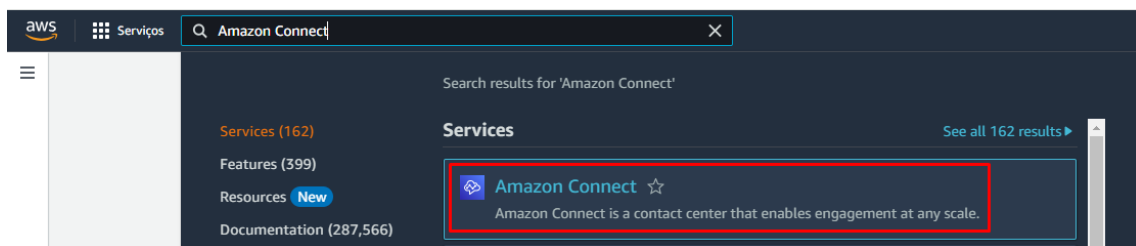




1. Faça login no Console de Gerenciamento da AWS

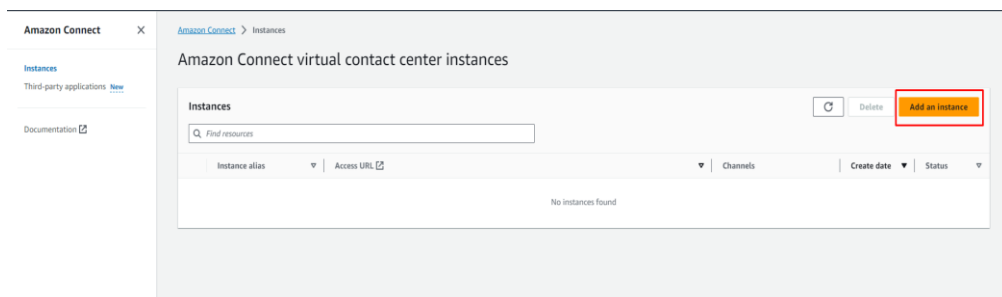
(<https://console.aws.amazon.com/console>) usando sua conta AWS na região da Virgínia.

2.No AWS Management Console, na parte superior da página pesquise por Amazon Connect



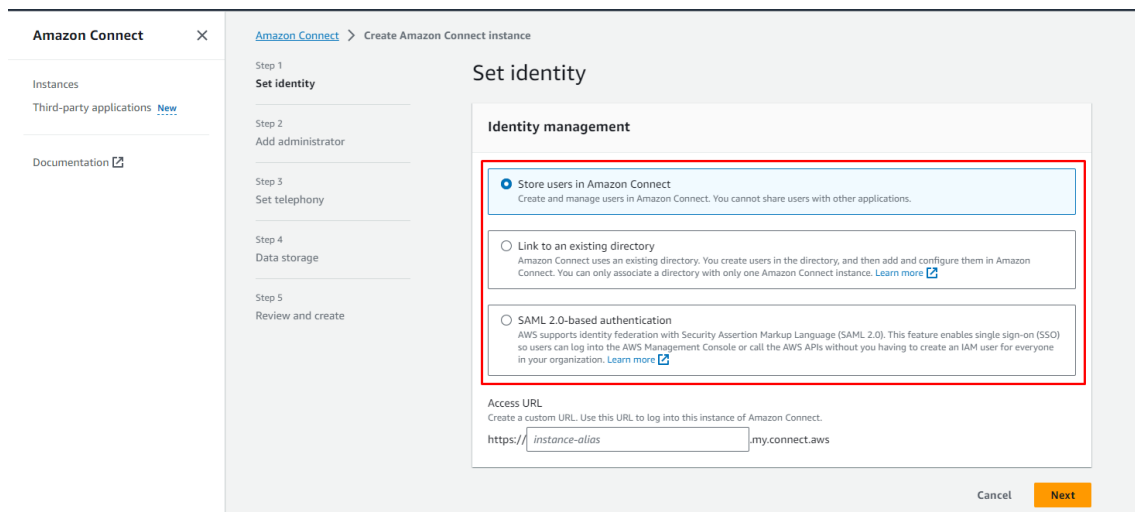
3. Escolha "Amazon Connect".

4.Na página do Amazon Connect, escolha "Adicionar uma instância".



## 5. Configuração de identidade de acesso ao Amazon Connect e URL de acesso

Ao criar uma instância, é necessário decidir como deseja gerenciar os usuários, pois não é possível alterar a opção de gerenciamento de identidade depois de criar a instância. Você pode escolher uma das seguintes soluções de gerenciamento de identidade:



The screenshot shows the 'Set identity' step in the Amazon Connect console. The left sidebar contains navigation links for 'Instances', 'Third-party applications', and 'Documentation'. The main content area is titled 'Set identity' and includes a progress bar with steps: 'Set identity', 'Add administrator', 'Set telephony', 'Data storage', and 'Review and create'. The 'Identity management' section has three radio button options: 'Store users in Amazon Connect' (selected), 'Link to an existing directory', and 'SAML 2.0-based authentication'. Below these options is an 'Access URL' section with a text input field for 'instance-alias' and a 'Next' button.

### Armazenar usuários com o Amazon Connect:

- Permite a criação e gerenciamento direto de contas de usuário no Amazon Connect.
- Cada usuário possui um nome de usuário e senha específicos para acesso ao Amazon Connect.

### Vincular a um diretório existente:

- Oferece a opção de usar um Active Directory já existente para autenticação.
- Os usuários realizam login no Amazon Connect usando suas credenciais corporativas.
- Exige que o diretório esteja associado à sua conta, configurado no AWS Directory Service e ativo na mesma região da instância do Amazon Connect.

### Autenticação baseada em SAML 2.0

- Facilita a federação de usuários com o Amazon Connect por meio de um provedor de identidade de rede existente.
- Os usuários só podem acessar o Amazon Connect através de um link configurado pelo provedor de identidade.
- É necessário configurar previamente o ambiente para SAML antes de criar a instância do Amazon Connect.

## 6. Neste tutorial, iremos utilizar armazenamento de usuários no Amazon Connect

The screenshot shows the 'Set identity' step in the Amazon Connect console. The left sidebar lists the steps: Step 1 (Set identity), Step 2 (Add administrator), Step 3 (Set telephony), Step 4 (Data storage), and Step 5 (Review and create). The main content area is titled 'Set identity' and contains three radio button options under 'Identity management':

- ☒ **Store users in Amazon Connect**  
Create and manage users in Amazon Connect. You cannot share users with other applications.
- ☐ **Link to an existing directory**  
Amazon Connect uses an existing directory. You create users in the directory, and then add and configure them in Amazon Connect. You can only associate a directory with only one Amazon Connect instance. [Learn more](#)
- ☐ **SAML 2.0-based authentication**  
AWS supports identity federation with Security Assertion Markup Language (SAML 2.0). This feature enables single sign-on (SSO) so users can log into the AWS Management Console or call the AWS APIs without you having to create an IAM user for everyone in your organization. [Learn more](#)

Below the options is the 'Access URL' section, which says: 'Create a custom URL. Use this URL to log into this instance of Amazon Connect.' The URL is shown as 'https://[instance-alias].my.connect.aws'. At the bottom right are 'Cancel' and 'Next' buttons.

## 7. O próximo passo é escolher uma URL de acesso, que deve ser um nome exclusivo.

This screenshot is similar to the previous one, showing the 'Set identity' step. The 'Store users in Amazon Connect' option is selected. The 'Access URL' section is highlighted with a red box, showing the text: 'Create a custom URL. Use this URL to log into this instance of Amazon Connect.' The URL field is currently empty, with a red box around it, indicating where the user should enter a custom URL. The 'Next' button is visible at the bottom right.

## 8. Após escolher URL de clique em Next

9. Na tela Data storage, iremos adicionar um usuário administrador ao Amazon Connect para garantir um acesso inicial seguro e em conformidade com as melhores práticas.

Embora a opção de utilizar o acesso IAM seja possível em emergências, essa prática não é aconselhável para uso regular devido a questões de segurança.

Para seguir as boas práticas de administração, optaremos por adicionar um usuário administrador.

The screenshot shows the 'Add administrator' step of the 'Create Amazon Connect instance' wizard. On the left, a sidebar contains 'Amazon Connect' with a close button, and a list of links: 'Instances', 'Third-party applications' (with a 'New' tag), and 'Documentation' (with an external link icon). The main area has a breadcrumb 'Amazon Connect > Create Amazon Connect instance' and a progress indicator with five steps: 'Step 1 Set identity', 'Step 2 Add administrator' (current), 'Step 3 Set telephony', 'Step 4 Data storage', and 'Step 5 Review and create'. The 'Add administrator' section is titled 'Add administrator' and includes an 'Administrator - optional' section with a radio button selected for 'Specify an administrator' (with a description: 'Specify an administrator for this instance of Amazon Connect. The administrator will have full permissions to access all of Amazon Connect.') and another radio button for 'No administrator'. Below this are input fields for 'First name' (filled with 'Vinicius'), 'Last name' (filled with 'Mariano'), 'Username' (redacted), 'Password' (masked with dots), 'Password (verify)' (masked with dots), and 'Email' (redacted). At the bottom, there is a 'Tags - optional' section with a description: 'Tags are key-value pairs that you can add to AWS resources to help identify, organize and search for resources.' At the bottom right are 'Cancel', 'Previous', and 'Next' buttons.

Após preencher informações do usuário clique em Next para ir próxima tela de configuração

10. Na tela "Set telephony", selecione quais tipos de ligações a instância poderá realizar. Deixe ambas as opções marcadas para que sua instância possa receber e efetuar ligações.

The screenshot shows the 'Set telephony' step of the 'Create Amazon Connect instance' wizard. The sidebar and breadcrumb are identical to the previous screenshot. The progress indicator shows 'Step 2 Add administrator' as completed and 'Step 3 Set telephony' as the current step. The 'Set telephony' section is titled 'Set telephony' and includes a 'Telephony Options' section with the instruction: 'Choose whether your contact center allows inbound calls, outbound calls, or both.' Below this are two checkboxes, both of which are checked: 'Allow incoming calls' and 'Allow outgoing calls'. At the bottom right are 'Cancel', 'Previous', and 'Next' buttons.

Após marcar as duas opções, clique em "Next" para ir à próxima tela de configuração, onde configuraremos o armazenamento da instância.

Por padrão, o Amazon Connect cria buckets para armazenar gravações de chamadas, transcrições de chats, relatórios exportados onde são criptografados usando o AWS Key Management Service e depois armazenados no bucket do Amazon S3.

Step 1  
[Set identity](#)

Step 2  
[Add administrator](#)

Step 3  
[Set telephony](#)

Step 4  
**Data storage**

Step 5  
[Review and create](#)

## Data storage

▼ Data storage

Call recordings, scheduled reports, and chat transcripts are stored in a S3 bucket that is created for you when you create an Amazon Connect instance. The stored data is encrypted by the AWS Key Management Service using a key specific to your Amazon Connect instance. Flow logs are stored in Amazon CloudWatch Logs in a log group created for you.

**Amazon Connect permissions**

By choosing Next, you are granting Amazon Connect permission to:

- Read and write to your S3 bucket.
- Read and write CloudWatch Logs.
- Encrypt your data.

**Connect data**  
Your Connect data will be stored in this S3 bucket:

amazon-connect- [redacted] [Copy](#)

**Flow logs**  
Your flow logs will be stored here in CloudWatch:

/aws/connect/ [redacted] [Copy](#)

☒ **Enable Customer Profiles**  
Customer Profiles uses your customer data, including Connect contact history, to identify and help personalize flows and your agent's interactions with contacts. You can further customize your Customer Profile domain later, including adding more data sources and changing data encryption settings. [Learn more](#)

☐ **Customize data storage (advanced)**

[Cancel](#) [Previous](#) [Next](#)

Para este tutorial, deixaremos as configurações padrão do Amazon Connect, mas você pode configurar para usar buckets e chaves pré-existentes, se desejar.

Nessa mesma tela, podemos ver que é criado um grupo de logs no Amazon CloudWatch onde ficarão armazenados logs das ligações.

Step 1

[Set identity](#)

Step 2

[Add administrator](#)

Step 3

[Set telephony](#)

Step 4

**Data storage**

Step 5

[Review and create](#)

## Data storage

▼ Data storage

Call recordings, scheduled reports, and chat transcripts are stored in a S3 bucket that is created for you when you create an Amazon Connect instance. The stored data is encrypted by the AWS Key Management Service using a key specific to your Amazon Connect instance. Flow logs are stored in Amazon CloudWatch Logs in a log group created for you.

Amazon Connect permissions

By choosing Next, you are granting Amazon Connect permission to:

- Read and write to your S3 bucket.
- Read and write CloudWatch Logs.
- Encrypt your data.

Connect data

Your Connect data will be stored in this S3 bucket:

amazon-connect-

Copy

Flow logs

Your flow logs will be stored here in CloudWatch:

/aws/connect/

Copy

☒ Enable Customer Profiles

Customer Profiles uses your customer data, including Connect contact history, to identify and help personalize flows and your agent's interactions with contacts. You can further customize your Customer Profile domain later, including adding more data sources and changing data encryption settings. [Learn more](#)

☐ Customize data storage (advanced)

Cancel

Previous

Next

Continuando na tela "Data storage", temos a opção de habilitar perfis de clientes. Essa opção usa os dados do cliente, incluindo o histórico de contatos do Connect, para identificar e ajudar a personalizar os fluxos e as interações do seu agente com os contatos.

Deixe marcado para ser habilitado.

Step 1

[Set identity](#)

Step 2

[Add administrator](#)

Step 3

[Set telephony](#)

Step 4

**Data storage**

Step 5

[Review and create](#)

## Data storage

▼ Data storage

Call recordings, scheduled reports, and chat transcripts are stored in a S3 bucket that is created for you when you create an Amazon Connect instance. The stored data is encrypted by the AWS Key Management Service using a key specific to your Amazon Connect instance. Flow logs are stored in Amazon CloudWatch Logs in a log group created for you.

Amazon Connect permissions

By choosing Next, you are granting Amazon Connect permission to:

- Read and write to your S3 bucket.
- Read and write CloudWatch Logs.
- Encrypt your data.

Connect data

Your Connect data will be stored in this S3 bucket:

amazon-connect-

Copy

Flow logs

Your flow logs will be stored here in CloudWatch:

/aws/connect/

Copy

☒ Enable Customer Profiles

Customer Profiles uses your customer data, including Connect contact history, to identify and help personalize flows and your agent's interactions with contacts. You can further customize your Customer Profile domain later, including adding more data sources and changing data encryption settings. [Learn more](#)

☐ Customize data storage (advanced)

Cancel

Previous

Next

Agora, avance para a próxima tela, onde será apresentado um resumo de todas as configurações aplicadas anteriormente.

Step 1  
[Set identity](#)

Step 2  
[Add administrator](#)

Step 3  
[Set telephony](#)

Step 4  
[Data storage](#)

Step 5  
**Review and create**

## Review and create

### Identity management

Edit

Storing users within Amazon Connect

### Add administrator

Edit

First name	Last name
Vinicius	Mariano
Username	
vinicius.mariano	
Password	Email
*****	

### Telephony Options

Edit

<b>Allow incoming calls</b> Your contact center can handle incoming calls.	<b>Allow outgoing calls</b> Your contact center can make outbound calls. You can set which users can place outbound calls in user permissions.
---	--

### Data storage

Edit

<b>Call recordings</b> Call recordings will be stored in this S3 bucket: amazon-connect- 	<b>Encrypted using this key</b> arn:aws:kms: key/
<b>Chat transcripts</b> Chat transcripts will be stored in this S3 bucket: amazon-connect- 	<b>Encrypted using this key</b> arn:aws:kms: key/
<b>Exported reports</b> Exported reports will be stored in this S3 bucket: amazon-connect- 	<b>Encrypted using this key</b> arn:aws:kms: key/
<b>Attachments</b> Attachments will be stored in this S3 bucket: <b>Not enabled</b>	<b>Encrypted using this key</b>
<b>Flow logs</b> Your flow logs will be stored here in CloudWatch: /aws/connect	
<b>Customer Profiles</b> <b>Enabled</b>	

► Tags

Edit

Cancel

Previous

Create instance

Após conferir as configurações anteriores, clique em "Criar Instância".