, o agente fica exposto a instruções escondidas em PDFs e e-mails.
Como não cair: UPIA e XPIA já são bloqueados por padrão nos agentes; um sistema externo de detecção é só monitoramento adicional opcional.

⚠ **Alerta de prova:** Reduzir a moderação nas configurações de IA generativa do agente para liberar respostas em um único tópico.
Como não cair: O nível do nó de respostas generativas prevalece sobre o do agente; ajuste no nó para não mudar todos os tópicos.

⚠ **Alerta de prova:** Marcar Return values to original topics no tópico de origem para mandar um valor ao tópico de destino.
Como não cair: Return devolve do chamado para quem chamou; para enviar ao destino, marque Receive values from other topics na variável do destino.

⚠ **Alerta de prova:** Escrever nas instruções do agente que ele peça confirmação antes de cancelar.
Como não cair: Instrução é orientação ao modelo e não garante nada; o controle é Ask the end user before running na ferramenta.

⚠ **Alerta de prova:** Desligar Enabled da ferramenta para que ela rode só pelo tópico.
Como não cair: Enabled desligado bloqueia inclusive o tópico; o certo é desmarcar Allow agent to decide dynamically when to use the tool.

⚠ **Alerta de prova:** Ligar Asynchronous response para o cliente receber logo o número de protocolo de um processo longo.
Como não cair: A resposta assíncrona devolve o resultado só no fim; para entregar algo logo, coloque Respond to the agent cedo e deixe o demorado depois.

⚠ **Alerta de prova:** Configurar o Catch para rodar também após is skipped, achando que assim o histórico registra a falha.
Como não cair: Se o Catch termina bem, a execução continua bem-sucedida; use Terminate com status Failed e mensagem no fim do Catch.

⚠ **Alerta de prova:** Contar que a aprovação encaminha sozinha ao superior depois de 72 horas sem resposta.
Como não cair: A aprovação não escala; defina Timeout na ação (como P3D) e uma nova aprovação com run after em has timed out.

⚠ **Alerta de prova:** Comparar Outcome com approve em minúsculas e não entender por que tudo cai no ramo de recusa.
Como não cair: Outcome é Approve ou Reject com inicial maiúscula; compare o valor exato e use Responses para os comentários.

⚠ **Alerta de prova:** Usar Authenticate with Microsoft num site próprio achando que ele repassa o token do usuário ao SharePoint.
Como não cair: Authenticate with Microsoft só serve ao canal Teams e Microsoft 365; fora dele, Authenticate manually.

⚠ **Alerta de prova:** Manter Agent author authentication e escrever nas instruções que o agente não revele dados de colegas.
Como não cair: Com a credencial do autor a ferramenta lê tudo o que ele vê; troque para User authentication para cada chamada usar a conexão de quem conversa.

⚠ **Alerta de prova:** Aceitar computer use com supervisão humana para lançar pagamentos num portal de banco que também tem API.
Como não cair: Computer use não é indicado para casos de alto risco, como transações financeiras, e a supervisão não é salvaguarda garantida; havendo API, use conector.

⚠ **Alerta de prova:** Personalizar o tópico Conversational boosting para filtrar fontes num agente com orquestração generativa.
Como não cair: Na orquestração generativa a busca no conhecimento é feita pelo orquestrador, sem esse tópico; a personalização deixa de ter efeito.

⚠ **Alerta de prova:** Definir isRequired e errorMessage para impedir que o texto digitado no lugar do cartão troque de tópico.
Como não cair: isRequired valida campos no envio do cartão; texto digitado é tratado por Allow switching to another topic e pelo Retry prompt do nó.

Como cai na prova

📝 **Como cai:** Cenário longo de empresa com canal, tipo de usuário e exigência de segurança, pedindo a configuração de autenticação.
Como resolver: Identifique o canal (Teams e Microsoft 365 ou site), se há anônimos e se precisa de token ou de fonte com permissão; elimine Authenticate with Microsoft fora do Teams e No authentication quando há SharePoint; prefira credencial federada quando segredo é proibido.

📝 **Como cai:** Ferramenta que se comporta errado: escolhida quando não devia, sem confirmação, perguntando valor fixo ou aceitando valor inválido.
Como resolver: Mapeie o sintoma para a opção: quem decide chamar (Allow agent to decide dynamically), confirmação (Ask the end user before running), valor fixo (Custom value), formato (Customize com Identify as e validação).

📝 **Como cai:** Fluxo de agente lento, falhando ou devolvendo erro genérico ao agente.
Como resolver: Separe tempo (Respond cedo ou Asynchronous response), volume (desligar express mode, Filter rows e Select columns), falha transitória (Retry policy) e falha tratada (run after, outro Respond to the agent, Terminate Failed).

📝 **Como cai:** Pedido restrito a um tópico ou nó, com alternativa que muda o agente inteiro.
Como resolver: Descarte as opções no nível do agente e na orquestração; procure a propriedade no nó (moderação, fontes, Web search, instruções personalizadas, Send a message).

📝 **Como cai:** Planejamento de integração com sistema que tem portal web, API, ou está atrás de firewall.
Como resolver: API existente vira conector ou ferramenta; sistema local usa gateway de dados local; computer use só onde não há API e nunca para transações financeiras; respostas de conector precisam caber em 5 MB, com seleção de campos e paginação.

📝 **Como cai:** Escolher o desenho para reaproveitar uma capacidade entre equipes do mesmo ambiente. **Como resolver:** Dono, publicação e ALM próprios apontam para agente conectado; tarefa interna sem publicação separada aponta para agente filho; prompt não leva conhecimento nem ferramentas.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Visitantes anônimos no site, sem conta na empresa e conteúdo interno que não pode vazar	**No authentication, só fontes públicas como conhecimento, sem SharePoint, e canal de site.**
Agente no Teams e no Microsoft 365 Copilot com o canal aparecendo bloqueado	**Trocar para Authenticate with Microsoft e ajustar tópicos que usavam User.AccessToken.**
Site próprio, Entra ID e proibição de segredo de cliente com validade	**Authenticate manually com Microsoft Entra ID V2 with federated credentials.**
Clientes sem login e funcionários autenticados só em um tópico do mesmo agente	**Authenticate manually com Require users to sign in desmarcado e nó Authenticate no tópico.**
Fluxo com gatilho certo que não aparece em Add a tool	**O fluxo não está numa solução.**
Fluxo de agente passa de dois minutos e o agente precisa do resultado final	**Asynchronous response em Respond to the agent, em ambiente na nova infraestrutura.**
Erro que cita limite de dados depois de ligar o express mode	**Desligar o express mode nesse fluxo.**
API responde 503 por alguns segundos e o fluxo falha na primeira tentativa	**Retry policy em Exponential interval ou Default.**
Tratar o 404 da API dentro do próprio tópico	**Continue on error no Send HTTP request e condição sobre o código de status.**
API que leva cerca de 45 segundos e falha por tempo esgotado no tópico	**Aumentar o Request timeout do nó, em milissegundos (padrão de 30 segundos).**
Gravar a frase original do usuário, mas o campo sai com a última resposta	**System.Recognizer.TriggeringMessage.Text no lugar de System.Activity.Text.**
Portal que incorpora o agente já sabe o contrato do cliente	**Variável global com External sources can set values e tempo limite.**
Erro dizendo que o bot não tem permissão de usar a variável de ambiente Secret	**Tag AllowedBots (ou AllowedEnvironments) no segredo do Azure Key Vault.**
SAP local com BAPIs e RFCs atrás do firewall, solução de baixo código	**Conector SAP ERP com gateway de dados local e SAP Connector for Microsoft .NET.**

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

- Teams e Microsoft 365 Copilot só funcionam com Authenticate with Microsoft; qualquer autenticação manual bloqueia esse canal.
- Fluxo usado pelo agente: When an agent calls the flow, Respond to the agent, dentro de solução, e só a versão publicada roda.
- Configuração no nó de respostas generativas vence a do agente e afeta só aquele tópico.
- Instrução não é controle: confirmação, acesso a dados e escopo de ferramenta se resolvem em configuração.
- Computer use não é para transação financeira; existindo API, use conector.

Essenciais para a prova (checklist)

☐ Sei escolher entre No authentication, Authenticate with Microsoft e Authenticate manually a partir do canal e do público.

☐ Sei que User.DisplayName vazio na autenticação manual indica falta do escopo profile.

☐ Sei diferenciar Allow agent to decide dynamically, Ask the end user before running e Enabled numa ferramenta.

☐ Sei quando usar Dynamically fill with AI, Custom value e Customize com Identify as.

☐ Sei os três requisitos para um fluxo aparecer como ferramenta e que Save draft não muda a execução.

☐ Sei montar tratamento de erro em fluxo com run after, Retry policy, Terminate e Respond to the agent no caminho de falha.

☐ Sei configurar Send HTTP request com JSON Content em Formula, Response data type por dados de exemplo, Continue on error e Request timeout.

☐ Sei passar valores entre tópicos com Receive values e Return values e limpar globais com Clear variable values.

☐ Sei corrigir cartões adaptáveis com Edit Schema, Formula, isRequired, regex, errorMessage e identificador em Action.Submit.

☐ Sei onde ver Copilot Credits por atividade (Monitor, See billing, Cost distribution) e como fluxos de agente são cobrados.

Questões de revisão do capítulo

R2.1 · Planejar e configurar soluções de agente

No agente da Agência de Turismo Rota Azul, só as respostas do tópico Roteiros, geradas pelo nó de respostas generativas, devem vir em passos numerados e com o aviso de que os preços podem mudar. As demais respostas do agente devem continuar como estão. Onde o desenvolvedor deve escrever essa orientação?

A. Nas instruções personalizadas da fonte de dados do nó desse tópico
B. Numa nova fonte de conhecimento com padrões de resposta
C. Nas instruções do agente, na página Overview, citando o tópico Roteiros
D. Na mensagem do tópico Conversation Start, que vale para toda a conversa

R2.2 · Planejar e configurar soluções de agente

Na Universidade Horizonte Aberto, o maker desmarcou Send a message no nó de respostas generativas, guardou a resposta numa variável e passou a mostrar o texto num cartão adaptável no Teams. A resposta aparece, mas as citações das fontes sumiram. O que explica isso?

A. A variável de saída guarda só o texto, sem a lista de fontes consultadas
B. Na resposta personalizada, o cartão precisa renderizar as citações
C. A fonte de conhecimento do nó perdeu a indexação depois da troca do canal
D. O Teams não aceita cartões adaptáveis vindos de nós de respostas generativas

R2.3 · Planejar e configurar soluções de agente

No agente da Livraria Página Viva, um tópico pergunta primeiro o título do livro e depois a dúvida do cliente, como e o frete. O nó de respostas generativas, com Input em Activity.Text, busca só o texto curto da dúvida e responde sem relação com o livro escolhido. O que ajustar no nó?

A. Aumentar o nível de moderação do nó para Highest, que melhora a busca
B. Definir o Input como uma fórmula que junta a variável do título e o texto da dúvida
C. Trocar o Input por System.Conversation.Id, que traz o histórico da conversa
D. Ligar Search only selected sources e deixar desmarcadas as fontes de conhecimento do agente

R2.4 · Planejar e configurar soluções de agente

O agente do Portal do Corretor da Seguradora Laço Forte usa Authenticate manually com o Microsoft Entra ID. A mensagem de boas-vindas usa User.DisplayName para cumprimentar o corretor pelo nome, mas a variável chega vazia, embora User.Id venha preenchido. Qual ajuste resolve?

A. Trocar a variável por System.Conversation.Id, que guarda o nome de quem conversa
B. Incluir o escopo profile na configuração da autenticação manual do agente
C. Mudar para No authentication, que preenche o nome a partir do navegador do usuário
D. Usar User.AccessToken na mensagem, que traz o nome do usuário

Respostas comentadas

R2.1. A) Nas instruções personalizadas da fonte de dados do nó desse tópico

Por quê: A modificação de prompt do nó de respostas generativas aceita instruções personalizadas sobre formato, tom e limites, com até 8.000 caracteres, variáveis e fórmulas Power Fx. Ela vale para o nó em que foi configurada.

✗ B) Incorreta. Um documento como conhecimento vira conteúdo para responder perguntas, não uma regra de formato confiável.

✗ C) Incorreta. As instruções da página Overview orientam o agente inteiro, e o pedido é mudar só as respostas desse tópico.

✗ D) Incorreta. Conversation Start define a mensagem de abertura da conversa; não orienta o formato das respostas geradas.

> **Dica de prova:** Formato só nas respostas de um tópico: instruções personalizadas no nó de respostas generativas.

R2.2. B) Na resposta personalizada, o cartão precisa renderizar as citações

Por quê: Desmarcar Send a message permite tratar a resposta antes de exibi-la, mas o agente deixa de montar a mensagem padrão. No Teams, quem personaliza a resposta precisa renderizar as citações por conta própria.

✗ A) Incorreta. As citações continuam disponíveis para uso; o problema é que o cartão personalizado não as inclui por conta própria.

✗ C) Incorreta. A troca de exibição não altera a indexação da fonte; a resposta continua fundamentada nela.

✗ D) Incorreta. O Teams exibe cartões adaptáveis (até a versão 1.5 do esquema); o ponto é o conteúdo do cartão.

> **Dica de prova:** Resposta generativa personalizada no Teams: inclua as citações à mão.

R2.3. B) Definir o Input como uma fórmula que junta a variável do título e o texto da dúvida

Por quê: O nó de respostas generativas recebe um Input (por padrão Activity.Text) e pode guardar a resposta em uma variável. Montar o Input com o contexto já coletado no tópico melhora a recuperação.

✗ A) Incorreta. Moderação mais alta filtra mais conteúdo e gera menos respostas; não melhora a relevância da busca.

✗ C) Incorreta. System.Conversation.Id é o identificador da conversa, não o histórico nem a pergunta do cliente.

✗ D) Incorreta. Sem fontes selecionadas, o nó deixa de pesquisar o conhecimento; essa combinação serve para responder só com dados personalizados de uma variável.

> **Dica de prova:** Pergunta curta sem contexto? Monte o Input do nó com as variáveis do tópico.

R2.4. B) Incluir o escopo profile na configuração da autenticação manual do agente

Por quê: Com autenticação, o agente oferece variáveis como User.DisplayName, User.Email e User.Id (com Authenticate manually, também User.AccessToken). Em fórmulas Power Fx elas são usadas com o prefixo System., como System.User.DisplayName.

✗ A) Incorreta. Conversation.Id identifica a conversa; não traz o nome do usuário.

✗ C) Incorreta. Sem autenticação, as variáveis de usuário como User.DisplayName nem ficam disponíveis.

✗ D) Incorreta. O token não deve aparecer em mensagens, por segurança, e não é um texto com o nome.

> **Dica de prova:** User.DisplayName vazio na autenticação manual? Falta o escopo profile.

03

CAPÍTULO 3 · 20-25% DA PROVA

Testar e gerenciar agentes

Este domínio vale 20-25% e se divide em duas metades: avaliação de agentes na página Evaluation e ALM com soluções, variáveis de ambiente e Pipelines da Power Platform. Na avaliação, a prova cobra qual método usar para cada critério, de onde vêm os casos de teste, os limites de cada tipo de conjunto e como ler e comparar resultados. No ALM, cobra detalhes de solução gerenciada x não gerenciada, o que viaja ou não na exportação, como variáveis de ambiente se comportam entre ambientes e as regras de host, estágios, delegação e extensões dos pipelines. Eu erro principalmente quando duas opções parecem fazer o mesmo, como Compare meaning x Text similarity, Upgrade x Update e Stage Owner x Service Principal, e quando a alternativa propõe um atalho que foge do processo (editar em produção, exportar gerenciada, importar à mão).

Neste capítulo

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

Tópicos-chave

Conjunto de teste de respostas únicas

Aceita até 100 casos, inclusive quando importados de arquivo. Pode nascer de Quick question set (10 perguntas geradas pela descrição, instruções e recursos do agente), Full question set (conhecimento ou tópicos como referência, com quantidade definida), Use your test chat conversation (perguntas do chat de teste mais recente), Import a file, digitação manual ou temas da análise. O arquivo de importação é .csv ou .txt com Question e Expected response como cabeçalhos da primeira linha; a resposta esperada é opcional, mas exigida pelos métodos que comparam.

Conjunto de teste de conversa

Avalia se o agente mantém o contexto ao longo de várias trocas, com até 20 casos e até 12 mensagens por caso, ou seja, 6 pares de pergunta e resposta. Pode vir de Quick conversation set, Full conversation set ou do chat de teste. Aceita General quality, Keyword match, Content safety e Custom; Compare meaning, Text similarity e Exact match ficam só para respostas únicas.

General quality

É o método padrão e o único que não exige resposta esperada nem palavras-chave. Avalia relevância, fundamentação (groundedness), completude e abstenção, e a resposta precisa atender a todos os critérios. Não tem nota mínima configurável e pode reprovar recusas corretas, caso em que se usa um método Custom.

Compare meaning

Compara a intenção e as ideias da resposta com a resposta esperada, não as palavras exatas, e serve quando a resposta pode ser redigida de várias formas corretas. A nota mínima de aprovação é configurável, com padrão de 50, e subir esse valor exige mais proximidade de sentido. Sem resposta esperada, o caso fica Invalid.

Text similarity e Exact match

Text similarity mede o quanto a redação se parece com a esperada, por similaridade de cosseno, com nota mínima, e serve quando a forma do texto importa e pequenas variações são aceitas. Exact match compara caractere por caractere e serve a números, códigos ou frases fixas, reprovando qualquer diferença de redação. Ambos exigem resposta esperada e são só para respostas únicas.

Keyword match, Tool use, Content safety e Custom

Keyword match confere termos esperados no modo Any (basta um) ou All (todos) e vale para respostas únicas e conversa. Tool use verifica se os tópicos ou ferramentas esperados foram usados, informados em cada caso ou para todos pelo cabeçalho da coluna. Content safety mede conteúdo nocivo, como ódio ou violência. Custom usa instruções de avaliação e dois ou mais rótulos com nome, descrição e resultado Pass ou Fail, por exemplo para aprovar recusas apropriadas.

Resultados da avaliação

Cada caso recebe Pass, Fail, Invalid ou Error com explicação, e falta de item esperado gera Invalid; a taxa de aprovação é calculada sobre Pass e Fail, então caso crítico exige filtrar por Fail e revisar um a um. No detalhe do caso ficam Show activity map e a lista de conhecimento, tópicos e ferramentas usados. Response time é medido de ponta a ponta em segundos, mas é só medida e não muda Pass nem Fail. Compare with compara duas execuções do mesmo conjunto com setas de melhora e piora, e Export test results gera um CSV com pergunta, resposta esperada, método, resposta, resultado e análise.

Quem vê e quem roda avaliações

Vários makers podem rodar o mesmo conjunto, mas só é possível rodar um teste por vez. Status e métricas de uma execução ficam visíveis a todos, enquanto respostas e explicações ficam restritas a quem iniciou a execução. A função Agent viewer dá acesso às abas Evaluation e Monitor sem permissões sobre o agente: executa conjuntos de outros makers e renomeia, cancela e exclui avaliações, mas não altera conjuntos compartilhados, não publica e não gerencia o compartilhamento.

Triagem de falhas na avaliação

Se o mapa de atividades mostra que nenhuma fonte foi recuperada ou que a fonte é errada, corrija a configuração ou a indexação do conhecimento e rode de novo. Se o agente escolheu o tópico ou a ferramenta errada, deixe nomes e descrições mais distintos; trocar de método só esconde a falha. Se a geração de casos falha, a causa pode ser moderação de conteúdo rígida demais, conteúdo sensível nas fontes ou instruções e tópicos que levam a conteúdo sinalizado.

Soluções, publisher e solução preferencial

O agente nasce na solução preferencial do maker ou, sem ela, na solução padrão, vista em Settings, Advanced, View solution; a Default Solution não pode ser exportada e o publisher dela não pode ser trocado. O publisher define o prefixo dos nomes de esquema, que não mudam depois de criados, então publisher e solução vêm antes dos componentes; dá para criá-los no próprio Copilot Studio pelo menu de três pontos, Solutions, New solution e New publisher. Set preferred solution é escolha de cada maker e vale para itens novos; escolher a solução em Agent settings, Advanced settings ao criar o agente já coloca os componentes futuros nela. Agente existente entra com Add existing, Agent, e componentes novos com Advanced, Add required objects.

Gerenciada x não gerenciada e camadas

Desenvolvimento usa solução não gerenciada; teste e produção recebem a solução exportada como gerenciada, e soluções gerenciadas não podem ser exportadas. Não é possível importar a gerenciada no ambiente que contém a não gerenciada de origem. Edição direta num componente gerenciado cria uma camada não gerenciada que prevalece sobre as versões importadas, removida em See solution layers com Remove unmanaged layer. Upgrade remove componentes que saíram da nova versão, Update os mantém, patch só adiciona ou atualiza, e excluir a solução gerenciada remove componentes e dados.

Exportação e importação de agentes

Tópicos com ponto no nome impedem a exportação; comentários de tópicos e nós, ícone, detalhes de canal e IDs de conversa, agente e ambiente não viajam, enquanto as instruções do agente vão. Depois de importar, abra o agente pela solução, refaça a autenticação e publique, porque sem publicação não dá para compartilhar; o ícone pode levar até 24 horas para aparecer. Erros IdentifierNotRecognized e Element disabled or not found ao publicar indicam dependência que faltou na solução, corrigida na origem. Remover um agente da solução deixa os componentes dele, com soluções separadas importa-se primeiro a do conector personalizado, e Show dependencies mostra quem usa um componente.

Referências de conexão

Soluções levam referências de conexão, não credenciais nem conexões. Em cada ambiente de destino, uma conexão local é associada à referência, durante ou depois da importação, ou informada no assistente do pipeline. A conexão do SharePoint guarda só a credencial; site e lista são parâmetros que vão em variáveis de ambiente.

Variáveis de ambiente

Têm definição (com valor padrão) e valor atual, que prevalece; o valor atual exportado viaja na solução e é usado no destino, então use Remove from this solution para não levar o valor de desenvolvimento. Os tipos incluem Text (URLs e textos), Two options (liga e desliga), JSON, Data source (parâmetros de conector, como site e lista do SharePoint em variáveis separadas) e Secret (Azure Key Vault), todos com limite de 2.000 caracteres. Em solução gerenciada, o valor atual é personalização não gerenciada e aparece na solução Default. No Copilot Studio são lidas como Environment.nome_de_esquema, somente leitura, e mudar o valor exige republicar o agente, exceto Secret, lida em tempo de execução.

Variável Secret com Azure Key Vault

A assinatura do cofre precisa do provedor de recursos Microsoft.PowerPlatform. Quem cria a variável e o Dataverse precisam da função Key Vault Secrets User, validada ao salvar; Key Vault Reader era a orientação antiga e não basta. Para o Copilot Studio usar o segredo, o serviço Microsoft Copilot Studio Service precisa de Key Vault Secrets User e o segredo precisa da tag AllowedBots (por agente) ou AllowedEnvironments (por ambiente).

Pipelines da Power Platform: ambientes e funções

O host é um ambiente de produção que guarda configurações, artefatos e histórico, sem precisar ser Managed Environment; os destinos precisam ser Managed Environments e o desenvolvimento pode ser ambiente de desenvolvedor. Um ambiente se associa a um único host. Pipelines pessoais no host da plataforma aceitam uma origem e dois destinos e não são compartilhados nem estendidos; para isso, host personalizado. Deployment Pipeline User executa pipelines compartilhados e Deployment Pipeline Administrator controla a configuração; os pipelines só aparecem em solução não gerenciada (não na padrão) e não implantam em outro tenant, caso em que se usa Azure DevOps ou GitHub com Build Tools.

Execução, delegação e extensões de pipeline

O pipeline exporta a solução ao pedir a implantação e guarda um artefato imutável que segue os estágios em sequência; mudança nova exige incrementar a versão e implantar desde o primeiro estágio. O assistente pede conexões para as referências e valores para variáveis sem valor, implanta como gerenciada e mostra notas geradas por IA, ligadas por pipeline em AI deployment notes no app Deployment Pipeline Configuration. Allow redeployments of older versions libera Redeploy de uma implantação anterior, sobrescrevendo a atual. A implantação delegada usa Stage Owner (não implanta referências de conexão OAuth) ou Service Principal; Pre-export Step Required usa OnDeploymentRequested e Pre-deployment Step Required usa OnPreDeploymentStarted com UpdatePreDeploymentStepStatus em 20 (concluir) ou 30 (rejeitar).

Macetes para memorizar

💡 Limites dos conjuntos

Única até 100; conversa 20 casos de 12 mensagens; Quick gera 10.

💡 Escolha do método

Sentido = Compare meaning; Forma = Text similarity; Idêntico = Exact; Palavras = Keyword; Caminho = Tool use; Regra própria = Custom; Nada de gabarito = General quality.

Invalid

General quality não pede nada; os demais pedem gabarito, e sem ele o caso vira Invalid.

Tipos de importação

Upgrade apaga o que sumiu; Update só substitui; patch nunca apaga.

Gerenciada

Dev não gerenciada, resto gerenciada; gerenciada não sai (não exporta) e editar nela cria camada que tranca as versões.

Extensões de pipeline

Pre-export pede OnDeploymentRequested; Pre-deployment pede OnPreDeploymentStarted; 20 aprova, 30 rejeita, 10 é pendente.

Sintaxe de variável de ambiente

Environment. no tópico; @environmentVariables no conector; Secret dispensa republicar.

Tabela de memorização: não confunda

Quando é...	...e quando é
General quality Não há respostas esperadas e o foco é relevância, fundamentação, completude e abstenção.	**Custom** O critério é próprio do negócio, como aprovar recusas apropriadas, com instruções e rótulos Pass ou Fail.
Compare meaning A mesma ideia pode vir com outras palavras.	**Text similarity** A redação e a estrutura das frases precisam ficar próximas da esperada, aceitando pequenas variações.
Keyword match A redação varia, mas certos termos (como protocolo e telefone) precisam aparecer, no modo Any ou All.	**Exact match** A resposta deve ser idêntica caractere por caractere, como um código ou frase fixa.
Upgrade Componentes retirados no desenvolvimento devem sumir também do destino.	**Update** Substituir a solução gerenciada mantendo no ambiente componentes que não estão na nova versão.
Stage Owner Implantação delegada simples, sem referências de conexão para conexões OAuth na solução.	**Service Principal** Implantação delegada de solução com referências de conexão OAuth, como Office 365 Outlook e SharePoint.
Pre-export Step Required Validar antes de a solução ser exportada do desenvolvimento, com fluxo em OnDeploymentRequested.	**Pre-deployment Step Required** Verificar depois da aprovação e antes de implantar, com OnPreDeploymentStarted e UpdatePreDeploymentStepStatus.
Pipelines da Power Platform Implantar no mesmo tenant, entre ambientes associados a um host, com aprovação e histórico.	**Azure DevOps ou GitHub com Build Tools** Entregar a clientes em outros tenants, com controle de código-fonte e configurações de implantação por cliente.

Números que caem

Item	Valor
Casos por conjunto de respostas únicas (inclusive importados)	**até 100**
Conjunto de conversa	**até 20 casos, cada um com até 12 mensagens (6 pares)**
Quick question set	**10 perguntas**
Nota mínima padrão do Compare meaning	**50**
Tamanho máximo do valor de variável de ambiente	**2.000 caracteres**
Status de etapa de pipeline	**10 pendente; 20 concluir; 30 rejeitar**
Ícone do agente após importar a solução	**pode levar até 24 horas para aparecer**
Pipeline pessoal no host da plataforma	**1 ambiente de origem e 2 de destino**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Adicionar Response time como método com limite de segundos, ou achar que a avaliação reprova casos lentos.
Como não cair: Response time é medida automática vista no caso; não é método e não muda Pass nem Fail.

⚠ **Alerta de prova:** Importar 260 perguntas num único arquivo porque o limite valeria só para casos criados à mão.
Como não cair: Conjuntos de respostas únicas têm até 100 casos também na importação; divida em vários conjuntos.

⚠ **Alerta de prova:** Usar um conjunto de conversa para caber mais casos.
Como não cair: Conjunto de conversa aceita até 20 casos, menos que os 100 de respostas únicas.

⚠ **Alerta de prova:** Escolher Compare meaning num conjunto de conversa.
Como não cair: Compare meaning, Text similarity e Exact match são só para respostas únicas.

⚠ **Alerta de prova:** Baixar a nota mínima do General quality ou trocar o método para Exact match para casos reprovados passarem.
Como não cair: General quality não tem nota configurável e trocar método esconde a falha; corrija conhecimento ou descrições.

⚠ **Alerta de prova:** Pedir a função Agent viewer ou o conjunto como coproprietário para ver respostas de uma execução de outro maker.
Como não cair: Respostas e explicações ficam com quem iniciou a execução; rode você mesmo o conjunto.

⚠ **Alerta de prova:** Publicar o agente ou definir a solução como preferencial para levar à solução componentes que já existem.
Como não cair: Publicar não mexe em soluções e a preferencial só vale para itens novos; use Add existing ou Add required objects.

⚠ **Alerta de prova:** Editar o tópico direto na produção e exportar a solução gerenciada como cópia, ou importar a gerenciada de volta no desenvolvimento.
Como não cair: Gerenciada não exporta nem pode ser importada sobre a origem; altere a não gerenciada no desenvolvimento e exporte nova versão gerenciada.

⚠ **Alerta de prova:** Entregar um patch ou importar com Update para remover tópico e ferramenta da produção.
Como não cair: Patch só adiciona ou atualiza e Update mantém componentes ausentes; exporte nova versão gerenciada e importe com Upgrade.

⚠ **Alerta de prova:** Preencher o valor padrão ou trocar o tipo para Secret para o assistente pedir o valor na importação.
Como não cair: O pedido aparece quando a variável chega sem valor padrão e sem valor atual; tire o valor atual com Remove from this solution.

⚠ **Alerta de prova:** Ler a variável de ambiente no Power Fx com Env., EnvironmentVariable() ou Global.
Como não cair: No Copilot Studio o prefixo é Environment seguido do nome de esquema; no conector personalizado a sintaxe é @environmentVariables.

⚠ **Alerta de prova:** Dar Key Vault Reader a quem cria a variável Secret quando aparece erro de autorização ao salvar.
Como não cair: A função exigida é Key Vault Secrets User; a tag AllowedBots resolve outro erro, o de uso pelo agente em tempo de execução.

⚠ **Alerta de prova:** Manter Stage Owner na implantação delegada de solução com conexões OAuth, ou criar um estágio por cliente para outros tenants.
Como não cair: Stage Owner não implanta referências de conexão OAuth (use Service Principal), e pipelines da Power Platform não cruzam tenants.

⚠ **Alerta de prova:** Corrigir um tópico sem mudar a versão e esperar que a correção chegue à produção pelo pipeline.
Como não cair: O pipeline leva o mesmo artefato já validado no estágio anterior; incremente a versão e implante desde o primeiro estágio.

Como cai na prova

📝 **Como cai:** Equipe descreve um critério de qualidade e pergunta qual método de avaliação usar.
Como resolver: Pergunte se há resposta esperada; se não, General quality ou Custom; se há, decida entre sentido (Compare meaning), forma (Text similarity), igualdade (Exact match), termos (Keyword match) ou caminho (Tool use).

📝 **Como cai:** Resultado de avaliação com taxa alta, caso reprovado ou execução de colega para analisar.
Como resolver: Abra o caso, filtre por Fail, use Show activity map e a lista de recursos; lembre que respostas de execução alheia só aparecem rodando você mesmo e que Response time não pesa.

📝 **Como cai:** Mudança precisa chegar à produção gerenciada e um maker propõe atalhos.
Como resolver: Descarte editar em produção, exportar gerenciada, converter tipos ou importar gerenciada no desenvolvimento; altere a não gerenciada, aumente a versão e importe como gerenciada (Upgrade para remover).

📝 **Como cai:** Valor que muda entre ambientes (URL, e-mail, site e lista, chave secreta, liga e desliga).
Como resolver: Escolha o tipo da variável de ambiente pelo dado, deixe o valor atual fora da solução e lembre de republicar o agente (exceto Secret) e de salvar de novo o conector personalizado.

📝 **Como cai:** Configuração de pipeline com requisitos de compartilhamento, número de estágios, aprovação, delegação ou outro tenant.
Como resolver: Mais de dois destinos, compartilhamento ou extensões pedem host personalizado; conexões OAuth na delegação pedem Service Principal; validação antes da exportação é Pre-export; outro tenant sai dos pipelines para Azure DevOps ou GitHub.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
Mais de 100 perguntas de resposta única com resposta esperada	**Dividir em vários conjuntos de teste de até 100 casos.**

Manter o contexto ao longo de várias trocas de mensagem	**Conjunto de teste de conversa (até 20 casos de 12 mensagens).**
Sem respostas esperadas, avaliar relevância, fundamentação e completude	**General quality.**
Recusa correta marcada para melhoria	**Método Custom com instruções e rótulos.**
Redação livre, mas termos obrigatórios em toda resposta	**Keyword match no modo All.**
Garantir que a ferramenta certa resolveu o pedido	**Método Tool use com a ferramenta esperada em cada caso.**
Ver quais casos melhoraram ou pioraram após uma mudança	**Compare with entre duas execuções do mesmo conjunto.**
Agente novo sem conhecimento nem tópicos e conjunto inicial rápido	**Quick question set (10 perguntas).**
IdentifierNotRecognized ao publicar agente importado	**Dependência que faltou na solução; incluir na origem e exportar de novo.**
Versões importadas com sucesso que não aparecem no agente da produção	**Remove unmanaged layer em See solution layers.**
Voltar a produção para a versão anterior sem importar arquivo à mão	**Allow redeployments of older versions e Redeploy no histórico.**
Chave de liga e desliga diferente por ambiente	**Variável de ambiente Two options.**
Prefixo próprio nos nomes de esquema de tudo que for criado	**Publisher com o prefixo e solução dele antes de criar os componentes.**
Maker não encontra a opção de implantação ao abrir o agente	**O agente está na solução padrão; colocá-lo numa solução não gerenciada própria.**

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

- General quality é o único método que não exige resposta esperada nem palavras-chave; os outros sem item esperado dão Invalid.
- Default Solution não exporta e soluções gerenciadas não exportam; o ALM parte de uma solução não gerenciada própria.
- Depois de importar o agente: refazer autenticação e publicar antes de compartilhar.
- Variável de ambiente: valor atual prevalece, limite de 2.000 caracteres, Environment. no tópico e republicar após mudar (exceto Secret).
- Pipelines exigem destinos Managed Environments, não cruzam tenants e levam sempre o mesmo artefato da versão.

Essenciais para a prova (checklist)

- ☐ Sei as formas de criar conjuntos de teste e os limites de 100 casos e de 20 casos com 12 mensagens.
- ☐ Sei escolher entre General quality, Compare meaning, Text similarity, Exact match, Keyword match, Tool use, Content safety e Custom.
- ☐ Sei interpretar Pass, Fail, Invalid e Error, usar Show activity map, Compare with e Export test results.
- ☐ Sei o que a função Agent viewer permite e quem vê as respostas de uma execução.
- ☐ Sei criar publisher e solução no Copilot Studio e usar Add existing, Agent e Add required objects.
- ☐ Sei o que não viaja na exportação de agentes e o que fazer após a importação.
- ☐ Sei quando usar Upgrade, Update ou patch e como remover uma camada não gerenciada.
- ☐ Sei escolher o tipo de variável de ambiente e controlar valor padrão e valor atual na exportação.
- ☐ Sei configurar o Key Vault para variáveis Secret, com Key Vault Secrets User e a tag AllowedBots.
- ☐ Sei montar pipelines com host personalizado, funções, delegação, extensões, reimplantação e notas por IA.

Questões de revisão do capítulo

R3.1 · Testar e gerenciar agentes

Na Corretora de Imóveis Lar Ideal, o maker quer criar no Evaluation um conjunto com 40 perguntas de resposta única geradas a partir das fontes de conhecimento do agente, que usa orquestração generativa. Qual caminho usar?

A. Full question set, com o número de perguntas e Knowledge sources como referência
B. Import a file, com o arquivo das fontes de conhecimento no lugar da planilha
C. Use your test chat conversation, que transforma as fontes em perguntas de teste
D. Quick question set, que gera as perguntas a partir das fontes de conhecimento escolhidas

R3.2 · Testar e gerenciar agentes

Na Cooperativa Leiteira Vale Verde, o conector personalizado do ERP ficou numa solução própria, e o agente, com a referência de conexão desse conector, ficou em outra solução. Ao levar tudo para o ambiente de teste, como ordenar a importação?

A. Importar a solução do agente primeiro, para criar a referência de conexão antes do conector
B. Importar primeiro a solução do conector personalizado e depois a solução do agente
C. Importar a solução do agente e deixar o conector ser criado pelo agente na publicação
D. Importar as duas soluções juntas num único arquivo compactado com as duas pastas

R3.3 · Testar e gerenciar agentes

O agente da Seguradora Porto Calmo chama, num nó Send HTTP request, uma API cuja URL base muda entre desenvolvimento, teste e produção. Ela foi criada como variável de ambiente com o nome de esquema psc_UrlApiApolices. Como montar a URL na fórmula Power Fx do nó?

A. EnvironmentVariable("psc_UrlApiApolices") & "/apolices"
B. Environment.psc_UrlApiApolices & "/apolices"
C. Env.psc_UrlApiApolices & "/apolices"
D. Global.psc_UrlApiApolices & "/apolices"

R3.4 · Testar e gerenciar agentes

O desenvolvedor do Frigorífico Campo Nobre vai guardar a chave da API de rastreabilidade no Azure Key Vault e referenciá-la numa variável de ambiente do tipo Secret, usada pelo agente. A assinatura já tem o provedor de recursos Microsoft.PowerPlatform registrado. Ao salvar a variável, aparece o erro: User isn't authorized to read secrets from Azure Key Vault path. O que resolve?

A. Dar ao desenvolvedor a função Key Vault Reader no cofre, em Access control (IAM)
B. Dar ao desenvolvedor a função Key Vault Secrets User no cofre, em Access control (IAM)
C. Adicionar ao segredo a tag AllowedBots com o ambiente e o nome de esquema do agente
D. Trocar o tipo da variável para Text e colar a chave no valor atual dela

Respostas comentadas

R3.1. A) Full question set, com o número de perguntas e Knowledge sources como referência
Por quê: Conjuntos de resposta única podem vir do Quick question set (10 perguntas da descrição e instruções), do Full question set (conhecimento ou tópicos, com quantidade definida), do chat de teste, de importação ou de escrita manual.
✗ B) Incorreta. A importação espera um arquivo .csv ou .txt com as colunas Question e Expected response, não os documentos das fontes.
✗ C) Incorreta. Essa opção usa as perguntas da conversa mais recente do chat de teste, não as fontes de conhecimento.
✗ D) Incorreta. O Quick question set gera 10 perguntas com base na descrição, nas instruções e nas capacidades do agente; não escolhe quantidade nem fonte.

> **Dica de prova:** Quantidade definida e base no conhecimento: Full question set.

R3.2. B) Importar primeiro a solução do conector personalizado e depois a solução do agente
Por quê: Com soluções separadas, importe as dependências antes de quem depende delas: conector personalizado primeiro, agente com referências de conexão depois. Uma solução que dependa de componente ausente falha na importação.
✗ A) Incorreta. A ordem é a inversa: o conector precisa existir no destino antes da solução que depende dele.
✗ C) Incorreta. A publicação do agente não cria conectores personalizados no ambiente.
✗ D) Incorreta. Cada solução é importada separadamente; a ordem de dependência continua valendo.

> **Dica de prova:** Conector personalizado em solução separada: ele entra primeiro.

R3.3. B) Environment.psc_UrlApiApolices & "/apolices"

Por quê: As variáveis no Copilot Studio têm prefixos por escopo: System, Global, Topic e Environment. Variáveis de ambiente são lidas com Environment e o nome de esquema, sem poder ser alteradas pelo autor.

✗ A) Incorreta. Não existe essa função no Power Fx do Copilot Studio; a variável é lida pelo prefixo Environment.

✗ C) Incorreta. O prefixo Env não existe no Copilot Studio; as variáveis de ambiente usam o prefixo Environment.

✗ D) Incorreta. Global é o escopo das variáveis globais da conversa, não das variáveis de ambiente da solução.

> **Dica de prova:** Variável de ambiente no Power Fx do Copilot Studio: prefixo Environment.

R3.4. B) Dar ao desenvolvedor a função Key Vault Secrets User no cofre, em Access control (IAM)

Por quê: Para variáveis de ambiente do tipo Secret, a assinatura do cofre precisa do provedor Microsoft.PowerPlatform, e o usuário que cria a variável e o Dataverse precisam da função Key Vault Secrets User. A validação de acesso roda ao salvar.

✗ A) Incorreta. Key Vault Reader era a função das instruções antigas e não basta para ler o conteúdo do segredo; a documentação pede Key Vault Secrets User.

✗ C) Incorreta. A tag AllowedBots libera o segredo para o agente em tempo de execução; o erro ao salvar indica falta de permissão de quem cria a variável.

✗ D) Incorreta. Uma chave em variável do tipo Text não é criptografada e fica exposta, o que contraria o uso do Key Vault.

> **Dica de prova:** Erro ao salvar variável Secret: falta Key Vault Secrets User para quem a cria.

DIA DA PROVA

Estratégia de prova

O exame AB-620 é de nível Associate e pensa como quem constrói e integra agentes no Copilot Studio: quase todo enunciado é um cenário de empresa com uma restrição que decide a resposta, como sem login, sem copiar dados, sem segredo, sem criar tópicos ou mantendo o ALM de outra equipe. As alternativas erradas costumam ser recursos reais aplicados no lugar errado, com o sentido invertido ou no escopo errado (agente inteiro quando se pede um nó). Muitas alternativas usam os nomes exatos das opções do Copilot Studio, e várias questões trazem mensagens de erro literais que apontam a causa. Há questões de múltipla resposta, em que cada afirmação precisa ser conferida isoladamente contra requisitos exatos. O domínio de integração tem o maior peso, então MCP, A2A, Foundry, Fabric, Azure AI Search e Application Insights pesam muito na nota.

Como responder

✓ Planeje o tempo: são 120 minutos para cerca de 40 a 60 itens (a Microsoft não divulga o número exato), com pontuação de 1 a 1000 e mínimo de 700.

✓ Distribua a revisão pelo peso oficial: Integrar e estender 40-45%, Planejar e configurar 30-35%, Testar e gerenciar 20-25%.

✓ Antes das alternativas, sublinhe a restrição do cenário (canal, público, cópia de dados, segredo, escopo de tópico, dono do componente) e decida o que ela elimina.

✓ Quando houver mensagem de erro literal, associe o código à causa antes de ler as opções e descarte quem trata de outra camada (autenticação x protocolo x política de dados).

✓ Em questões de múltipla resposta, julgue cada afirmação como verdadeira ou falsa sozinha e desconfie de limites inventados, sincronizações automáticas e prazos de cache.

✓ Prefira sempre o controle configurável e específico à instrução em texto: confirmação, acesso a dados e escopo de ferramenta não se resolvem nas instruções do agente.

✓ Nas questões de configuração, localize onde a opção mora (Microsoft 365 admin center, Power Platform admin center, Azure, Fabric, Foundry ou Copilot Studio) e elimine as que mudam a coisa no lugar errado.

✓ Marque para revisão as questões de dúvida entre duas opções parecidas e volte nelas com o par de comparação na cabeça.

Erros que derrubam candidatos

✗ Usar Authenticate with Microsoft fora do Teams e Microsoft 365 ou esquecer que a autenticação manual bloqueia esse canal.

✗ Confundir Copilot connector (copia para o Graph) com conhecimento em tempo real (consulta a fonte com o token do usuário).

✗ Trocar protocolos: informar a URL do cartão no A2A, usar MCP para delegar a outro agente ou SSE como transporte.

✗ Escolher agente filho quando o cenário exige dono, publicação e ALM próprios, ou dividir em agentes conectados sem necessidade.

✗ Resolver no agente inteiro o que o enunciado pede só para um tópico ou nó, como moderação e fontes.

✗ Escolher o método de avaliação pelo nome sem conferir se ele exige resposta esperada e se vale para conjunto de conversa.

✗ Propor atalhos fora do ALM: editar a produção gerenciada, exportar solução gerenciada, usar Update ou patch para remover componentes.

Na semana da prova

- ☐ Revise as comparações de cada capítulo até conseguir dizer, para cada par, a frase de quando usar cada lado.
- ☐ Refaça as provas práticas por domínio, começando pelo de integração, e anote cada erro com a restrição do cenário que você ignorou.
- ☐ Monte uma folha com mensagens de erro e causas (400 Activity, 404 Version not found, CuaInsert... sem HTTPS, DataLossPreventionViolation, IdentifierNotRecognized, A JSON could not be generated, Analysis failed).
- ☐ Decore os números que viram alternativa: 100 e 20x12 casos, 2.000 caracteres, 30 segundos de timeout, 2 minutos do fluxo, 5 MB de payload, 25 fontes, 500 arquivos, 90 dias de retenção.
- ☐ Na véspera, releia só as seções lembrar e macetes dos três capítulos e descanse.

☐ No dia, leia primeiro a pergunta no fim do enunciado e só depois o cenário, procurando a restrição que decide.

REVISÃO FINAL

Folha de cola

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

1. Integrar e estender agentes no Copilot Studio

‣ HTTP 400 dizendo que o endpoint não suporta Activity → **Habilitar o protocolo Activity no agente do Foundry pela API REST ou pelo SDK.**

‣ 404 - Version not found ao conectar agente do Foundry → **Agente criado no portal anterior do Foundry, não suportado.**

‣ CuaInsertCredentialNotAllowedInInsecureWebsites → **O site é acessado por http; o computer use não insere credenciais sem HTTPS.**

‣ Botão Publish indisponível e banner com Details listando a fonte de conhecimento → **Política de dados no Power Platform admin center bloqueando o conector da fonte.**

‣ DataLossPreventionViolation num agente com servidor MCP → **Relatório de violações na página Channels e liberação do conector na política.**

⚠ O campo pede o endpoint de comunicação; o cartão é lido sozinho a partir do caminho padrão.

⚠ Endpoints de agentes do Foundry não aceitam chave de API; a autorização é Entra ID com RBAC (Foundry Agent Consumer).

⚠ Log conversation details grava ID, nome e texto do usuário; propriedades sensíveis são Log sensitive Activity properties; para privacidade, só Enable logging.

2. Planejar e configurar soluções de agente

‣ Visitantes anônimos no site, sem conta na empresa e conteúdo interno que não pode vazar → **No authentication, só fontes públicas como conhecimento, sem SharePoint, e canal de site.**

‣ Agente no Teams e no Microsoft 365 Copilot com o canal aparecendo bloqueado → **Trocar para Authenticate with Microsoft e ajustar tópicos que usavam User.AccessToken.**

‣ Site próprio, Entra ID e proibição de segredo de cliente com validade → **Authenticate manually com Microsoft Entra ID V2 with federated credentials.**

‣ Clientes sem login e funcionários autenticados só em um tópico do mesmo agente → **Authenticate manually com Require users to sign in desmarcado e nó Authenticate no tópico.**

‣ Fluxo com gatilho certo que não aparece em Add a tool → **O fluxo não está numa solução.**

⚠ UPIA e XPIA já são bloqueados por padrão nos agentes; um sistema externo de detecção é só monitoramento adicional opcional.

⚠ O nível do nó de respostas generativas prevalece sobre o do agente; ajuste no nó para não mudar todos os tópicos.

⚠ Return devolve do chamado para quem chamou; para enviar ao destino, marque Receive values from other topics na variável do destino.

3. Testar e gerenciar agentes

‣ Mais de 100 perguntas de resposta única com resposta esperada → **Dividir em vários conjuntos de teste de até 100 casos.**

‣ Manter o contexto ao longo de várias trocas de mensagem → **Conjunto de teste de conversa (até 20 casos de 12 mensagens).**

‣ Sem respostas esperadas, avaliar relevância, fundamentação e completude → **General quality.**

‣ Recusa correta marcada para melhoria → **Método Custom com instruções e rótulos.**

‣ Redação livre, mas termos obrigatórios em toda resposta → **Keyword match no modo All.**

⚠ Response time é medida automática vista no caso; não é método e não muda Pass nem Fail.

⚠ Conjuntos de respostas únicas têm até 100 casos também na importação; divida em vários conjuntos.

⚠ Conjunto de conversa aceita até 20 casos, menos que os 100 de respostas únicas.

GABARITO

Respostas do diagnóstico

D1. D) Nome, descrição e URL do servidor, além do tipo de autenticação exigido por ele → revise o capítulo 1

Por quê: O assistente de MCP é a forma recomendada de conectar um servidor existente: nome, descrição e URL, mais o tipo de autenticação. As ferramentas expostas pelo servidor aparecem no agente sem cadastro manual.

✗ A) Incorreta. As ferramentas e seus esquemas vêm do próprio servidor e são lidos dinamicamente; não são digitados pelo maker.

✗ B) Incorreta. O arquivo OpenAPI com a extensão do protocolo é usado no caminho alternativo, criando um conector personalizado no Power Apps, não no assistente.

✗ C) Incorreta. O assistente pede a URL do servidor remoto; não há campo para comando de inicialização local.

> **Dica de prova:** Assistente de MCP: nome, descrição, URL e autenticação.

D2. A) Usar Maker-provided credentials, com a conta da empresa na conexão → revise o capítulo 1

Por quê: Cada ferramenta escolhe a autenticação: End user (padrão), em que cada usuário acessa só o que pode ver, ou Maker-provided, que usa as credenciais do autor para recursos compartilhados.

✗ B) Incorreta. Pedir chave de API ao visitante expõe o segredo e não resolve a falta de conta.

✗ C) Incorreta. Authenticate with Microsoft deixa o agente disponível no Teams e no Microsoft 365 com contas da organização, não para visitantes anônimos do site.

✗ D) Incorreta. Credenciais do usuário final exigem que cada pessoa tenha acesso ao serviço, o que os visitantes não têm.

> **Dica de prova:** Dado igual para todos e usuário sem conta: Maker-provided credentials na ferramenta.

D3. C) Ajustar o conector de conhecimento do SharePoint na política de dados → revise o capítulo 1

Por quê: Fontes de conhecimento do Copilot Studio são governadas por conectores na política de dados, como Knowledge source with SharePoint and OneDrive in Copilot Studio. Uma violação desativa Publish e mostra os itens afetados em Details.

✗ A) Incorreta. O bloqueio vem da classificação do conector na política de dados, não do tipo de autenticação do agente.

✗ B) Incorreta. Políticas de dados da Power Platform são configuradas no Power Platform admin center, não no Microsoft Purview.

✗ D) Incorreta. A isenção de política de dados para agentes não é mais suportada; a aplicação das políticas vale para todos os locatários.

> **Dica de prova:** Publish desativado com fonte listada em Details: política de dados no Power Platform admin center.

D4. D) Desmarcar Allow agent to decide dynamically when to use the tool → revise o capítulo 2

Por quê: Em Additional details da ferramenta, Allow agent to decide dynamically when to use the tool permite à orquestração generativa escolher a ferramenta. Desmarcada, a ferramenta fica restrita às chamadas explícitas de tópicos.

✗ A) Incorreta. Sem descrição o orquestrador escolhe pior, mas a ferramenta continua disponível para ele.

✗ B) Incorreta. Desligar Enabled bloqueia a ferramenta para qualquer uso, inclusive pelo tópico.

✗ C) Incorreta. Essa opção só pede confirmação ao usuário; o orquestrador continuaria escolhendo a ferramenta.

> **Dica de prova:** Ferramenta só pelo tópico: desmarque Allow agent to decide dynamically.

D5. A) Reduzir a moderação nas propriedades do nó desse tópico, que prevalece sobre a do agente → revise o capítulo 2

Por quê: Os níveis de moderação vão de Lowest a Highest (padrão High) no agente e no nó. Nível mais baixo gera mais respostas com mais risco de conteúdo nocivo; mais alto filtra mais e responde menos. O nível do nó prevalece sobre o do agente.

✗ B) Incorreta. O nível do agente é o padrão e não prevalece sobre o do nó; além disso, mudaria o comportamento de todos os tópicos, contra o requisito.

✗ C) Incorreta. Trocar a orquestração não muda a regra de precedência da moderação e afetaria o agente inteiro.

✗ D) Incorreta. O Conversational boosting também usa um nó de respostas generativas sujeito à moderação; não é um caminho sem filtro.

> **Dica de prova:** Moderação no nó de respostas generativas vence a do agente para aquele tópico.

D6. A) Marcar a variável do nome no destino com Receive values from other topics e passá-la ao redirecionar → revise o capítulo 2

Por quê: Variáveis de tópico podem receber valores de outros tópicos, devolver valores ao tópico de origem, ou ambos. Isso evita globais; variáveis de data e hora, duração, múltipla escolha e entidades personalizadas não podem ser passadas.

✗ B) Incorreta. Uma variável global não pode voltar a ser variável de tópico, e o requisito é não criar globais.

✗ C) Incorreta. Return values to original topics devolve um valor do tópico chamado para quem o chamou; aqui o valor precisa ir da origem para o destino.

✗ D) Incorreta. Variáveis baseadas em entidades personalizadas não podem ser passadas entre tópicos, e uma entidade não compartilha valores.

> **Dica de prova:** Passar valor no redirecionamento: Receive values from other topics no destino.

D7. A) Criar um publisher com prefixo solo e uma solução dele antes de novos itens → revise o capítulo 3

Por quê: O publisher define o prefixo dos nomes de esquema. Como o nome de um item de metadados não muda depois de criado, defina publisher e prefixo antes de criar os componentes.

✗ B) Incorreta. O publisher das soluções de sistema não pode ter o prefixo trocado.

✗ C) Incorreta. Exportar como gerenciada não muda nomes de esquema; o prefixo segue com o componente.

✗ D) Incorreta. O nome de um item de metadados não pode ser mudado depois de criado; o novo prefixo vale para componentes novos.

> **Dica de prova:** Prefixo próprio: publisher e solução antes de criar componentes.

D8. D) Se a opção AI deployment notes do pipeline está como Enabled no app Deployment Pipeline Configuration → revise o capítulo 3

Por quê: As notas de implantação geradas por IA vêm habilitadas por padrão e podem ser ligadas ou desligadas por pipeline no app Deployment Pipeline Configuration. Elas preenchem o campo de notas, que o maker pode revisar.

✗ A) Incorreta. A configuração das notas por IA fica em cada pipeline, no app de configuração do host, e não numa chave de locatário.

✗ B) Incorreta. Não existe pasta de notas na solução; as notas por IA são geradas pelo pipeline com base na solução.

✗ C) Incorreta. Implantação delegada define quem implanta; não é requisito para gerar notas por IA.

> **Dica de prova:** Notas de implantação por IA: configuração AI deployment notes do pipeline.

D9. C) Abrir Agent settings na criação e escolher a solução Garantias em Advanced settings → revise o capítulo 3

Por quê: Componentes novos só entram sozinhos na solução quando o agente está no contexto dela, seja por ter sido criado nela, em Agent settings, Advanced settings, seja por ser editado a partir dela ou pela solução preferencial. Fora disso, é preciso usar Add required objects antes de exportar.

✗ A) Incorreta. Publicar o agente atualiza os canais, mas não coloca componentes numa solução.

✗ B) Incorreta. A solução padrão não pode ser exportada para outros ambientes, e o pedido é usar a solução Garantias.

✗ D) Incorreta. Patches servem para atualizações incrementais de uma solução, não para mapear o agente a ela.

> **Dica de prova:** Agente novo já na solução certa: escolha a solução em Advanced settings ao criá-lo.

Agora, treine no formato real

Faça as 6 provas completas do curso AB-620: 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.