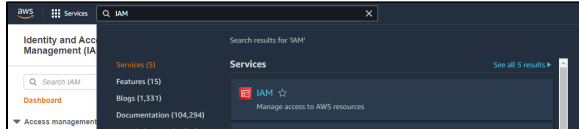


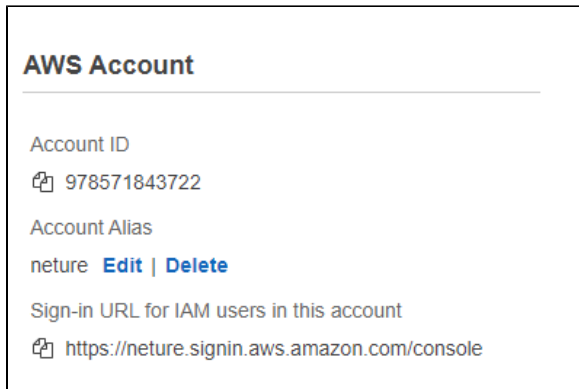
Como liberar acesso à Neture via Role de acesso (Amazon Web Services)

Nesta sessão, será disponibilizado o processo de instruções para configuração de acesso da Neture à sua conta Amazon Web Services.

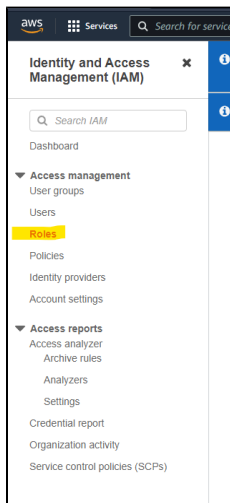
Acesse o **AWS IAM** para configuração do acesso:



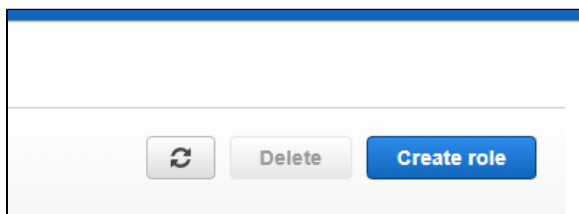
Crie um Account Alias para ficar mais fácil identificar sua empresa, através do menu a sua direita, clicando em **EDIT**:



Agora, acesse **Roles**:



Clique em **Create role** para criar uma nova Role de acesso:



Selecione o tipo de Role "**AWS account**" e selecione a opção **Another AWS account** abaixo:

Dados Importantes

Número da Conta da Neture (Account ID): 978571843722

Políticas de acesso somente para Leitura

Utilizado geralmente para assessment de ambientes

- AWSBillingReadOnlyAccess
- ReadOnlyAccess

Políticas de acesso para Gestão total do ambiente

- AdministratorAccess
- AWSBillingReadOnlyAccess

Select trusted entity

Trusted entity type

☐ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☒ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ Web identity
Allow users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

An AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ This account (978571843722)

☒ Another AWS account
Account ID
Identifier of the account that can use this role

Account ID is a 12-digit number.

Options

☐ Require external ID (Best practice when a third party will assume this role)

☐ Require MFA
Requires that the assuming entity use multi-factor authentication.

* Não selecione as opções Require external ID e Require MFA, pois estas opções vão limitar o acesso via AWS CLI, necessário para diversas manutenções/gestão do ambiente.

Digite o Account ID da Neture no campo **Account ID** (localizado neste documento à direita):

Select trusted entity

Trusted entity type

☐ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☒ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ Web identity
Allow users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

An AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ This account (978571843722)

☒ Another AWS account
Account ID
Identifier of the account that can use this role

Account ID is a 12-digit number.

Options

☐ Require external ID (Best practice when a third party will assume this role)

☐ Require MFA
Requires that the assuming entity use multi-factor authentication.

Clique em **Next** para avançar para próxima tela.

Selecione as opções de acesso (Políticas) conforme a necessidade repassada pela equipe da Neture, ou utilize uma das opções de acesso à direita deste documento:

Add permissions

Permissions policies (Selected 1/1758)

Choose one or more policies to attach to your new role.

146 matches

Policy name (if available)	Type	Description
<input type="checkbox"/> AWSTransientAccess	AWS m...	Provides read-only access to IAM via the AWS Management Console.
<input type="checkbox"/> AmazonEC2ReadOnlyAccess	AWS m...	Provides read-only access to Amazon EC2 instances. Note that this policy also grants access to Amazon EC2 roles.
<input checked="" type="checkbox"/> AmazonEC2ReadOnlyAccess	AWS m...	Provides read-only access to AWS services and resources.
<input checked="" type="checkbox"/> AmazonEC2ReadOnlyAccess	AWS m...	Provides access to use Resource Groups and Tag Editor, but does not allow editing of tags via the Tag Editor.
<input type="checkbox"/> AmazonEC2ReadOnlyAccess	AWS m...	Provides read-only access to Amazon EC2 instances.
<input type="checkbox"/> AmazonEC2ReadOnlyAccess	AWS m...	Provides read-only access to AWS IAM architecture.

Set permissions boundary - optional

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Clique em **Next** para avançar para próxima tela.

Por último, dê o nome da Role de **NetureAccess**, que será utilizado por nossa equipe para acessar o ambiente:

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and "-", "@", "_" characters.

Description
Add a short explanation for this role.

Maximum 1000 characters. Use alphanumeric and "-", "@", "_" characters.

Confira os acessos concedidos, adicione tags caso seja de preferência e clique em **Create role** para criar a Role de acesso.

Pronto, este procedimento foi concluído, basta informar a equipe da Neture para validar o acesso. 😊

