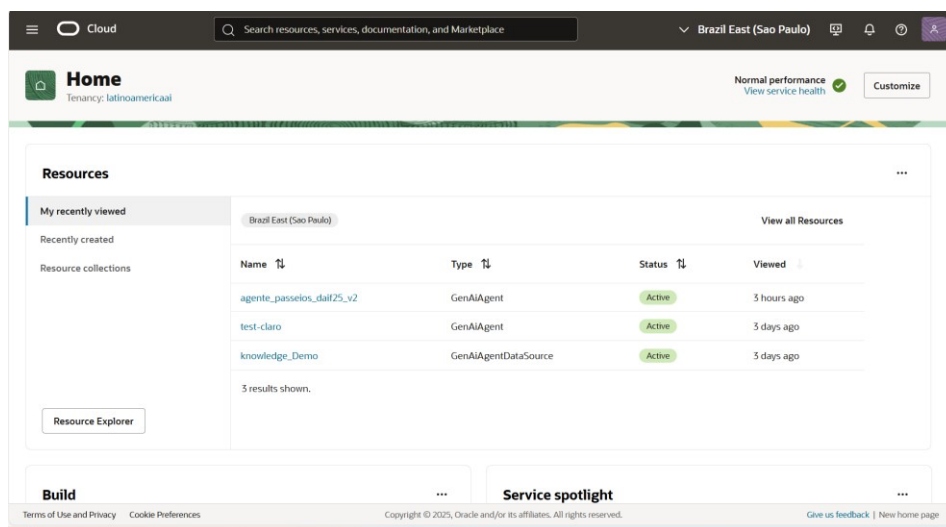


Laboratório prático de AI Agents OCI

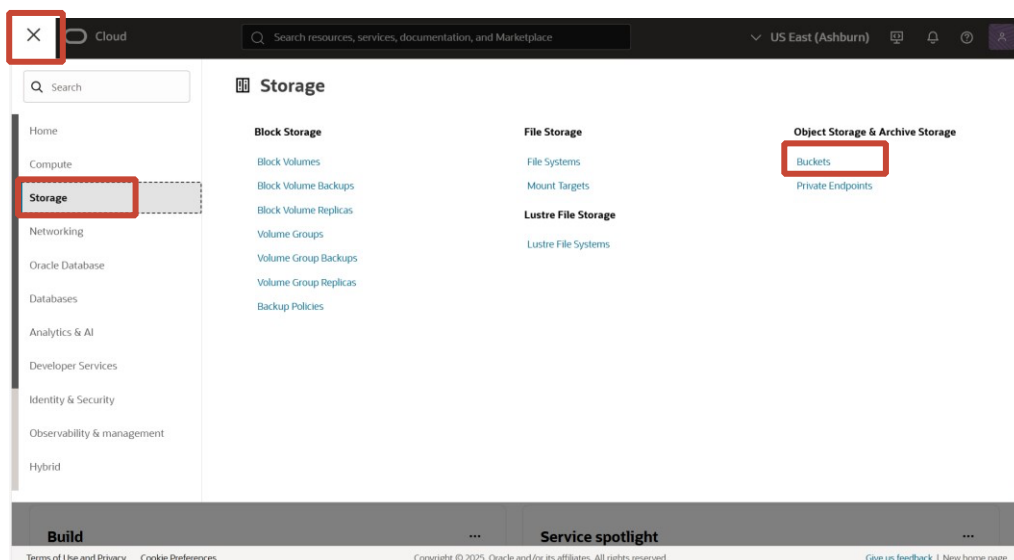


Subindo os arquivos para o agente ter acesso no bucket

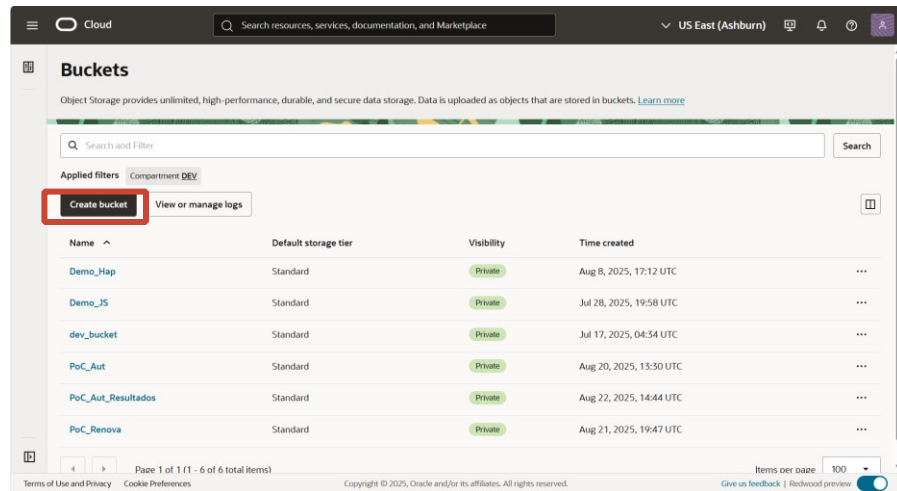
Como pré-requisito você deve ter acesso a console da OCI, como na imagem abaixo.



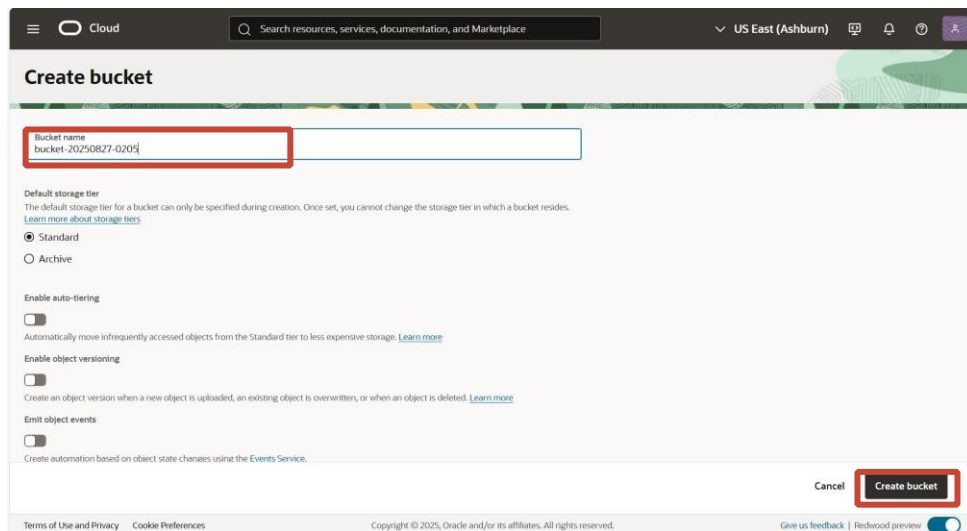
No menu lateral esquerdo, mais conhecido como menu de “hamburger”, vamos procurar storage e acessar o serviço bucket. Bucket é um serviço de armazenamento de arquivos, muitos utilizado como um repositório seguro dentro dos ambientes corporativos.



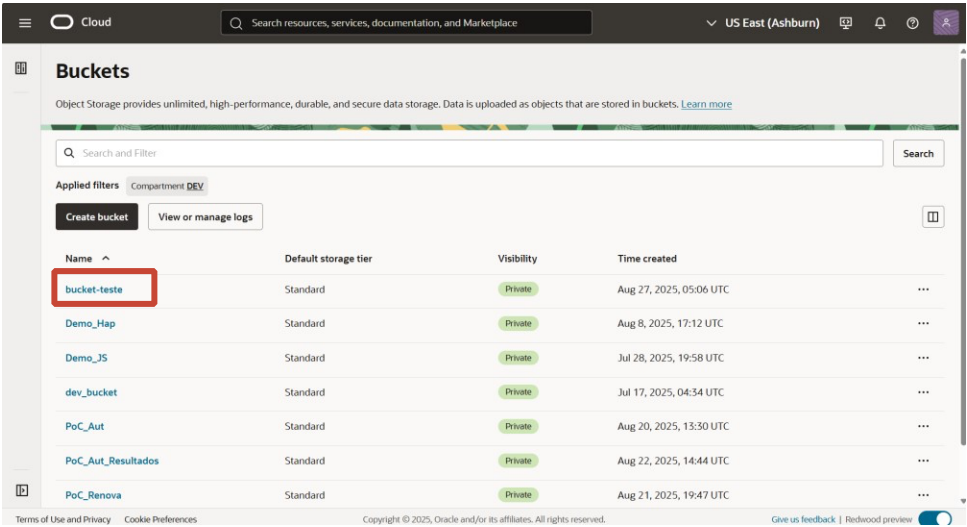
A tela principal do serviço deve apresentar todos os buckets que você tem criado no tenancy, região e compartment que estiverem selecionados.



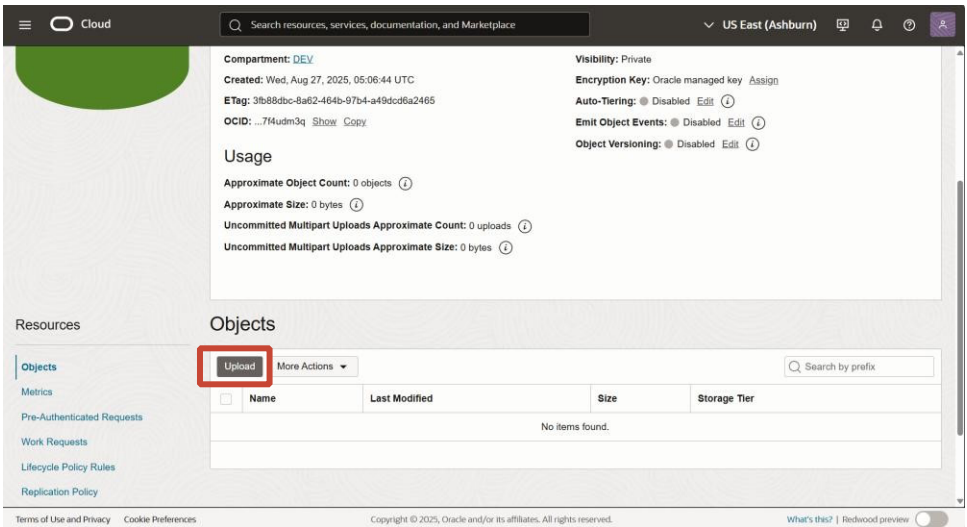
Vamos clicar em “create bucket”.



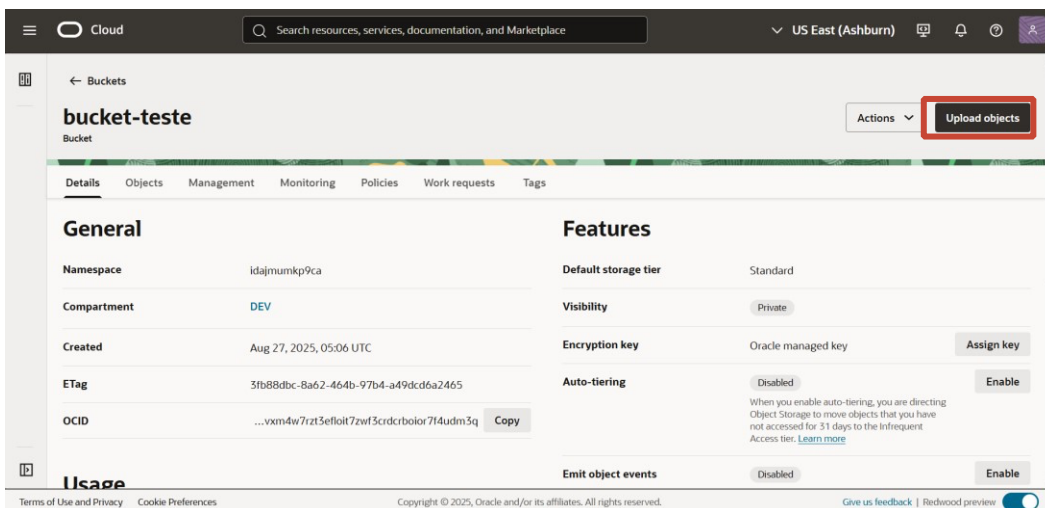
Todas as configurações vamos deixar padrão. A única alteração recomendada é inserir um nome que seja fácil de encontrar, mais para frente teremos que seleccionar esse bucket criado. Depois de alterar o nome clique em “create bucket”.



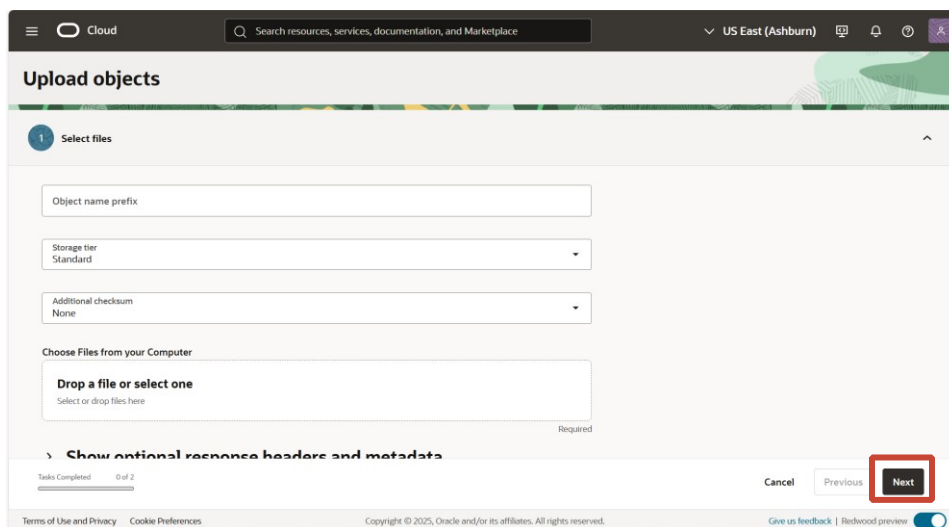
Logo, seu bucket já deve estar listado como disponível. Acesse ele clicando no seu nome.



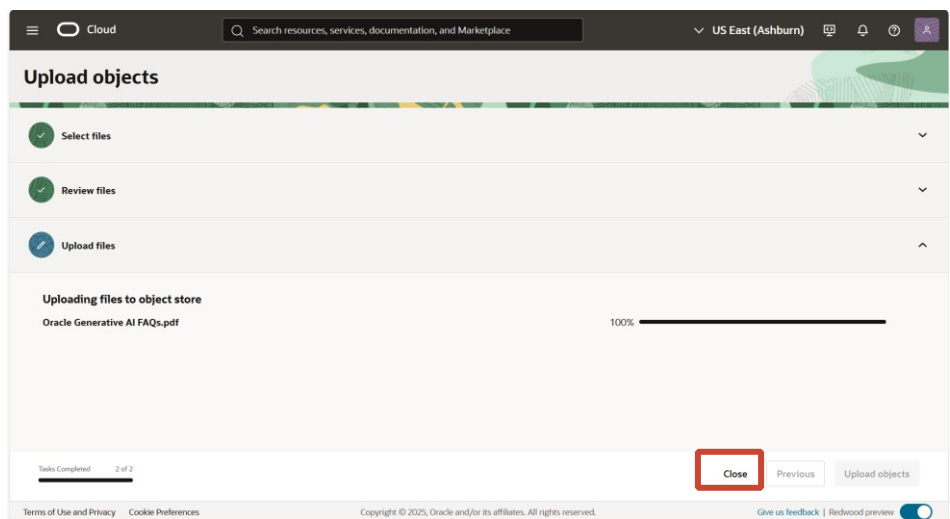
Dentro do bucket, você deve encontrar um botão mais para baixo da tela com a opção de fazer upload. Você pode estar com essa versão de cima, ou a de baixo. São versões de interface da OCI, a versão acima é antiga e a versão da imagem abaixo é a nova versão. De todo modo você vai encontrar facilmente o botão de upload na tela, clique nele.



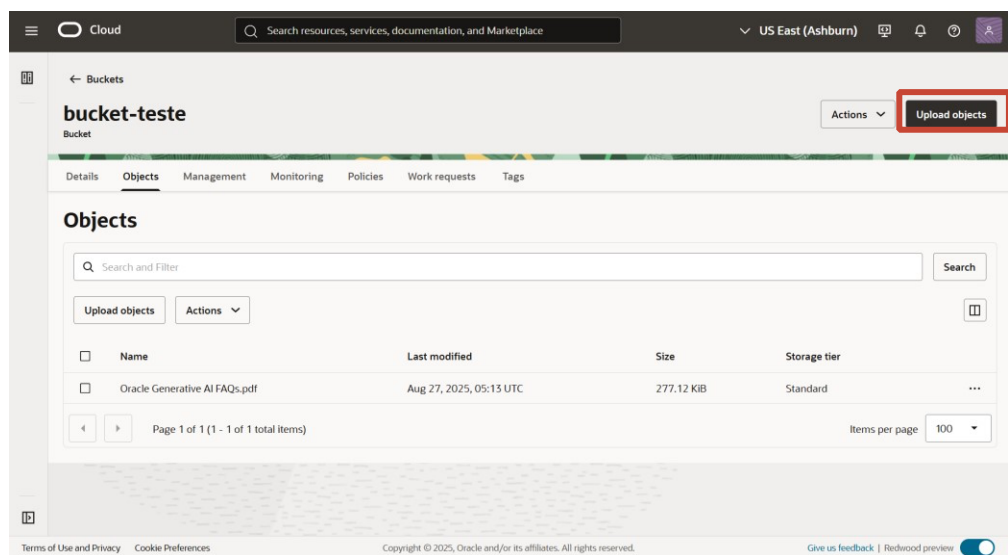
Você não precisa modificar nada nessa tela, apenas adicionar os arquivos via “Drag and drop” e clicar em next para seguir com a adição.



Vá clicando em “next” até que você encontre o botão de “upload files”. Como na tela abaixo. Nesse momento o sistema já concluiu a adição dos arquivos selecionados e você pode fechar essa tela via “close” no canto inferior direito.

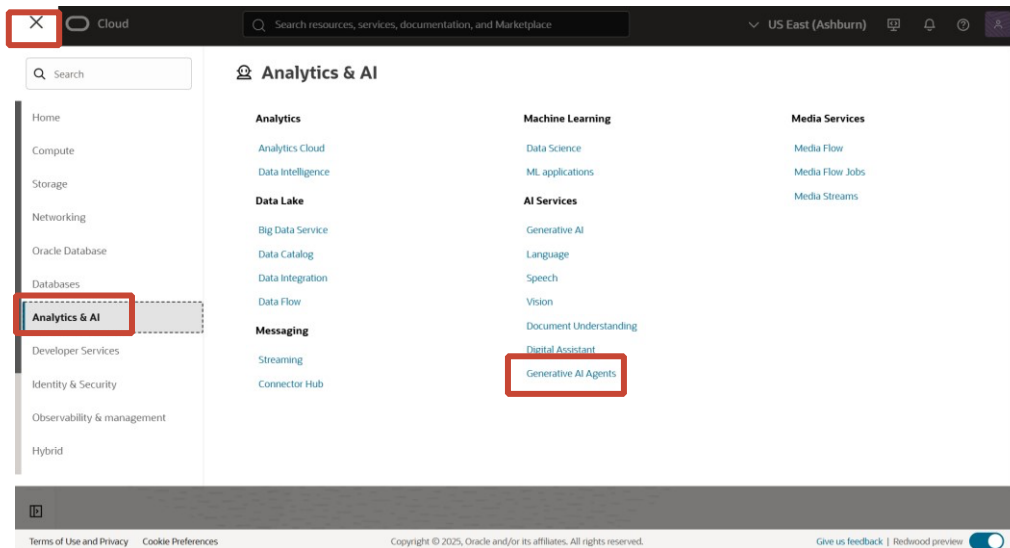


Verifique os documentos adicionados acessando “objects” dentro do bucket.

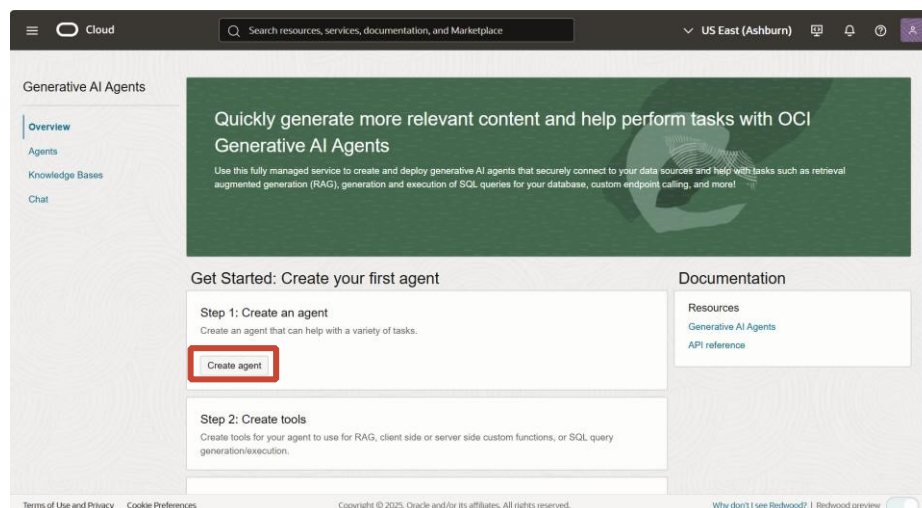


Criando o agente

Agora que você já tem os documentos que seu agente vai utilizar como base de conhecimento, vamos começar a criação do agente utilizando o serviço de Agents OCI da Oracle. Para isso, retorne ao menu de hamburguer e selecione o menu de “Analytics & AI”, buscando a opção de “Generative AI Agents”.



A tela que aparece é a interface do serviço de agentes. Na página de overview é possível ver os passos simples da criação de um agente. No menu lateral esquerdo também existe a aba “Agents” que lista todos os agentes criados, “Knowledge Base” que lista as bases de conhecimento desenvolvidas, ativas ou deletadas. E o menu “chat”, que permite que você converse com um agente ativo.



Vamos clicar em “create agent” no centro da tela para começar a criação do nosso agente.

The screenshot shows the 'Create agent' interface in the Oracle Cloud console. The 'Basic information' step is active, with a sidebar on the left showing steps 1 through 4. The main form contains fields for 'Name', 'Compartment' (set to 'DEV'), 'Description' (optional), 'Welcome message' (optional), and 'Routing instructions' (optional). The 'Name' field, the 'Welcome message' field, and the 'Next' button at the bottom are highlighted with red boxes. The footer includes 'Terms of Use and Privacy', 'Cookie Preferences', 'Copyright © 2025, Oracle and/or its affiliates. All rights reserved.', and a 'Redwood preview' toggle.

O primeiro passo é composto por informações básicas do agente. É obrigatório adicionar um nome para seu agente. Você também pode adicionar uma mensagem inicial dele no “Welcome message”, uma saudação para seu usuário. Uma descrição interna, para identificar do que se trata esse agente e rotas de instrução, para adicionar regras de como ele deve agir em cada nova execução. Nesse momento, vamos apenas adicionar nome e mensagem de boas-vindas, pode deixar os demais campos vazios. Quanto finalizar, clique no botão inferior esquerdo de “Next”.

The screenshot shows the 'Tools' step of the 'Create agent' interface. The sidebar on the left indicates that step 2, 'Add tool', is the current step. The main area is titled 'Tools' and contains a table with columns 'Name', 'Tool type', and 'Description'. The table is currently empty, with a message 'No items found.' and a pagination control 'Showing 0 items < 1 of 1 >'. The 'Add tool' button is highlighted with a red box. The footer is identical to the previous screenshot.

O segundo passo é composto por um dos elementos mais importantes de um agente, que é suas ferramentas. Nessa etapa vamos clicar no botão de adicionar ferramentas “Add tool”.

The screenshot shows the 'Add tool' step in the 'Create agent' wizard. On the left, a sidebar lists the steps: 1. Basic information, 2. Add tool (selected), 3. Setup agent endpoint, and 4. Review and create. The main area is titled 'Add tool' and contains four tool options: RAG, SQL, Custom tool, and Agent tool. The RAG tool is selected and highlighted with a blue checkmark. Below the tool options, the 'RAG Configuration' section is visible. It has a 'Name' field and a 'Description (required for routing)' field, both of which are highlighted with red boxes. Below these fields is a 'Custom instructions' field with the text 'You're a travel advisor. Answer in a conversational tone'. At the bottom of the 'RAG Configuration' section, there is a 'Create knowledge base' button, which is also highlighted with a red box. The bottom of the screen shows the 'Previous', 'Next', and 'Cancel' buttons, along with the 'Add tool' and 'Cancel' buttons for the current step.

Existem várias ferramentas pré construídas. RAG para processar informações não estruturadas, como textos. SQL para informações estruturadas, como bancos de dados transacionais. Custom tool para funções ou endpoints de serviços. E finalmente Agent tool para adicionar uma camada multi agêntica, permitindo que um agente seja adicionado como um recurso para outro agente. Nesse laboratório, como vamos utilizar PDFs para alimentar a base de conhecimentos, vamos utilizar somente a primeira opção, RAG.

This screenshot shows the 'Add tool' step in the 'Create agent' wizard, specifically the 'RAG Configuration' section. The 'Name' field is empty. The 'Description (required for routing)' field is empty. The 'Custom instructions' field contains the text 'You're a travel advisor. Answer in a conversational tone'. Below this, the 'Add knowledge bases' section is visible. It has a 'Compartment' dropdown menu with 'DEV' selected. Below the dropdown, there is a 'Create knowledge base' button, which is highlighted with a red box. The bottom of the screen shows the 'Previous', 'Next', and 'Cancel' buttons, along with the 'Add tool' and 'Cancel' buttons for the current step.

Descendo a tela na opção RAG, vamos precisar preencher um nome no campo “Name” e um prompt descritivo no campo “Description”. Esse prompt é exatamente as instruções que o agente vai utilizar para montar as repostas para o usuário final sobre a sua base de conhecimento então coloque um prompt bem descrito.

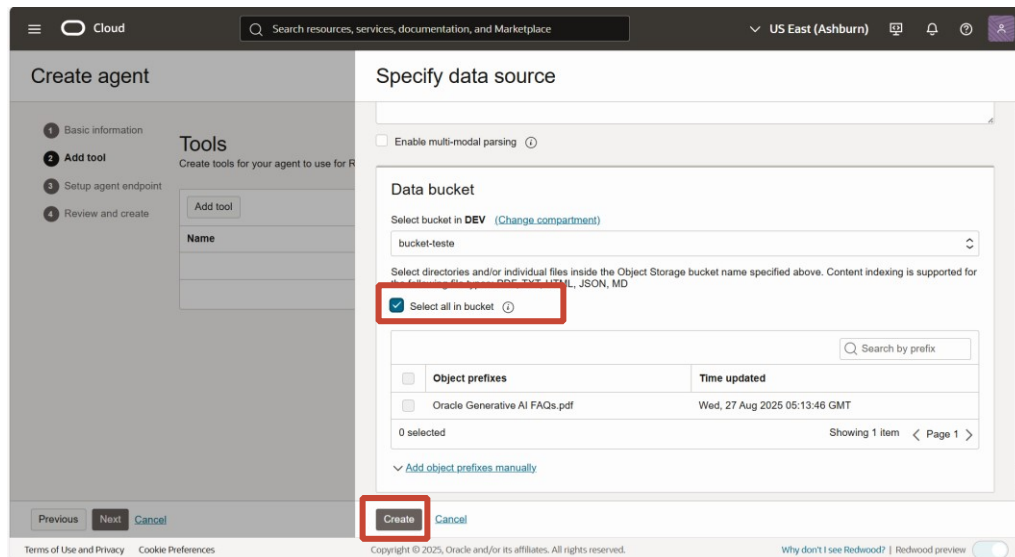
Uma vez preenchido, vamos criar uma base de conhecimento, clicando no botão “Create knowledge base”.

The screenshot shows the 'New knowledge base' form in the Oracle Cloud console. The form is titled 'New knowledge base' and has a subtitle 'Create a knowledge base that either imports content into a retrieval-augmented generation (RAG) system or uses your own data store.' The form includes several fields: 'Name' (a text input field), 'Compartment' (a dropdown menu with 'DEV' selected), 'Description' (a text input field with 'Optional' as a placeholder), 'Data store type' (a dropdown menu with 'Object storage' selected), and 'Enable hybrid search' (a checked checkbox). Below these fields is a section titled 'Data sources' which contains a button labeled 'Specify data source' (highlighted with a red rectangle). At the bottom of the form are 'Create' and 'Cancel' buttons. The left sidebar shows the 'Create agent' process with steps: 1. Basic information, 2. Add tool, 3. Setup agent endpoint, and 4. Review and create. The 'Add tool' step is currently selected.

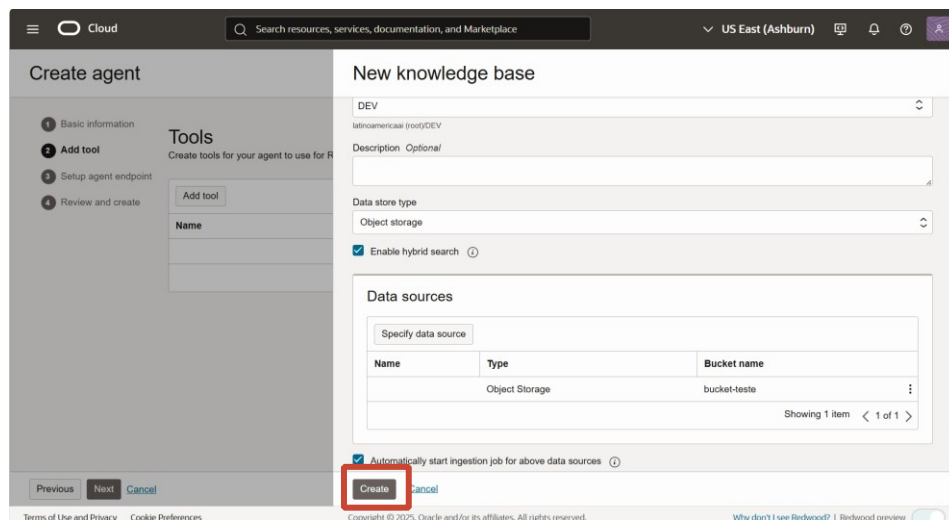
Nessa tela vamos apenas apontar para o bucket que criamos na sessão anterior. Clique em “Specify data source” e encontre seu bucket nas opções listadas. Lembre-se de estar na mesma região em que você criou o bucket, se não, ele não será listado.

The screenshot shows the 'Specify data source' form in the Oracle Cloud console. The form is titled 'Specify data source' and has a subtitle 'Information ingested into the knowledge base is securely stored and used as reference context when the Agent generates responses. The ingestion process does not attempt to identify, filter, or remove personal information from the input.' The form includes several fields: 'Name' (a text input field), 'Description' (a text input field with 'Optional' as a placeholder), and 'Enable multi-modal parsing' (an unchecked checkbox). Below these fields is a section titled 'Data bucket' which contains a dropdown menu (highlighted with a red rectangle) showing a list of buckets: 'Demo_Hap', 'Demo_JS', 'PoC_Aut', and 'PoC_Aut_Resultados'. At the bottom of the form are 'Create' and 'Cancel' buttons. The left sidebar shows the 'Create agent' process with steps: 1. Basic information, 2. Add tool, 3. Setup agent endpoint, and 4. Review and create. The 'Add tool' step is currently selected.

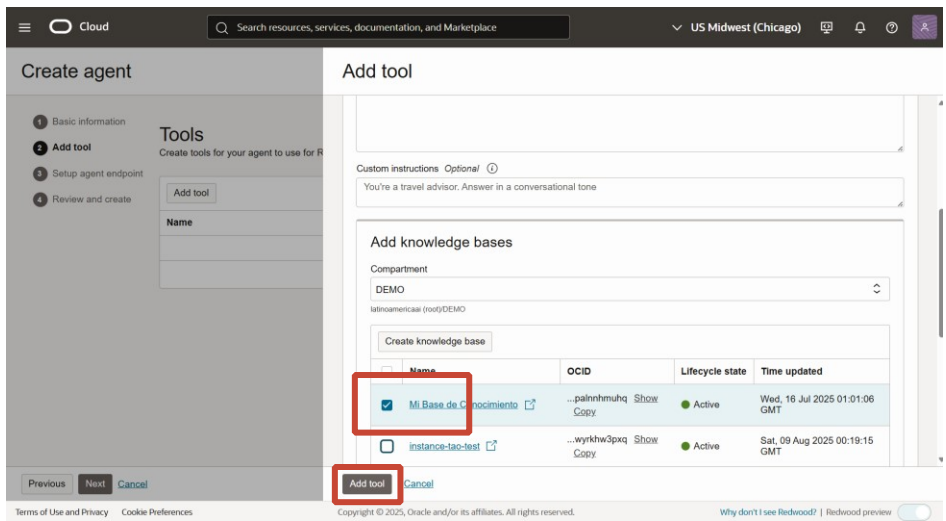
Selecione seu bucket e na mesma tela você vai ver todos os arquivos que estão presentes nele. Você deve ou marcar a opção de selecionar tudo que tem dentro do bucket, como o exemplo abaixo, ou selecionar apenas os arquivos que você deseja inserir na base do agente. Observe que ele aceita apenas PDF, TXT, HTML, JSON e MD, qualquer outro formato de arquivo, será ignorado.



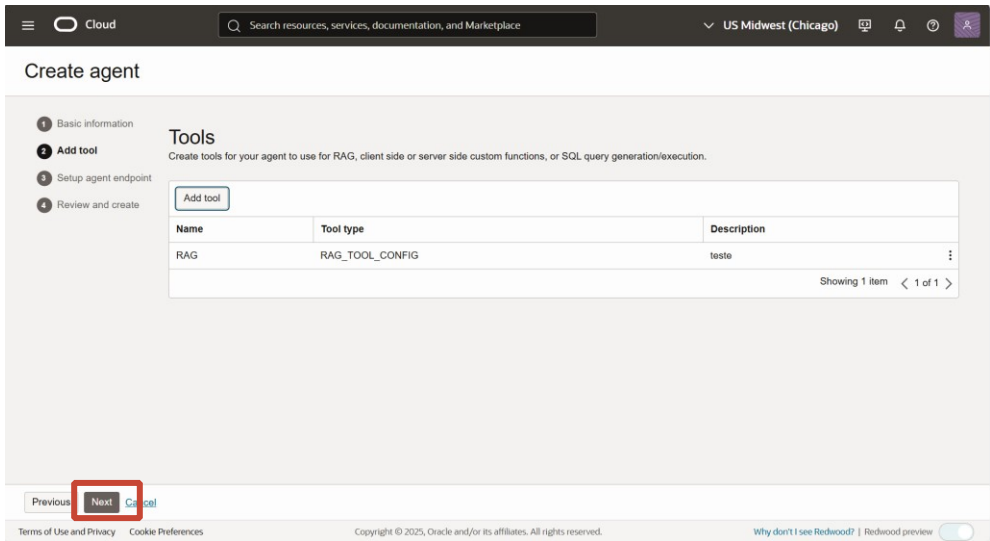
Uma vez que os arquivos estão selecionados, clique em “Create”.



Ele deve aparecer no seu data sources, clique em “Create” novamente. Não precisa alterar nada.



Selecione a sua base de conhecimento criada e clique em “Add tool”.



Nesse momento você terá sua ferramenta de base de conhecimento criada e conectada no bucket com seus PDFs. Podemos então avançar para o passo 3, clicando em “next”.

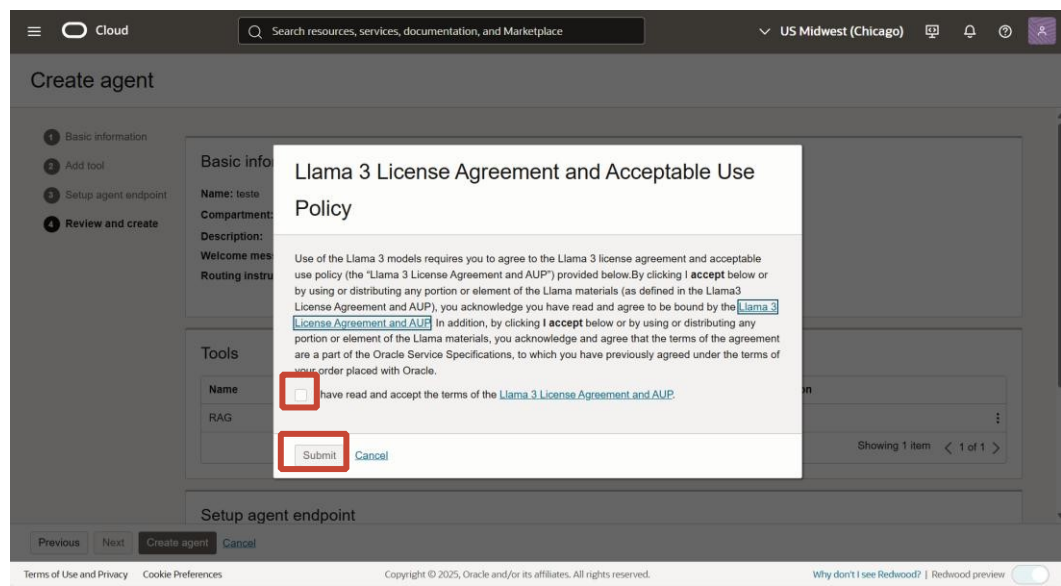
The screenshot shows the 'Create agent' wizard in the Oracle Cloud console, specifically the 'Setup agent endpoint' step. The left sidebar shows the progress: 1. Basic information, 2. Add tool, 3. Setup agent endpoint (current), and 4. Review and create. The main content area is titled 'Setup agent endpoint' and includes a checkbox for 'Automatically create an endpoint for this agent' which is checked. Below this is a section for 'Guardrails' with a 'Content moderation' subsection. At the bottom, there are three buttons: 'Previous', 'Next' (highlighted with a red box), and 'Cancel'.

O seguinte passo é para configuração do endpoint, automaticamente o serviço vai criar o agente e criar um endpoint para você interagir com esse agente. Esse endpoint pode ter algumas configurações de segurança que estão pré construídas na OCI, como é o exemplo dos Guardrails. Eles são superimportantes em casos reais, nesse passo a Oracle já oferece 3 guardrails pré configurados para você ativar, se quiser. Os guardrails são: Moderação de conteúdos violentos ou impróprios, detecção de tentativa de manipulação de prompt e identificação de compartilhamento de informações pessoais. Nesses três casos você tem a opção de escolher bloquear a ação ou apenas informar ao usuário.

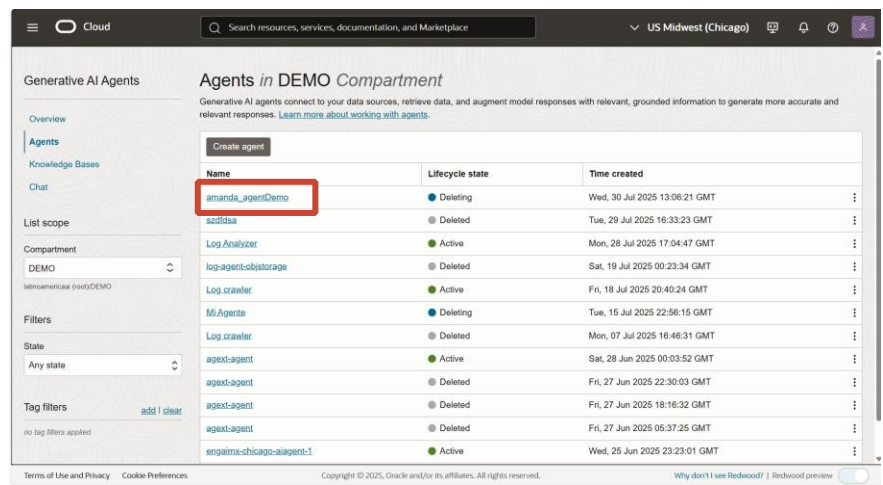
No nosso laboratório vamos deixar tudo no default, ou seja, desativado. Mas fique a vontade para testar novas possibilidades mais tarde. Seguindo para o último passo, vamos clicar em “Next” para chegar ao 4º passo.

The screenshot shows the 'Create agent' wizard in the Oracle Cloud console, specifically the 'Review and create' step. The left sidebar shows the progress: 1. Basic information, 2. Add tool, 3. Setup agent endpoint, and 4. Review and create (current). The main content area is titled 'Basic information' and shows fields for 'Name: teste', 'Compartment: ...j6k54yhka', 'Description:', 'Welcome message:', and 'Routing instructions:'. Below this is a 'Tools' section with a table showing one tool: 'RAG' with type 'RAG_TOOL_CONFIG' and description 'teste'. At the bottom, there are four buttons: 'Previous', 'Next', 'Create agent' (highlighted with a red box), and 'Cancel'.

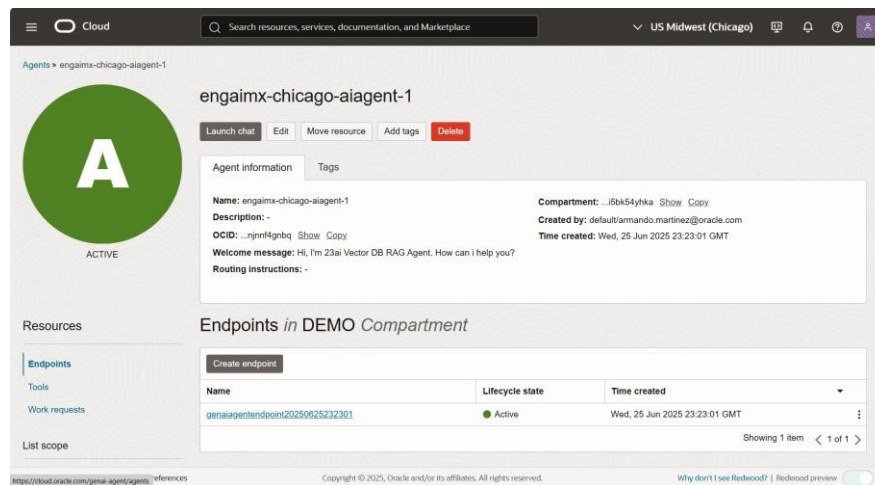
Essa etapa é apenas para conferência, você pode conferir as informações selecionadas e clicar em “Create agent” para concluir a criação do agente.



Quando você clicar em criar agente, uma licença do Llama irá surgir na sua tela, concorde e clique em “Submit”.



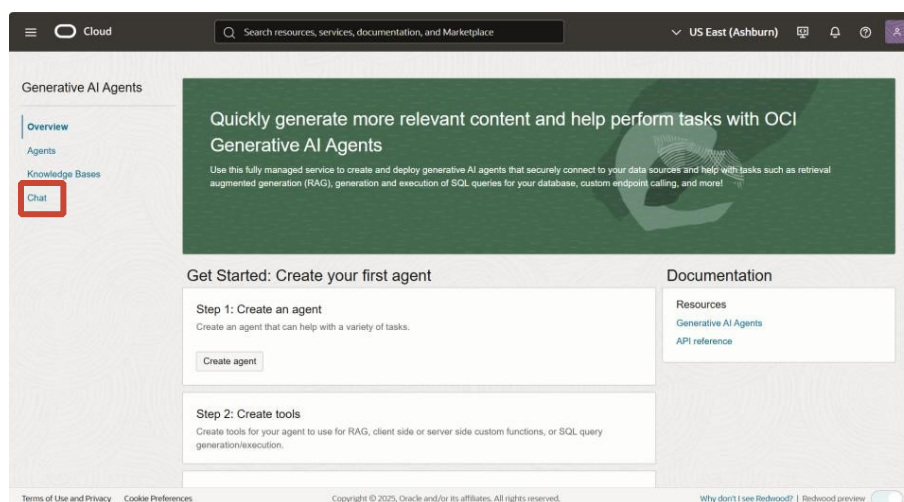
Seu agente deve aparecer com status de “Creating”. Aguarde até que ele fique ativo, isso deve demorar 7 minutos em média. Assim que ele estiver ativo, clique no nome do seu agente para abrir ele.



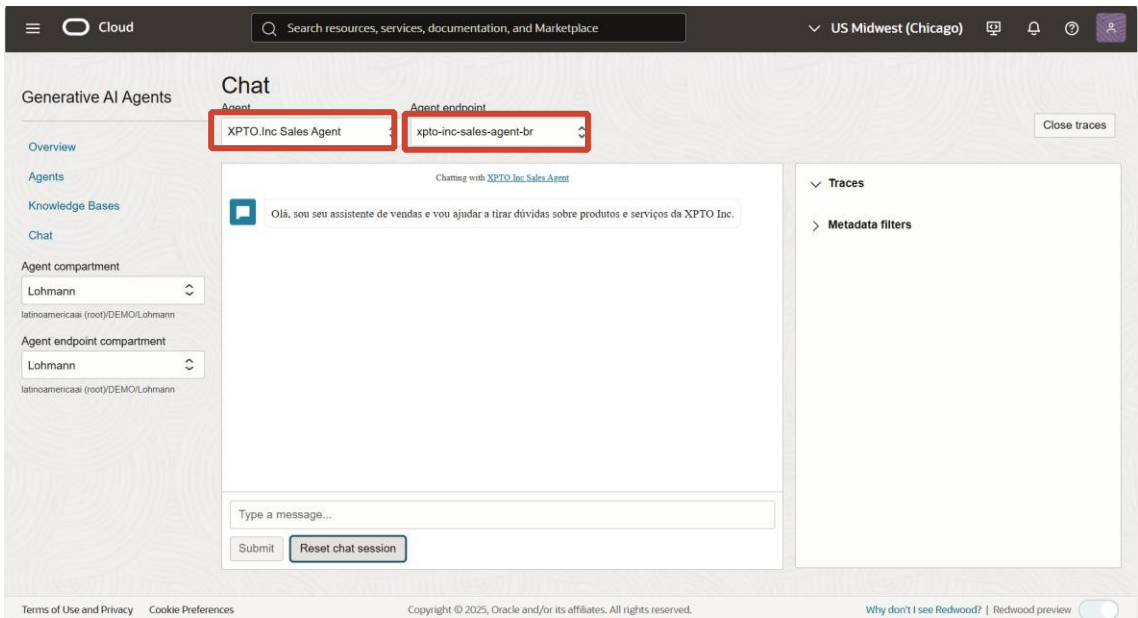
Nessa página você tem acesso ao endpoint, tools e todas as demais informações do seu agente. Se ele estiver ativo e obtiver um endpoint também ativo, o botão de “Launch chat” estará habilitado.

Interagindo com meu agente

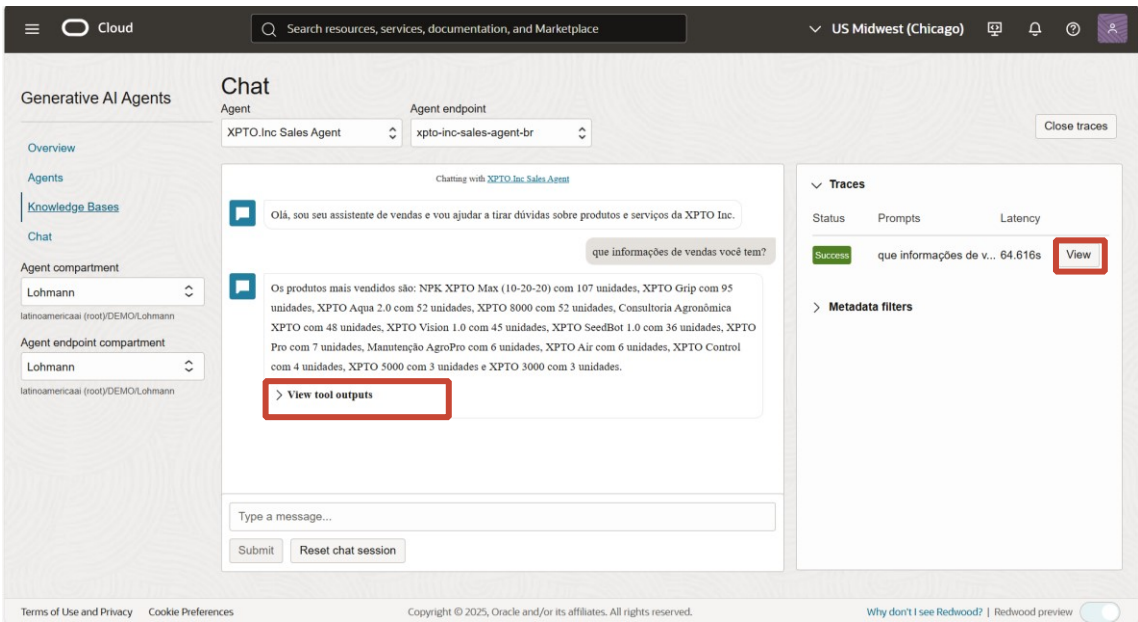
Uma vez que o agente está ativo e tem um endpoint ativo, você já pode se comunicar com ele. Uma das opções é abrir o agente, como na última imagem da sessão anterior, e clicar no botão launch chat. Ou, você pode na página inicial do serviço de Generative AI Agents e clicar no menu lateral esquerdo na parte de “chat”.



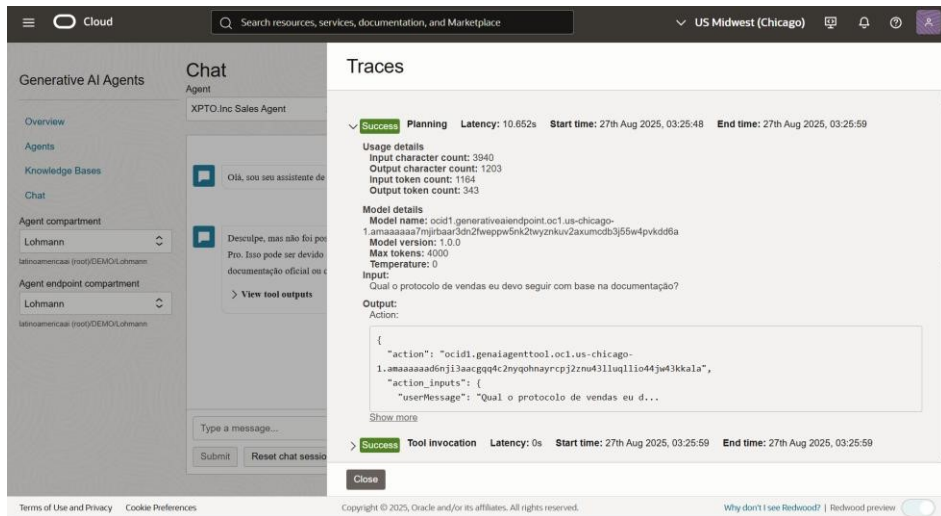
Na página de chat, você tem a opção de escolher algum dos agentes ativos no menu flutuante “Agent” e um endpoint no menu “Agent endpoint”. Caso você tenha acessado via “launch chat” essas informações já estarão todas preenchidas. Nessa tela é possível também notar que a mensagem de boas-vindas do agente imediatamente aparece na tela.



Quando você enviar uma pergunta para o agente, ele deve esperar e responder diretamente na tela. Seu agente vai, além de responder a sua pergunta, informar a citação de onde a informação veio, logo abaixo da resposta.



Outra habilidade interessante dessa tela é o “Traces”, clicando em “view” é possível ver a linha de pensamento, passo a passo que o agente seguiu para construir sua resposta. Todos os documentos, as páginas e demais ferramentas que ele usou para compor a resposta final e sua linha de raciocínio para atender a solicitação.

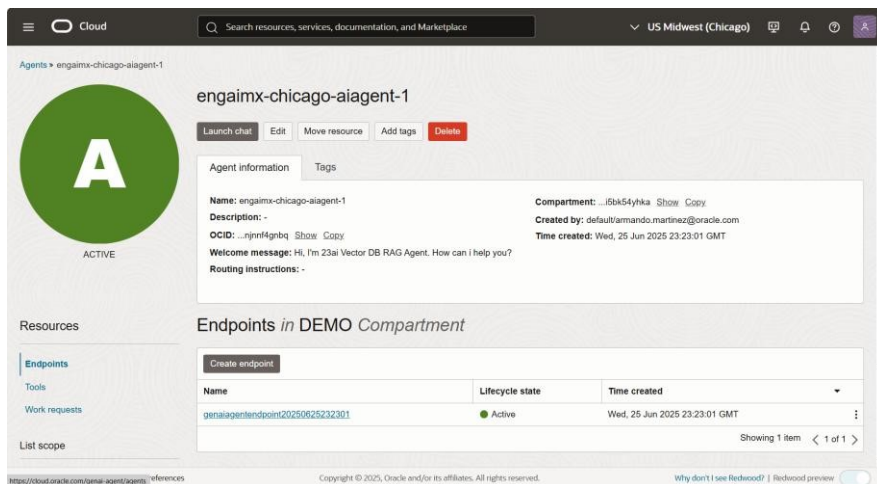


O traces é uma ferramenta poderosa para investigar o que o agente fez e conseguir ajustar prompt.

Ajustando o agente

Caso você não tenha obtido a resposta que gostaria com seu agente, você pode editar algumas partes dele. Na tela principal do agente, você pode editar o prompt tanto do agente quanto das tools. O prompt é a parte mais importante de qualquer aplicação de IA generativa, não subestime o poder de um prompt bem escrito.

Se seu problema for os arquivos, quando inseridos no bucket eles têm ingestão automática, então se seu ajuste é sobre adicionar documentação, você pode fazê-lo direto adicionando no bucket, deve demorar no máximo 2 minutos a ingestão da nova informação.



Você criou seu primeiro agente totalmente sem código com OCI.

Parabéns!