

Configurar a conta do AWS Multi-cloud vManage com IAM

Contents

[Introduction](#)

[Background](#)

[Problema](#)

[Solução](#)

[Referência](#)

Introduction

Este documento descreve como resolver problemas de confiança que ocorrem quando você tenta usar a conta IAM para automação de várias nuvens.

Background

Quando você usa o recurso de várias nuvens da Cisco com o AWS TGW e a conta AWS da sua empresa, há problemas de confiança. Isso porque a empresa única Account ID é diferente do vManage EC2 instância no AWS.

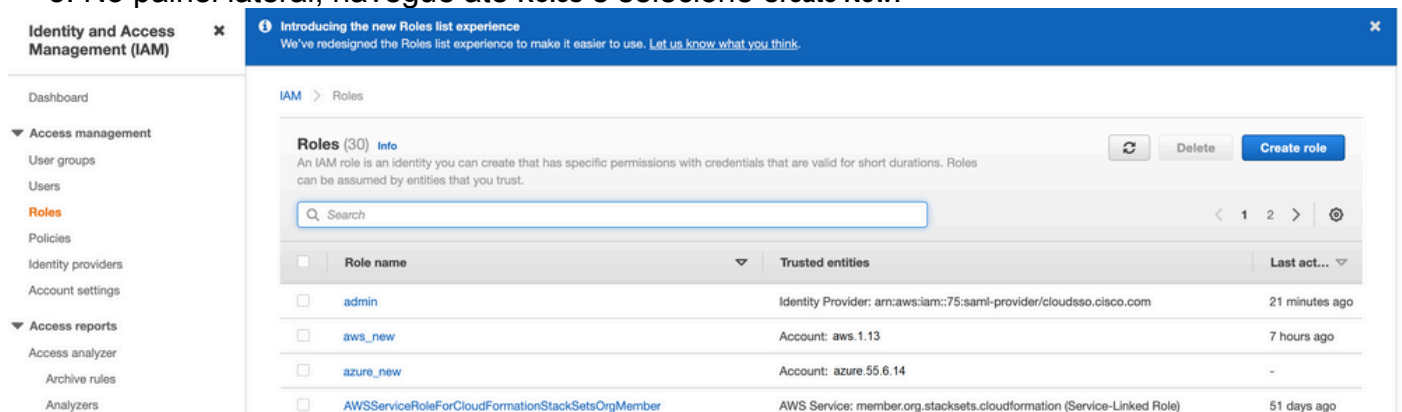
Problema

Quando você usa a conta IAM para automação de várias nuvens, isso causa um problema de confiança.

Solução

Para resolver esse problema:

1. Navegue até **AWS > Identity and Access Management (IAM)** e criar uma nova **ROLE** ou outro **ROLE**.
2. Na guia **AWS** portal, insira **IAM** na barra de pesquisa. O **IAM** abre.
3. No painel lateral, navegue até **Roles** e selecione **Create New**.



The screenshot shows the AWS IAM console interface. At the top, there is a blue banner with the text "Introducing the new Roles list experience" and a link "Let us know what you think". Below the banner, the breadcrumb "IAM > Roles" is visible. The main content area displays "Roles (30)" with an "Info" link and a "Create role" button. A search bar is present. Below the search bar is a table with the following columns: "Role name", "Trusted entities", and "Last act...". The table contains the following rows:

<input type="checkbox"/>	Role name	Trusted entities	Last act...
<input type="checkbox"/>	admin	Identity Provider: arn:aws:iam::75:saml-provider/cloudsso.cisco.com	21 minutes ago
<input type="checkbox"/>	aws_new	Account: aws.1.13	7 hours ago
<input type="checkbox"/>	azure_new	Account: azure.55.6.14	-
<input type="checkbox"/>	AWSServiceRoleForCloudFormationStackSetsOrgMember	AWS Service: member.org.stacksets.cloudformation (Service-Linked Role)	51 days ago

4. Selecione a opção **Another AWS Account** como uma opção.

5. O **Account ID** é o **AWS Account** e tem o **vManage EC2** instância criada. Para contas Cisco Hosted, a ID da conta é "2002388880647". (Não é sua própria **AWS Account ID**.) Consulte Referência no final deste artigo.

6. Marque a caixa para "**External ID**" e insira um valor em **vManage > Cloud onRamp for multi-cloud > Account Management > Add AWS Account**.

⚙️ **CONFIGURATION** [Cloud OnRamp For Multi-Cloud](#) > [Cloud Account Management](#) > Associate Cloud Account

Provide Cloud Account Details

Cloud Provider

 Amazon Web Services

Cloud Account Name

Description (optional)


Use for Cloud Gateway

Yes No

Login in to AWS with

Key IAM Role

Role ARN

External Id 

<http://vm/can/do>

Create role

- 1
- 2
- 3
- 4

Select type of trusted entity

- AWS service**
EC2, Lambda and others
- Another AWS account**
Belonging to you or 3rd party
- Web identity**
Cognito or any OpenID provider
- SAML 2.0 federation**
Your corporate directory

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID* ⓘ

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

You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. [Learn more](#)

External ID

Important: The console does not support using an external ID with the Switch Role feature. If you select this option, entities in the trusted account must use the API, CLI, or a custom federation proxy to make cross-account iam:AssumeRole calls. [Learn more](#)

Require MFA ⓘ

7. Defina permissões.

Create role

- 1
- 2
- 3
- 4

▼ Attach permissions policies

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

Filter policies Showing 32 results

	Policy name	Used as
<input type="checkbox"/>	▶ AmazonEC2ContainerRegistryFullAccess	None
<input type="checkbox"/>	▶ AmazonEC2ContainerRegistryPowerUser	None
<input type="checkbox"/>	▶ AmazonEC2ContainerRegistryReadOnly	None
<input type="checkbox"/>	▶ AmazonEC2ContainerServiceAutoscaleRole	None
<input type="checkbox"/>	▶ AmazonEC2ContainerServiceEventsRole	None
<input type="checkbox"/>	▶ AmazonEC2ContainerServiceforEC2Role	None
<input type="checkbox"/>	▶ AmazonEC2ContainerServiceRole	None
<input checked="" type="checkbox"/>	▶ AmazonEC2FullAccess	Permissions policy (1)

▶ Set permissions boundary

8. Ignore as marcas.

9. Revise a última página e nomeie a atribuição. Lançar a criação de **ROLE** e copiar o **ARN** nos **AWS** portal.

Create role



Review

Provide the required information below and review this role before you create it.

Role name*




Use alphanumeric and '+,.,@-_' characters. Maximum 64 characters.

Role description

Maximum 1000 characters. Use alphanumeric and '+,.,@-_' characters.

Trusted entities The account aws_account_1234567

Policies

-  AdministratorAccess [↗](#)
-  AmazonVPCFullAccess [↗](#)
-  AmazonEC2FullAccess [↗](#)

Permissions boundary Permissions boundary is not set

No tags were added.

[Roles](#) > aws_account_1234567

Summary


Role ARN	arn:aws:iam::75:role/aws_account_1234567 ↗
Role description	aws multicloud test Edit
Instance Profile ARNs	↗
Path	/
Creation time	2021-08-05 23:21 EDT
Last activity	Not accessed in the tracking period
Maximum session duration	1 hour Edit
Give this link to users who can switch roles in the console	https://signin.aws.amazon.com/switchrole?roleName=aws_account&account=1234567

10. Verifique se a sintaxe sob o comando "**Trust Relationship > Edit Relationship**"corresponde a este exemplo JSON (com os valores definidos):

```
{ "Version": "2022-05-04", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam:::account_number:root" }, "Action": "sts:AssumeRole", "Condition": { "StringEquals": { "sts:ExternalId": "vm:site_address" } } } ] }
```

11. Copie o **ARN** de **AWS** e preencha os detalhes no **vManage** página de várias nuvens.

Cloud Account Credentials - Update

Cloud Provider	<input type="text" value="aws Amazon Web Services"/>
Cloud Account Name	<input type="text" value="name_here"/>
Description (optional)	<input type="text"/>
Use for Cloud Gateway	<input checked="" type="radio"/> Yes <input type="radio"/> No
Login in to AWS with	<input type="radio"/> Key <input checked="" type="radio"/> IAM Role
Role ARN	<input type="text"/>
External Id 	<input type="text" value="vm: 1234567"/>

O `"/var/log/nms/containers/cloudagent-v2/cloudagent-v2.log"` O arquivo tem mensagens valiosas (com os valores definidos por você):

```
[2021-08-06T02:47:07UTC+0000:140360670770944:INFO:ca-v2:grpc_service.py:432] Returning
ValidateAccountInfo Response: { "mcCtxt": { "tenantId": "VTAC5 - 19335", "ctxId": "ebd23ec1-
95fa-4e27-8f6a-e3b10c086f95" }, "accountInfo": { "cloudType": "AWS", "accountName":
"aws_accountname", "orgName": "VTAC5 - 19335", "description": "", "billingId": "",
"awsAccountInfo": { "accountSpecificInfo": { "authType": "IAM", "iamBasedAuth": { "arn":
"HUIZ82ywKt+EfSdKS8kaMpWCFE7W3vLjqaJCPgmSP1D61Rsd1yrIldmQsf9bW7OFNhUKH5LQg+2Gkdey0IyTUg==" ,
```

Referência

[Cisco Cloud onRamp for IaaS AWS Version2.html](#)