

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.

The screenshot shows the Oracle Cloud Home page. At the top, there's a search bar and a location dropdown set to 'Brazil East (Sao Paulo)'. Below the header, the 'Resources' section is visible, displaying a table of recently viewed resources. The table has columns for Name, Type, Status, and Viewed. Three resources are listed: 'agente_passeios_dail25_v2' (GenAIAgent, Active, 3 hours ago), 'test-claro' (GenAIAgent, Active, 3 days ago), and 'knowledge_Demo' (GenAIAgentDataSource, Active, 3 days ago). At the bottom of the table, it says '3 results shown.' A 'Resource Explorer' button is located at the bottom left of the table area.

No menu lateral esquerdo, mais conhecido como menu de “hamburguer”, 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.

The screenshot shows the Oracle Cloud Storage service page. The left sidebar has a 'Storage' item highlighted with a red box. The main content area is divided into three sections: 'Block Storage' (Block Volumes, Block Volume Backups, Block Volume Replicas, Volume Groups, Volume Group Backups, Volume Group Replicas, Backup Policies), 'File Storage' (File Systems, Mount Targets), and 'Object Storage & Archive Storage' (Buckets, Private Endpoints). The 'Buckets' item under Object Storage is also highlighted with a red box. The bottom of the page includes a 'Build' section and a 'Service spotlight' section.

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

The screenshot shows the Oracle Cloud Object Storage Buckets page. At the top, there's a search bar and a compartment dropdown set to "US East (Ashburn)". Below the header, a table lists six buckets:

Name	Default storage tier	Visibility	Time created
Demo_Hap	Standard	Private	Aug 8, 2025, 17:12 UTC
Demo_JS	Standard	Private	Jul 28, 2025, 19:58 UTC
dev_bucket	Standard	Private	Jul 17, 2025, 04:34 UTC
PoC_Aut	Standard	Private	Aug 20, 2025, 13:50 UTC
PoC_Aut_Resultados	Standard	Private	Aug 22, 2025, 14:44 UTC
PoC_Renova	Standard	Private	Aug 21, 2025, 19:47 UTC

At the bottom of the table, it says "Page 1 of 1 (1 - 6 of 6 total items)". There are also links for "Terms of Use and Privacy" and "Cookie Preferences". On the right, there are buttons for "Items per page" (set to 100) and "Give us feedback | Redwood preview".

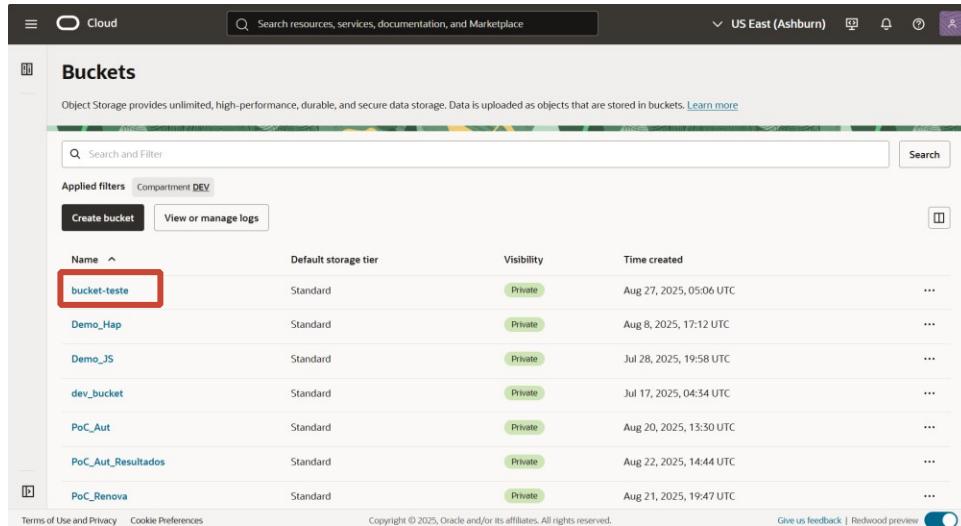
Vamos clicar em “create bucket”.

The screenshot shows the Oracle Cloud Create bucket page. At the top, there's a search bar and a compartment dropdown set to "US East (Ashburn)". The main area is titled "Create bucket" and contains a form with the following fields:

- Bucket name:** A text input field containing "bucket-20250827-0205" with a red box highlighting it.
- Default storage tier:** A section explaining the default storage tier can only be specified during creation. It includes a link "Learn more about storage tiers".
 - Standard
 - Archive
- Enable auto-tiering:** A toggle switch that is off.
- Enable object versioning:** A toggle switch that is off.
- Emit object events:** A toggle switch that is off.

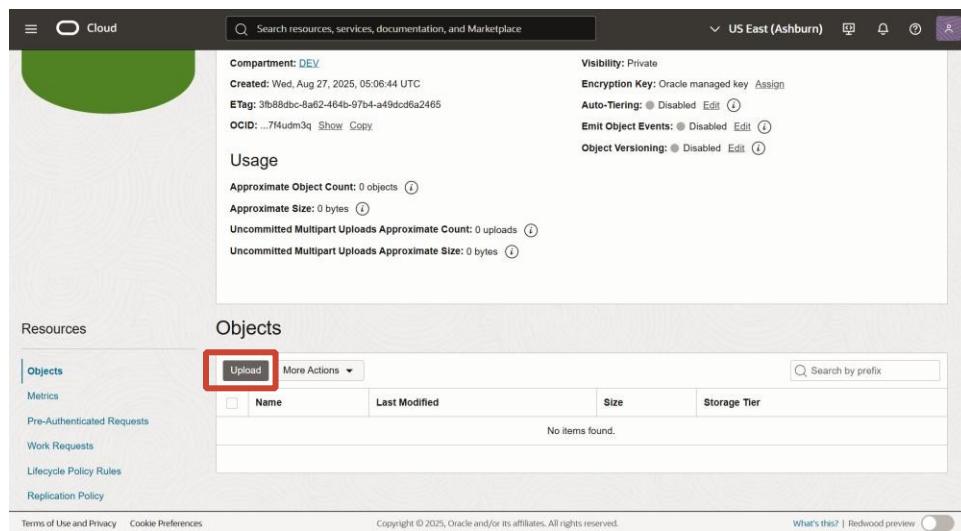
At the bottom right, there are "Cancel" and "Create bucket" buttons, with the "Create bucket" button highlighted by a red box.

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



The screenshot shows the Oracle Cloud Buckets page. At the top, there's a search bar and a compartment dropdown set to "US East (Ashburn)". Below the header, a section titled "Buckets" displays a list of buckets. The first item, "bucket-teste", is highlighted with a red box. Other buckets listed include "Demo_Hap", "Demo_JS", "dev_bucket", "PoC_Aut", "PoC_Aut_Resultados", and "PoC_Renova". Each bucket entry includes columns for Name, Default storage tier, Visibility, and Time created. A "Create bucket" button is visible at the top left of the list area.

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



The screenshot shows the details page for the "bucket-teste" bucket. At the top, it displays basic information: Compartment: DEV, Created: Wed, Aug 27, 2025, 05:06:44 UTC, ETag: 3fb88dbc-8a62-464b-97b4-a49dd6a2465, and OCID: ...764udm3q. It also shows Usage statistics: Approximate Object Count: 0 objects, Approximate Size: 0 bytes, Uncommitted Multipart Uploads Approximate Count: 0 uploads, and Uncommitted Multipart Uploads Approximate Size: 0 bytes. On the right side, there are settings for Visibility (Private), Encryption Key (Oracle managed key), Auto-Tiering (disabled), Emit Object Events (disabled), and Object Versioning (disabled). Below this, the "Objects" tab is selected in the navigation bar, and the "Upload" button is highlighted with a red box. The main content area shows a table with columns for Name, Last Modified, Size, and Storage Tier, with a message indicating "No items found."

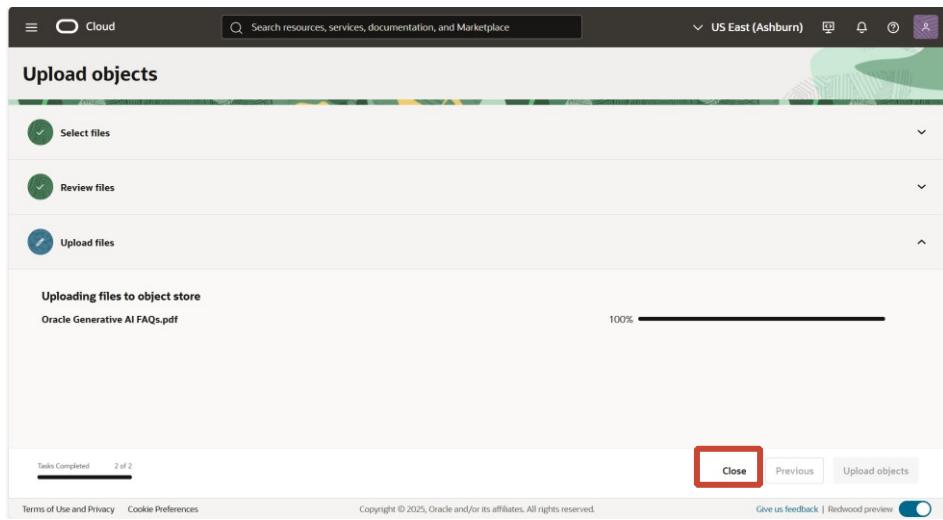
Dentro do bucket, você deve encontrar um botão mais para baixo da tela com a opção de fazer upload. Você pode estar com essa versão de cima, ou a de baixo. São versões de interface da OCI, a versão acima é antiga e a versão da imagem abaixo é a nova versão. De todo modo você vai encontrar facilmente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

Screenshot of the Oracle Cloud Infrastructure Bucket Details page for 'bucket-teste'. The 'Actions' dropdown menu is open, and the 'Upload objects' button is highlighted with a red box. The page shows various bucket details like Namespace, Compartment, and Storage tier.

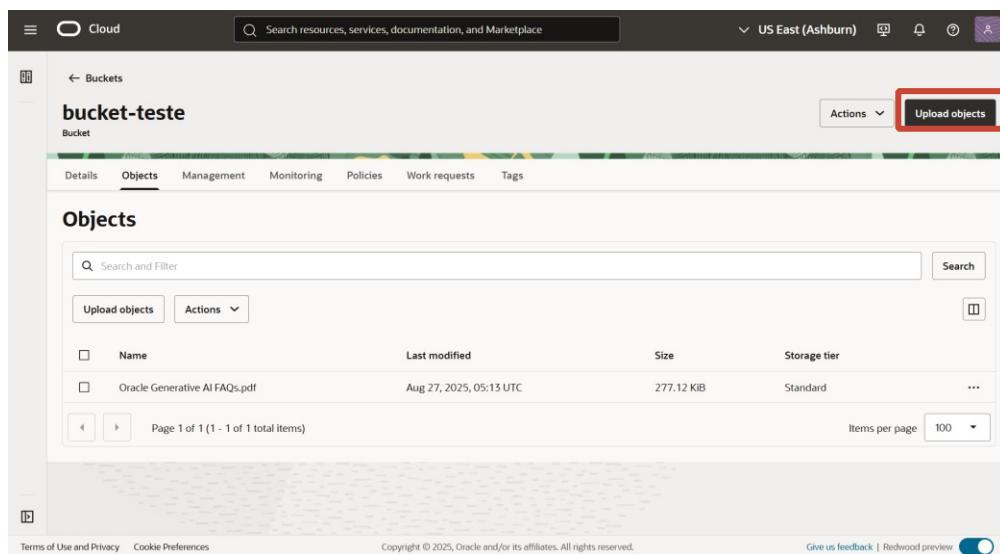
Você não precisa modificar nada nessa tela, apenas adicionar os arquivos via “Drag and drop” e clicar em next para seguir com a adição.

Screenshot of the Oracle Cloud Infrastructure 'Upload objects' wizard, Step 1: Select files. The 'Next' button at the bottom right is highlighted with a red box. The form includes fields for Object name prefix, Storage tier, Additional checksum, and a file upload area.

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.

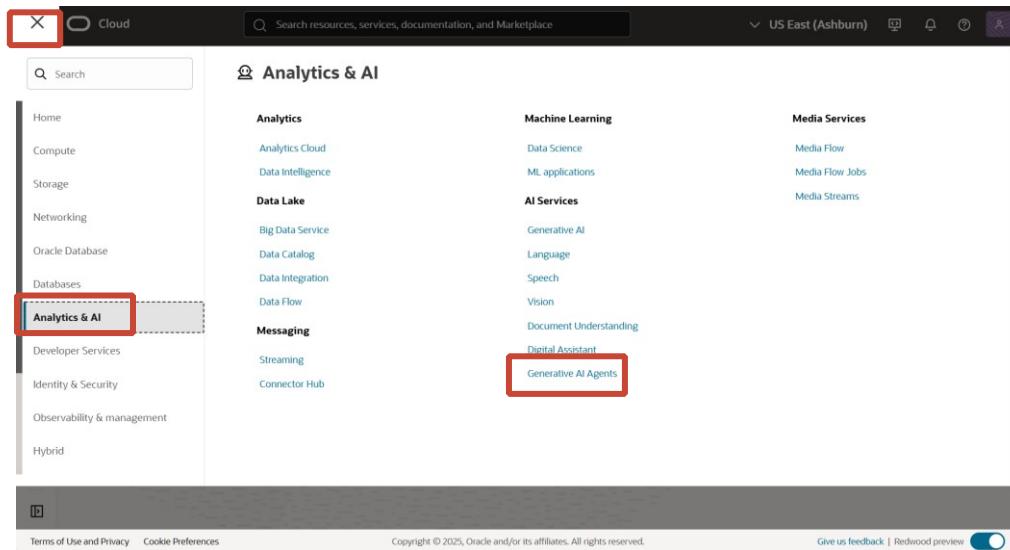


Verifique os documentos adicionados acessando “objects” dentro do bucket.

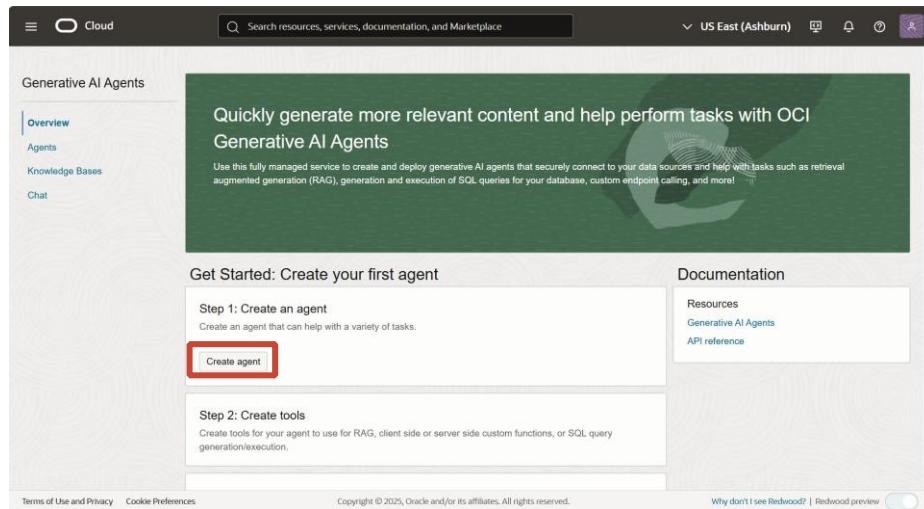


Criando o agente

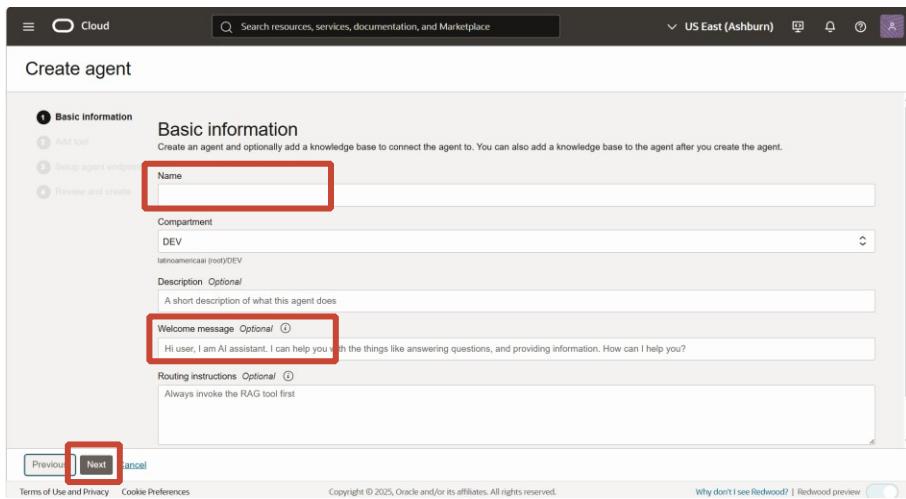
Agora que você já tem os documentos que seu agente vai utilizar como base de conhecimento, vamos começar a criação do agente utilizando o serviço de Agents OCI da Oracle. Para isso, retorne ao menu de hamburguer e selecione o menu de “Analytics & AI”, buscando a opção de “Generative AI Agents”.



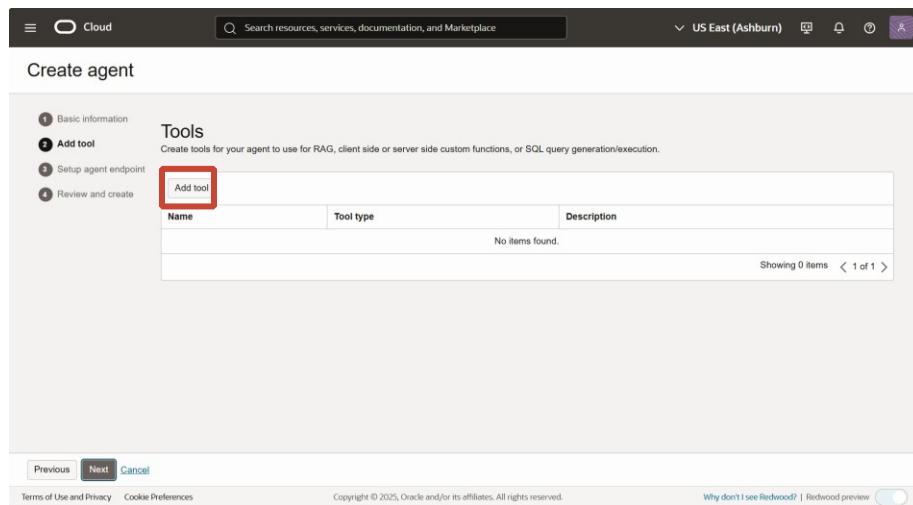
A tela que aparece é a interface do serviço de agentes. Na página de overview é possível ver os passos simples da criação de um agente. No menu lateral esquerdo também existe a aba “Agents” que lista todos os agentes criados, “Knowledge Base” que lista as bases de conhecimento desenvolvidas, ativas ou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



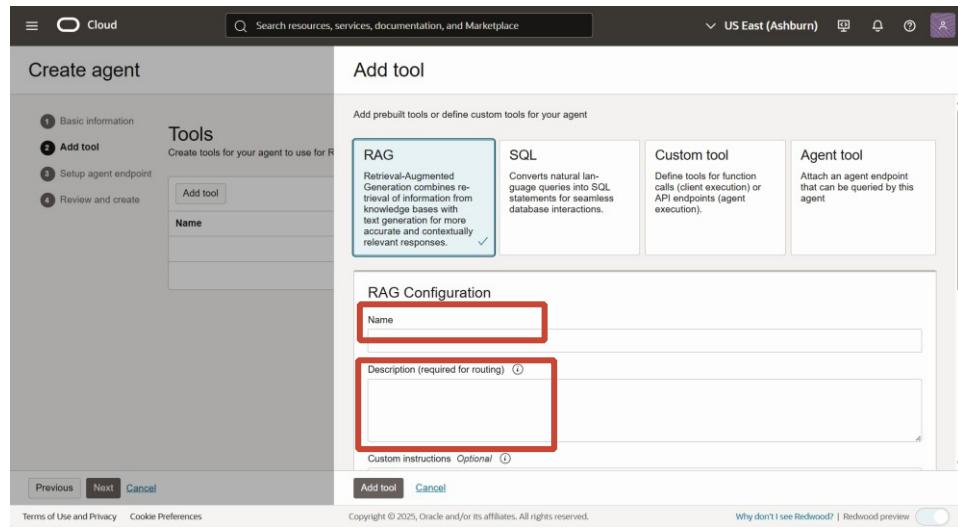
Vamos clicar em “create agent” no centro da tela para começar a criação do nosso agente.



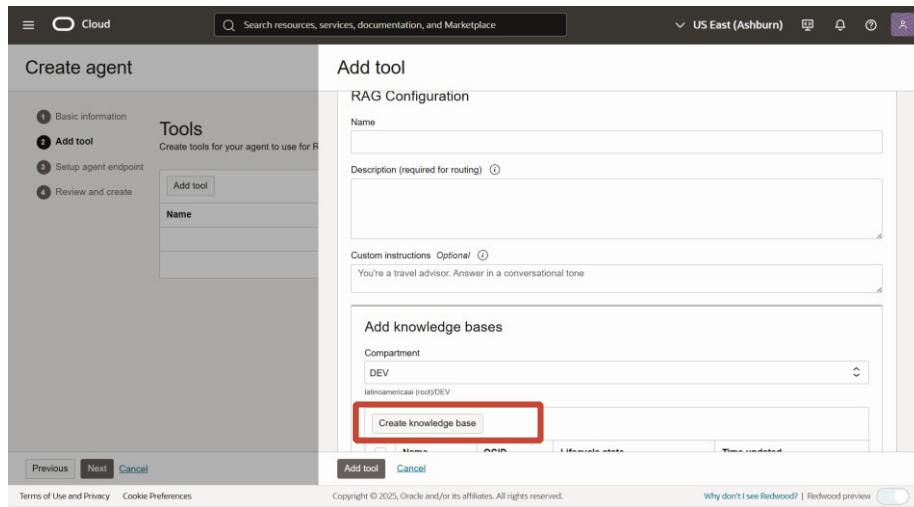
O primeiro passo é composto por informações básicas do agente. É obrigatório adicionar um nome para seu agente. Você também pode adicionar uma mensagem inicial dele no “Welcome message”, uma saudação para seu usuário. Uma descrição interna, para identificar do que se trata esse agente e rotas de instrução, 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”.



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”.

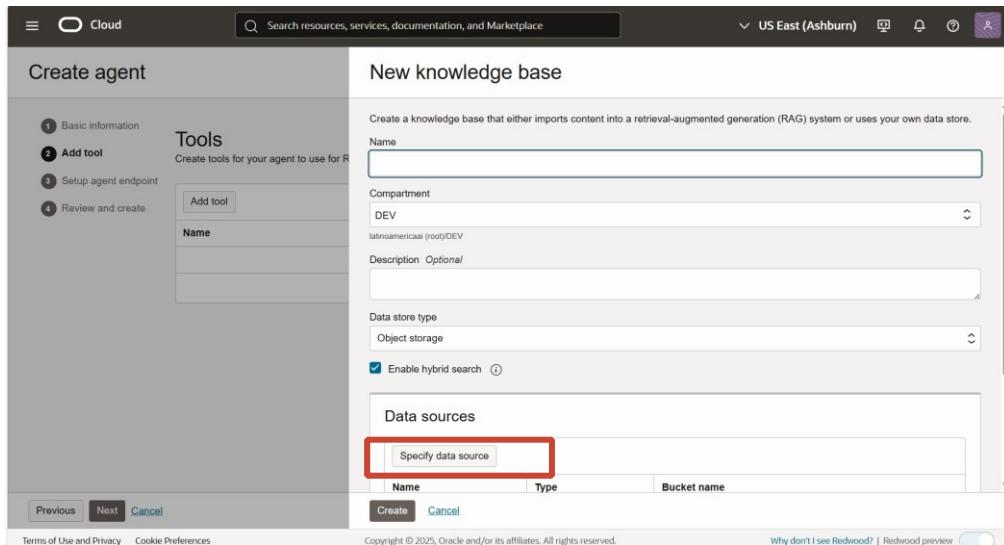


Existem várias ferramentas pré construídas. RAG para processar informações não estruturadas, como textos. SQL para informações estruturadas, como bancos de dados transacionais. Custom tool para funções ou endpoints de serviços. E finalmente Agent tool para adicionar uma camada multi agêntica, permitindo 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.

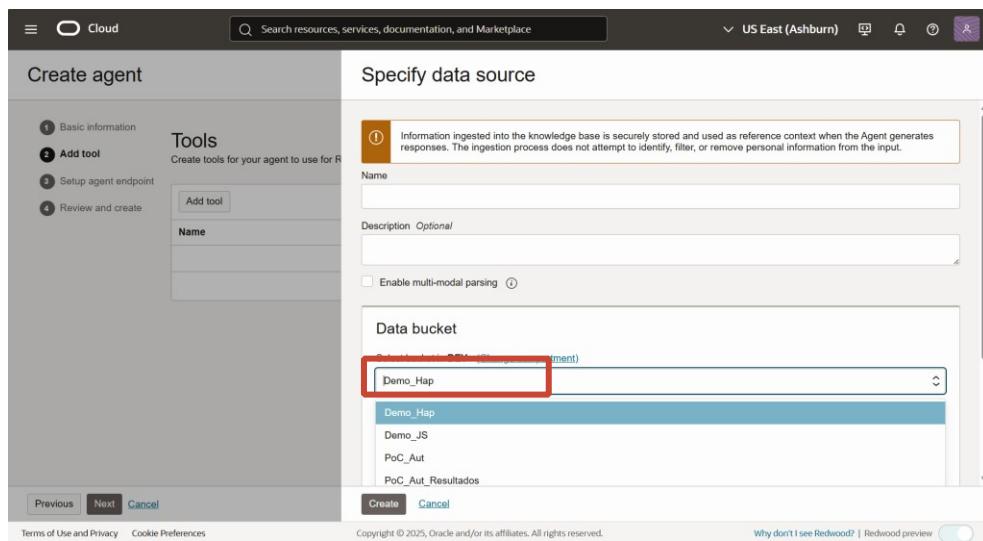


Descendo a tela na opção RAG, vamos precisar preencher um nome no campo “Name” e um prompt descritivo no campo “Description”. Esse prompt é exatamente as instruções que o agente vai utilizar para montar as repostas para o usuário final sobre a sua base de conhecimento então coloque um prompt bem descrito.

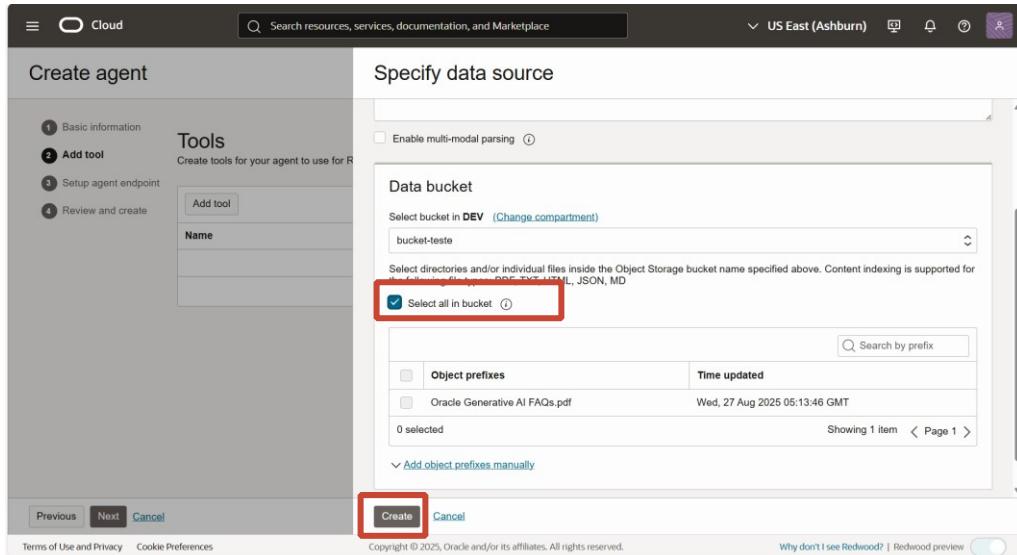
Uma vez preenchido, vamos criar uma base de conhecimento, clicando no botão “Create knowledge base”.



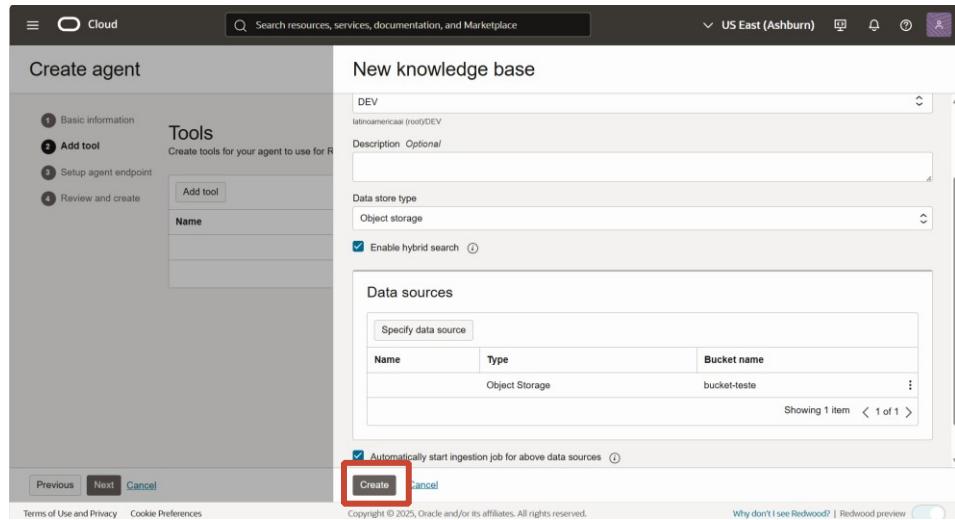
Nessa tela vamos apenas apontar para o bucket que criamos na sessão anterior. Clique em “Specify data source” e encontre seu bucket nas opções listadas. Lembre-se de estar na mesma região em que você criou o bucket, se não, ele não será listado.



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.

The screenshot shows the 'Add tool' step of a 'Create agent' wizard. On the left, a sidebar lists steps: 1. Basic information, 2. Add tool (which is selected and highlighted in blue), 3. Setup agent endpoint, and 4. Review and create. The main area is titled 'Tools' with the sub-instruction 'Create tools for your agent to use for RAG, client side or server side custom functions, or SQL query generation/execution.' A table titled 'Create knowledge base' lists two entries:

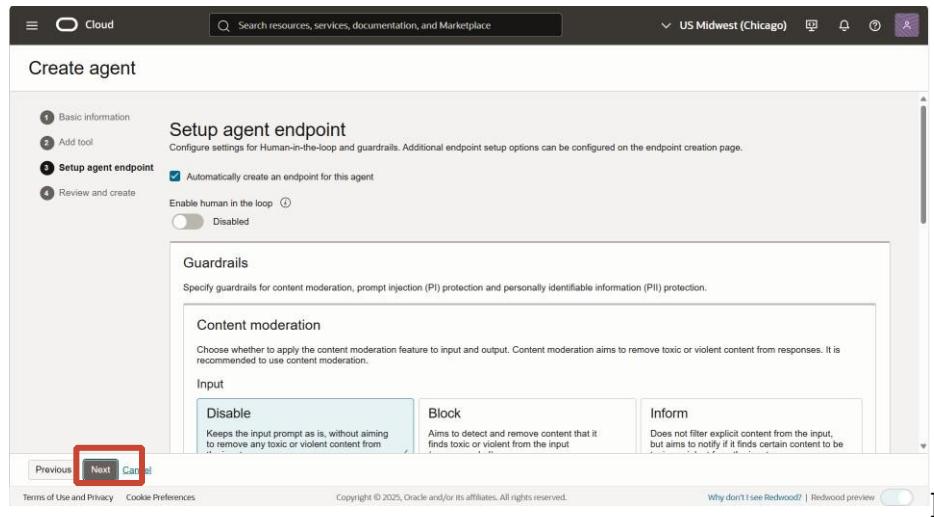
Name	OCID	Lifecycle state	Time updated
...painnhmuq	Show Copy	Active	Wed, 16 Jul 2025 01:01:06
...wyrikhw3pxq	Show Copy	Active	Sat, 09 Aug 2025 00:19:15

The first entry, '...painnhmuq', has a checked checkbox next to it. The 'Add tool' button at the bottom of the table is highlighted with a red box. At the very bottom of the page, the 'Add tool' button is also highlighted with a red box.

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

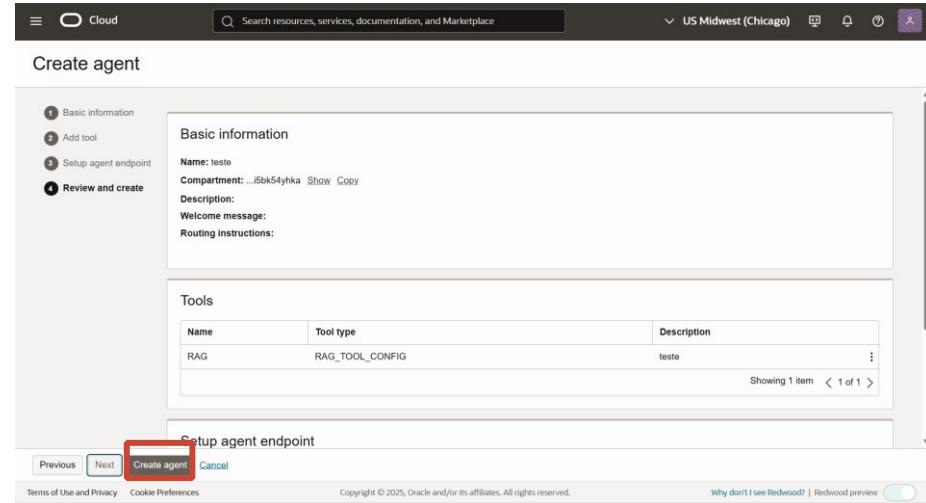
This screenshot shows the final step of the 'Create agent' wizard, labeled 'Review and create'. The 'Tools' section is visible, showing the previously selected knowledge base '...painnhmuq' and the 'RAG' tool entry. The 'Add tool' button at the bottom of the table is highlighted with a red box. The 'Next' button at the bottom of the page is also highlighted with a red box.

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”.

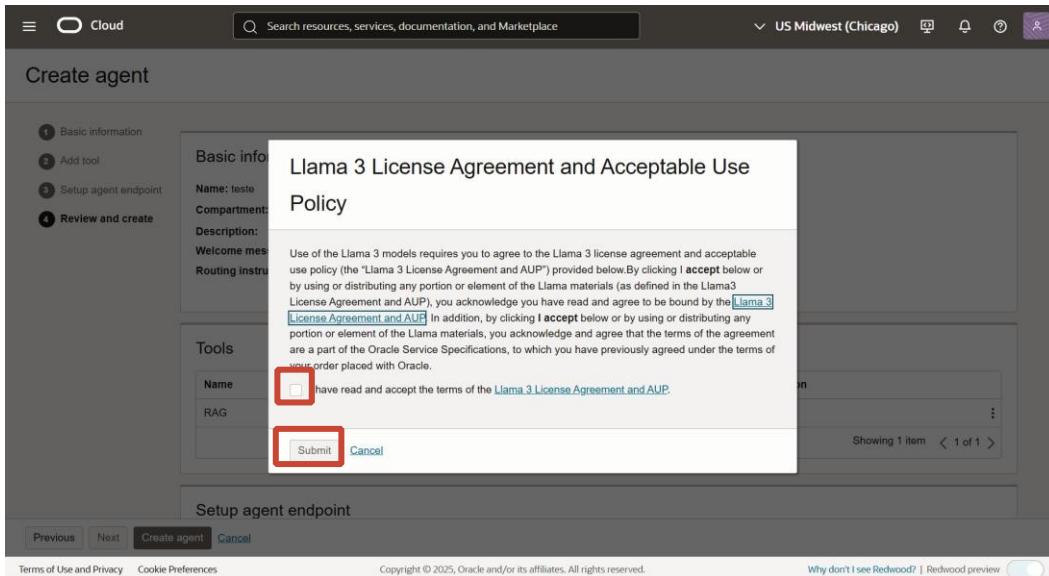


O seguinte passo é para configuração do endpoint, automaticamente o serviço vai criar o agente e criar um endpoint para você interagir com esse agente. Esse endpoint pode ter algumas configurações de segurança que estão pré construídas na OCI, como é o exemplo dos Guardrails. Eles são superimportantes 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.



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”.

Name	Lifecycle state	Time created
amanda_agentDemo	● Deleting	Wed, 30 Jul 2025 13:06:21 GMT
szldsa	● Deleted	Tue, 29 Jul 2025 16:33:23 GMT
Log Analyzer	● Active	Mon, 28 Jul 2025 17:40:47 GMT
log-agent:objstorage	● Deleted	Sat, 19 Jul 2025 00:23:34 GMT
Log crawler	● Active	Fri, 18 Jul 2025 20:40:24 GMT
Mi.Agente	● Deleting	Tue, 15 Jul 2025 22:56:15 GMT
Log crawler	● Deleted	Mon, 07 Jul 2025 16:48:31 GMT
agext:agent	● Active	Sat, 28 Jun 2025 00:03:52 GMT
agext:agent	● Deleted	Fri, 27 Jun 2025 22:30:03 GMT
agext:agent	● Deleted	Fri, 27 Jun 2025 18:16:32 GMT
agext:agent	● Deleted	Fri, 27 Jun 2025 05:37:25 GMT
engaimx-chicago-agagent:1	● Active	Wed, 25 Jun 2025 23:23:01 GMT

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.

The screenshot shows the Oracle Cloud interface for managing agents. The top navigation bar includes 'Cloud', a search bar, and location 'US Midwest (Chicago)'. The main content area is titled 'engaimx-chicago-aiagent-1'. On the left, there's a large green circular icon with a white letter 'A' and the word 'ACTIVE' below it. To the right of the icon, there are buttons for 'Launch chat', 'Edit', 'Move resource', 'Add tags', and 'Delete'. A section titled 'Agent information' displays details: Name: engaimx-chicago-aiagent-1, Description: -, OCID: ..., and a Welcome message: 'Hi, I'm 23ai Vector DB RAG Agent. How can i help you?'. Below this is a 'Resources' sidebar with 'Endpoints' selected, showing 'Tools' and 'Work requests' options. The main pane is titled 'Endpoints in DEMO Compartiment' and lists one item: 'genaiagentendpoint20250625232301' with a Lifecycle state of 'Active' and a Time created of 'Wed, 25 Jun 2025 23:23:01 GMT'. At the bottom, there's a copyright notice and a link to 'Redwood preview'.

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”.

The screenshot shows the Oracle Cloud Generative AI Agents service. The top navigation bar includes 'Cloud', a search bar, and location 'US East (Ashburn)'. The main content area is titled 'Generative AI Agents'. On the left, there's a sidebar with 'Overview' (selected), 'Agents', 'Knowledge Bases', and 'Chat' (highlighted with a red box). The main pane features a green banner with the text 'Quickly generate more relevant content and help perform tasks with OCI Generative AI Agents'. Below the banner, there are two main sections: 'Get Started: Create your first agent' and 'Step 2: Create tools'. The 'Get Started' section has a 'Create agent' button. The 'Step 2' section has a 'Create tools' button. At the bottom, there's a 'Documentation' sidebar with links to 'Resources' (Generative AI Agents) and 'API reference'. At the very bottom, there are 'Terms of Use and Privacy' and 'Cookie Preferences' links, along with a 'Copyright © 2025, Oracle and/or its affiliates. All rights reserved.' notice and a 'Redwood preview' toggle.

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.

The screenshot shows the Oracle Cloud Generative AI Agents Chat interface. On the left, there's a sidebar with options like Overview, Agents, Knowledge Bases, and Chat. Under Chat, Agent compartment and Agent endpoint compartment dropdowns are set to 'Lohmann'. The main area is titled 'Chat' and shows a message from 'XPTO.Inc Sales Agent': 'Olá, sou seu assistente de vendas e vou ajudar a tirar dúvidas sobre produtos e serviços da XPTO Inc.' Below this is a text input field with placeholder 'Type a message...', a 'Submit' button, and a 'Reset chat session' button. To the right, there's a 'Traces' section with a 'Metadata filters' dropdown. At the bottom, there are links for 'Terms of Use and Privacy' and 'Cookie Preferences', and a note about Redwood preview.

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.

This screenshot shows the same Oracle Cloud Generative AI Agents Chat interface after a question has been asked. The 'Knowledge Bases' option in the sidebar is now selected. The main chat area shows a message from 'XPTO.Inc Sales Agent': 'Olá, sou seu assistente de vendas e vou ajudar a tirar dúvidas sobre produtos e serviços da XPTO Inc.' followed by another message: 'Os produtos mais vendidos são: NPK XPTO Max (10-20-20) com 107 unidades, XPTO Grip com 95 unidades, XPTO Aqua 2.0 com 52 unidades, XPTO 8000 com 52 unidades, Consultoria Agronômica XPTO com 48 unidades, XPTO Vision 1.0 com 45 unidades, XPTO SeedBot 1.0 com 36 unidades, XPTO Pro com 7 unidades, Manutenção AgroPro com 6 unidades, XPTO Air com 6 unidades, XPTO Control com 4 unidades, XPTO 5000 com 3 unidades e XPTO 3000 com 3 unidades.' Below this message is a red box around the link '> View tool outputs'. The 'Traces' section on the right shows a success status with the message 'que informações de v... 64.616s' and a 'View' button, which is also highlighted with a red box.

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.

The screenshot shows the Oracle Cloud Generative AI Agents interface. On the left, there's a sidebar with 'Generative AI Agents' and 'Agents'. Under 'Agents', it lists 'XPTO Inc Sales Agent' and 'Lohmann'. The main area is titled 'Chat Agent' with a sub-section 'XPTO Inc Sales Agent'. It shows a conversation history with messages from the agent and the user. Below the conversation is a text input field 'Type a message...' and buttons 'Submit' and 'Reset chat session'. To the right, a large panel is titled 'Traces'. It displays two entries: one for a 'Success' event with a latency of 10.652s, and another for a 'Tool invocation' with a latency of 0s. Each entry includes details like usage statistics, model information, and the raw JSON response sent to the agent. At the bottom of the traces panel, there are buttons for 'Close' and 'Show more'.

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.

The screenshot shows the Oracle Cloud Agents interface. On the left, it lists 'Agents' and 'engaimx-chicago-aiagent-1'. The main area shows a circular icon with a large letter 'A' and the word 'ACTIVE'. Below it are tabs for 'Agent information' and 'Tags'. Under 'Agent information', there are fields for 'Name' (engaimx-chicago-aiagent-1), 'Description' (empty), 'OCID' (...nprn4grnbq), 'Compartiment' (...j6ba54yhka), 'Created by' (default/armando.martinez@oracle.com), and 'Time created' (Wed, 25 Jun 2025 23:23:01 GMT). A 'Welcome message' is also present. On the right, there's a table for 'Endpoints in DEMO Compartiment' with one item: 'geniaagentendpoint20250625232301' (Active, Wed, 25 Jun 2025 23:23:01 GMT). At the bottom, there are buttons for 'Launch chat', 'Edit', 'Move resource', 'Add tags', and 'Delete'. The footer includes links for 'References' and 'Copyright © 2025, Oracle and/or its affiliates. All rights reserved.'.

Você criou seu primeiro agente totalmente sem código com OCI.

Parabéns!