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**:

AWS Account	
Account ID 伦 978571843722	
Account Alias neture Edit Delete	
Sign-in URL for IAM users in this account	

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

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:

Trusted entity type							
 AWS service Allow AVS 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 Allows users indensited 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 pert	y to perform actions in this account.						
An AWS account Allow entities in other AWS accounts belonging to you or a 3rd pert This account (9785/1843722) Another AWS account	r lo perferm actions in this account.						
An AWS account Allow entities in other AWS accounts belonging to you or a 3rd pert This account (9785/1643722) Account ID Account ID Account ID	r to perform actions in this account.						
An AWS account Arose entres in other ARIS accounts beforiging to you or a 3rd pert This account (078071643722) A Ancher AWS account Account ID Marchine AWS account A	y to perfere actions in this account.						
An AWS account Aware effities in the XRM accounts beforinging to you or a 3rd pert Than account (RRMS71645722) Another XRMS account Count ID Benefities of the account that can use the rule Account ID is a 12 digit surface.	y la perform adona in lles account.						
An AWS account Maker either in nihre /k0% accounts beforging by sour is bit part This account (\$7857164722) Account ID Account ID Account ID Account ID is a 12-bit humber. Account ID is a 12-bit humber.	y to perform actions in the account.						
An AWS account We write the drive All account beinging by you or 3 bit pert The account (078071641722) Another MVB account Account ID Control I	In partnern actions in the account						

* 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):

AWS service Allow AWS services Re EC2, Lambda, or others to parform 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 Allows users federated by the specified external web identity provider to assume this role to perform actions
		in this account.
 SAML 2.0 Recetation Allow users individual with SAML 2.0 from a corporate devicery to perform actions in this account. 	Custom trust policy Create a custom trust policy to enable others to perform actions in this account.	
This account (978571843722) Another AWS account count ID		
rener of the account that can use this role 78571845722		
count ID is a 12-digit number.		

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:

Permissions policies (Selected 1/758) Choose one or more policies to attach to your new role. Q. Ptime policies by property or policy neme and press enter			Crease policy (2 Crease policy (2 145 matches (1 2 3 4 5 6 7 8)
	Policy name (?	a. 7ype ∵	Description
	O IAVReadOnyAccess	AWS m	Provides read only access to IAM via the AIVS Management Console.
	Original ReadOnlyAccess	AWS m	Provides read only access to Amazon Neptune. Note that this policy also grants access to Amazon RDS reso
	ReadOnlyAccess	AVIS m	Provides read-only access to AWS services and resources.
	ResourceGroupsandTagEditorReadOnlyAccess	AV/IS m	Provides access to use Resource Groups and Tag Editor, but does not allow editing of tags via the Tag Editor.
	B SeniceQuotasReadOnlyAccess	AW8 m	Provides read only access to Bervice Quotas
	WetArchitectedConsideReadOnlyAccess	AWS m	Provides read-only access to AWS Well-Architected Tool via the AWS Management Console

Clique em Next para avançar para próxima tela.

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

Name, review, and create				
Role details				
Role name Entre a maximglal name to identify this role.				
NetweAccess				
Moximum 64 characters. Use alphanameric and '+=, @' characters.				
Description Ad a short explanation for this rele.				
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. 🙂