Configuración de la cuenta vManage de nube múltiple de AWS con IAM

Contenido

Introducción

Este documento describe cómo resolver los problemas de confianza que se producen cuando intenta utilizar la cuenta IAM para la automatización de varias nubes.

Background

Cuando utiliza la función de nube múltiple de Cisco con AWS TGW y la cuenta de AWS de su empresa, surgen problemas de confianza. Esto se debe a que la empresa única **Account ID** es diferente de la **vManage EC2** instancia en AWS.

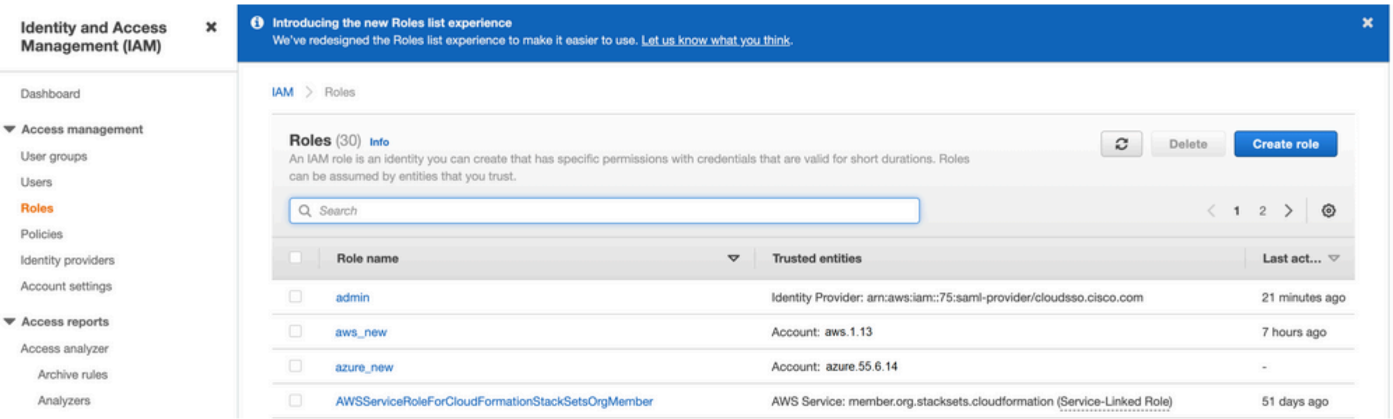
Problema

Cuando se utiliza la cuenta IAM para la automatización de varias nubes, se produce un problema de confianza.

Solución

Para resolver este problema:

1. Vaya a **AWS > Identity and Access Management (IAM)** y crear una nueva **ROLE** u otro elemento enumerado **ROLE.**
2. En el **AWS** portal, entrar **IAM** en la barra de búsqueda. El **IAM** se abre.
3. En el panel lateral, vaya a **Roles** y, a continuación, seleccione **Create New.**



Identity and Access Management (IAM)

- Dashboard
- Access management
  - User groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
- Access reports
  - Access analyzer
    - Archive rules
    - Analyzers

Introducing the new Roles list experience
We've redesigned the Roles list experience to make it easier to use. Let us know what you think.

IAM > Roles

Roles (30) Info

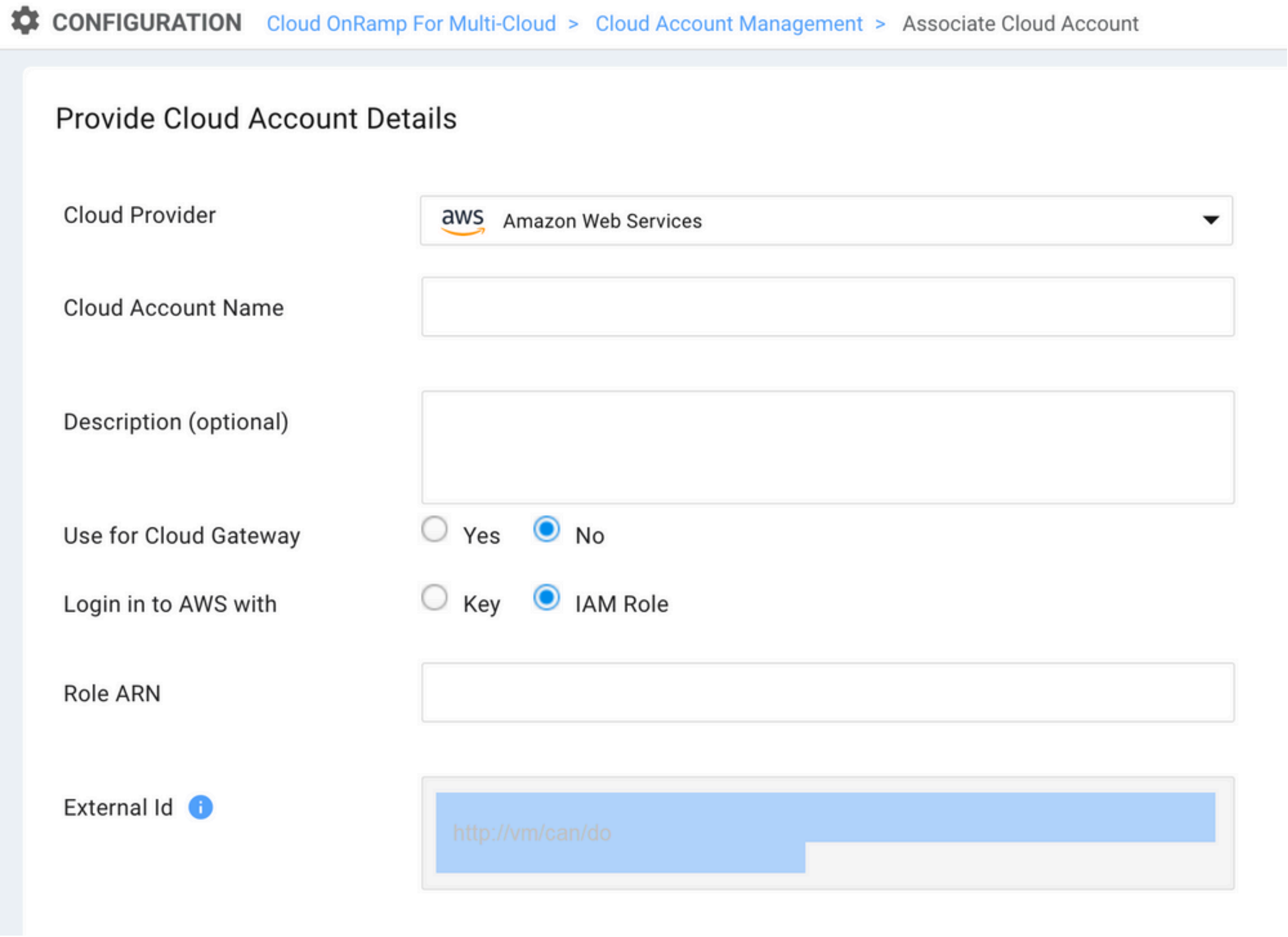
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

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

4. Seleccione el **Another AWS Account** como opción.

5. El **Account ID** es el **AWS Account** y tiene el **vManage EC2** instancia creada. Para cuentas alojadas de Cisco, el ID de cuenta es "200238880647". (NO es el suyo propio **AWS Account ID**.) Consulte la Referencia al final de este artículo.

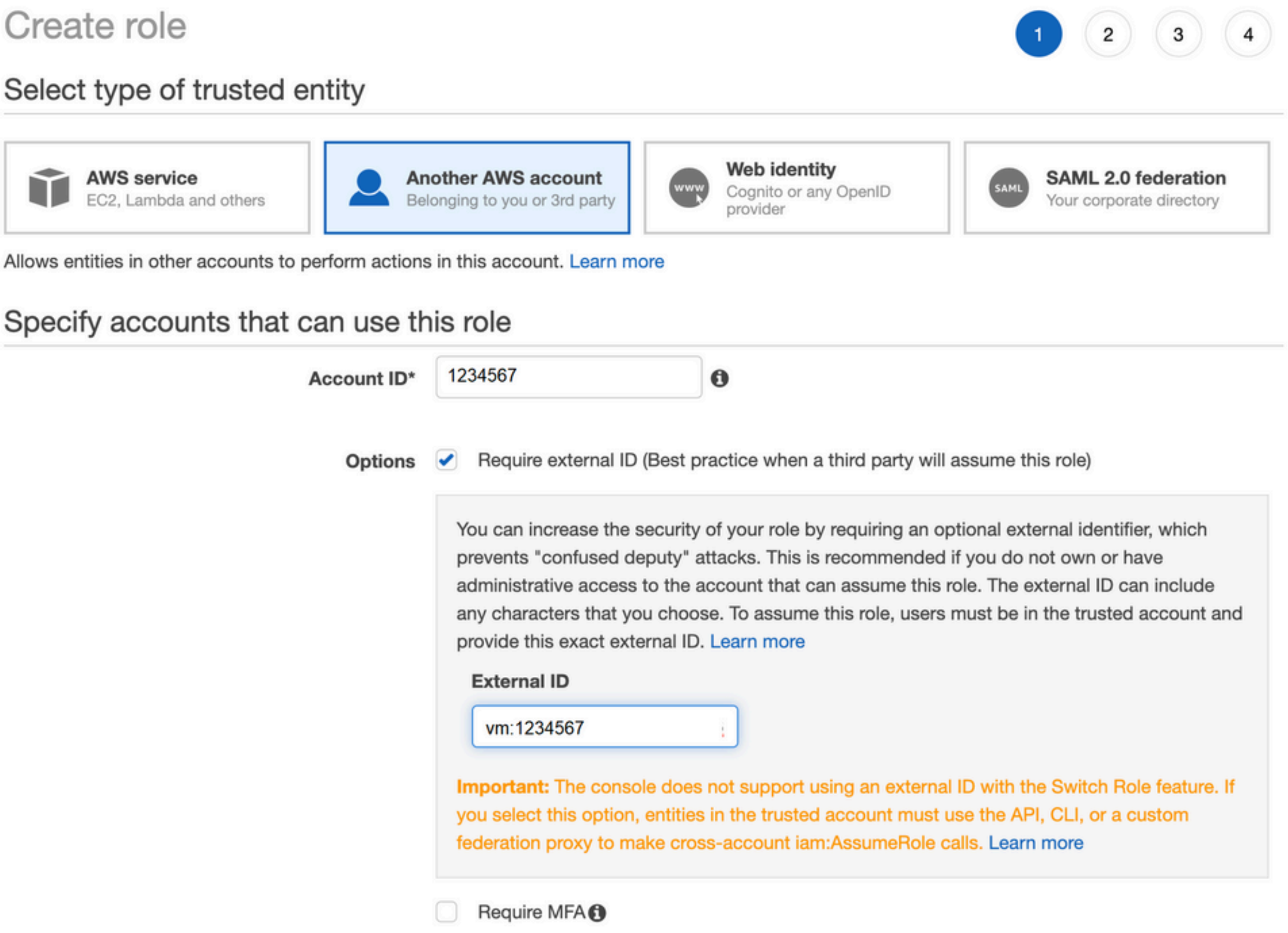
6. Active la casilla de verificación **"External ID"** e introduzca un valor en **vManage > Cloud onRamp for multi-cloud > Account Management > Add AWS Account.**



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

Select type of trusted entity

Allows entities in other accounts to perform actions in this account. Learn more

Specify accounts that can use this role

Account ID* 1234567

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

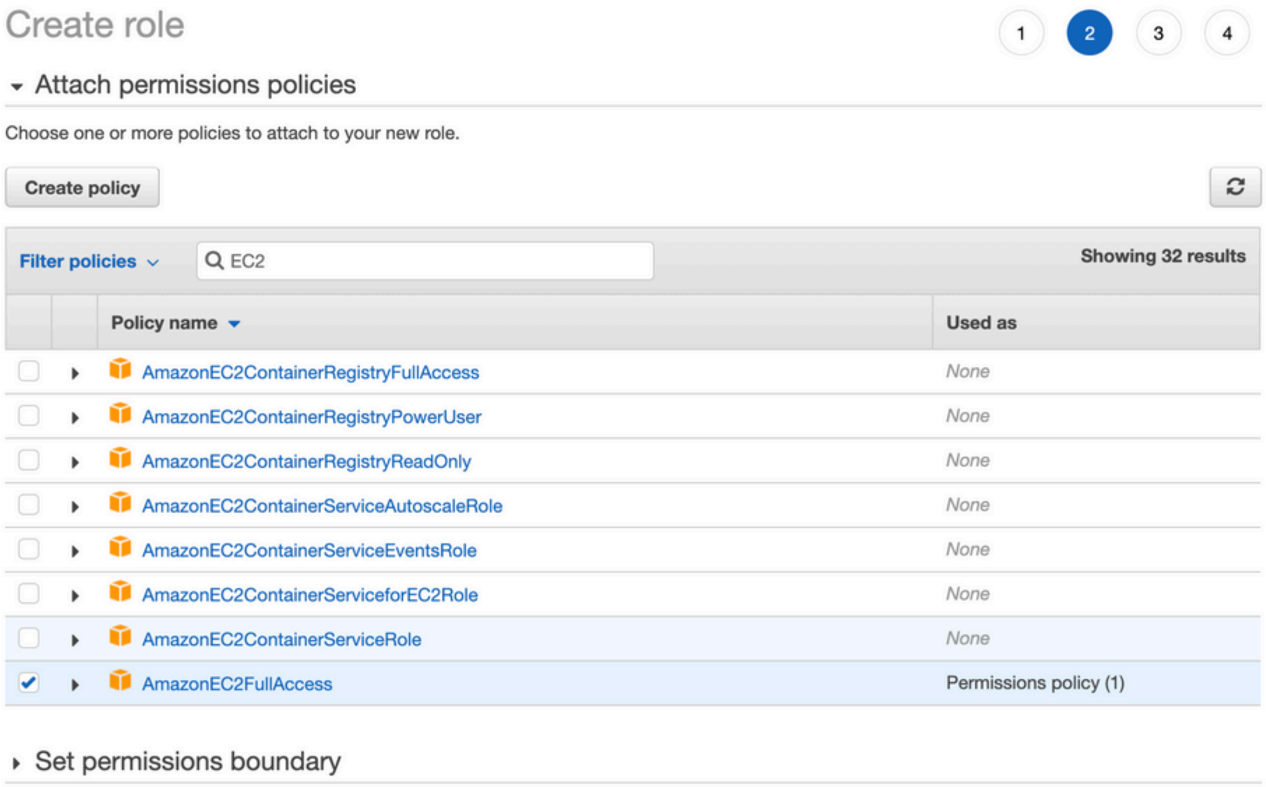
You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose.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

External ID vm:1234567

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. Establezca permisos.



Create role

Attach permissions policies

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

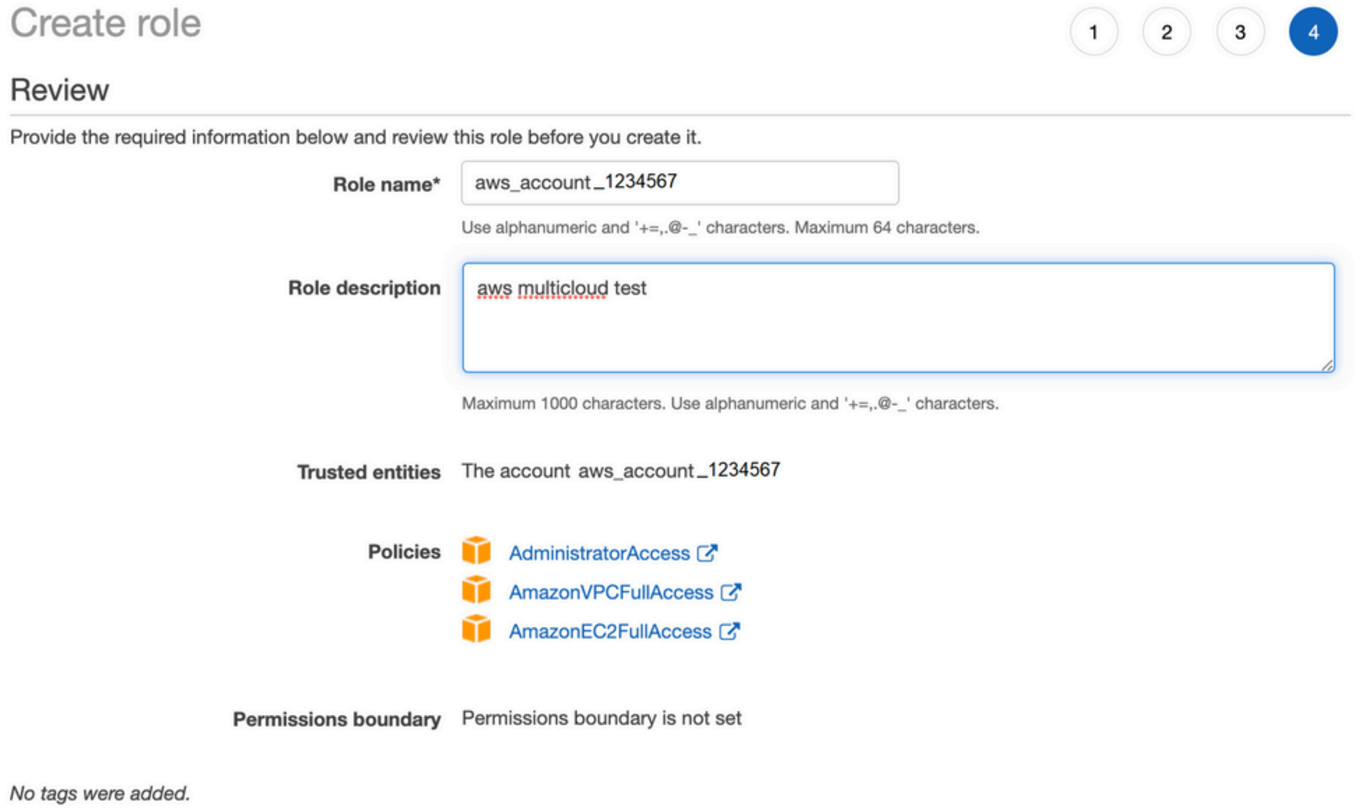
Filter policies EC2 Showing 32 results

		Policy name	Used as
□	▸	AmazonEC2ContainerRegistryFullAccess	None
□	▸	AmazonEC2ContainerRegistryPowerUser	None
□	▸	AmazonEC2ContainerRegistryReadOnly	None
□	▸	AmazonEC2ContainerServiceAutoscaleRole	None
□	▸	AmazonEC2ContainerServiceEventsRole	None
□	▸	AmazonEC2ContainerServiceforEC2Role	None
□	▸	AmazonEC2ContainerServiceRole	None
☑	▸	AmazonEC2FullAccess	Permissions policy (1)

Set permissions boundary

8. Omita las etiquetas.

9. Revise la última página y asigne un nombre al rol. Publicar la creación de **ROLE** y copie el **ARN** desde **AWS** portal.



Create role

Review

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

Role name* aws_account_1234567

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

Role description aws multicloud test

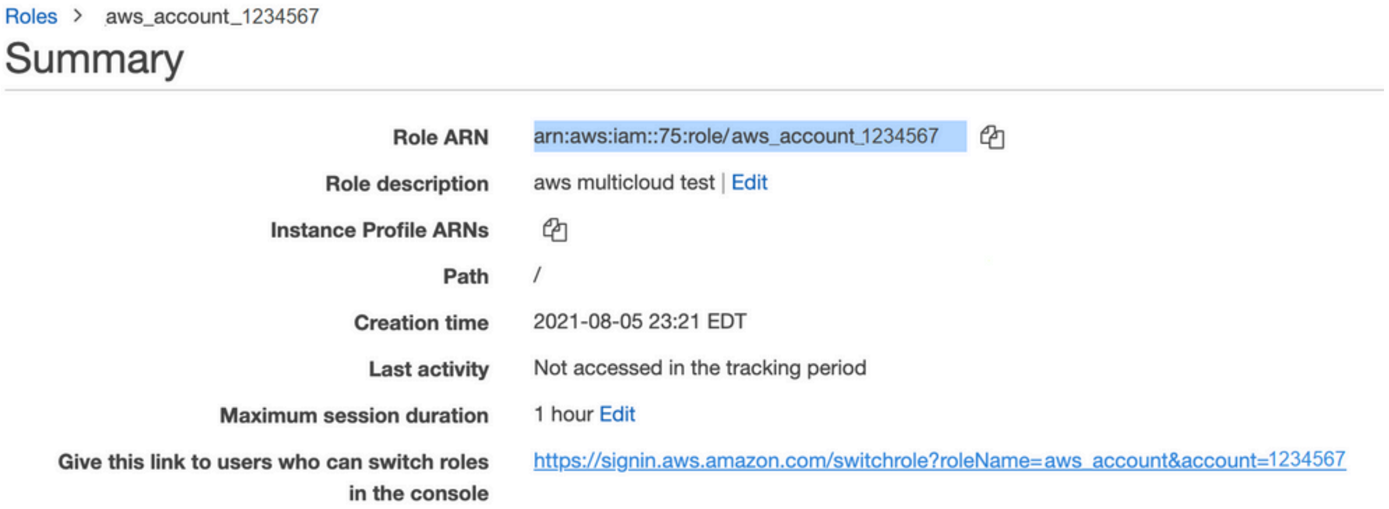
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

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

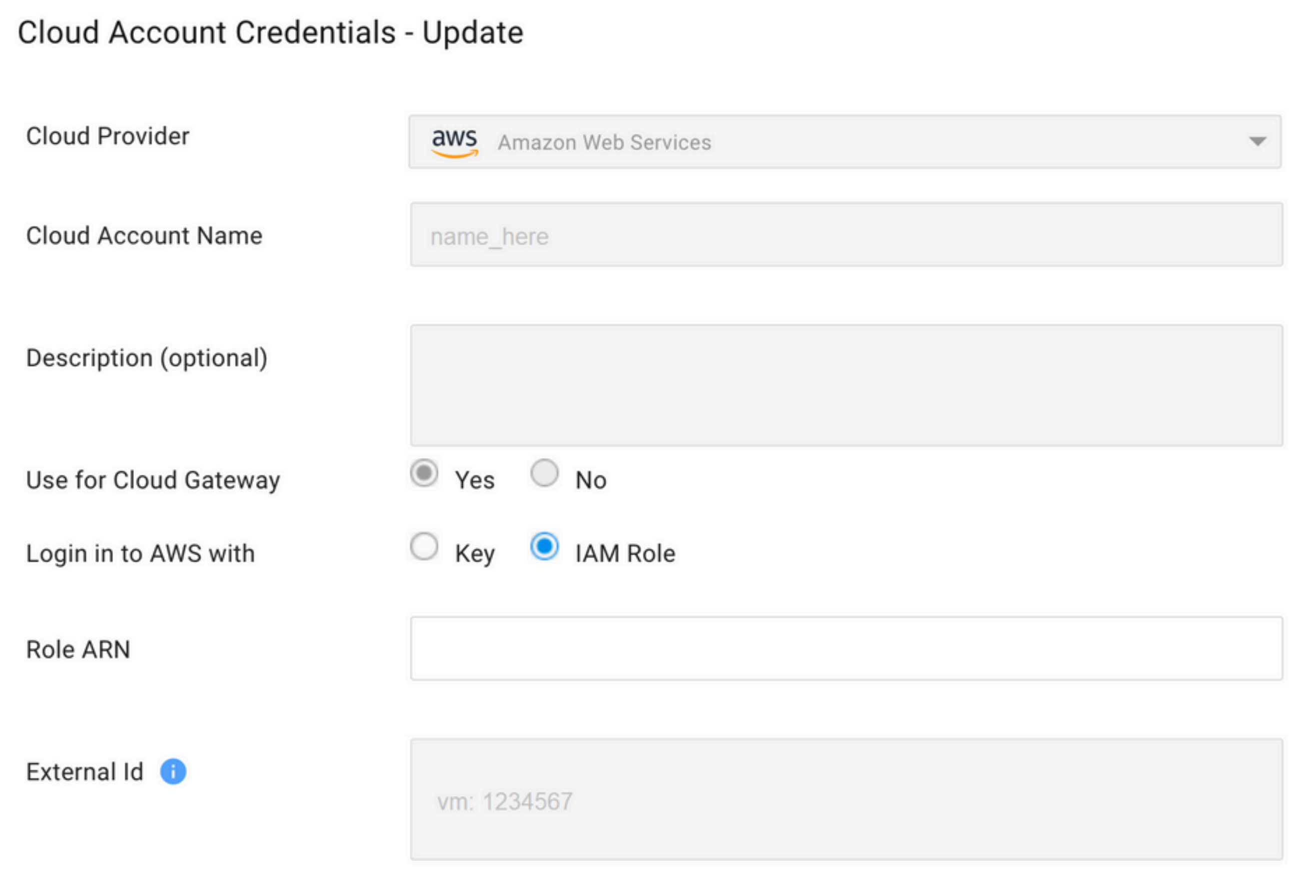
Summary

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. Asegúrese de que la sintaxis de la **"Trust Relationship > Edit Relationship"**coincide con este ejemplo de JSON (con los 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 el **ARN** desde **AWS** y rellene los detalles de la **vManage** página de nube múltiple.



Cloud Account Credentials - Update

Cloud Provider: aws Amazon Web Services

Cloud Account Name: name_here

Description (optional):

Use for Cloud Gateway: ● Yes ○ No

Login in to AWS with: ○ Key ● IAM Role

Role ARN:

External Id: vm: 1234567

"**/var/log/nms/containers/cloudagent-v2/cloudagent-v2.log**" contiene mensajes valiosos (con los valores que haya establecido):

```
[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==",
```

Referencia

Cisco_Cloud_onRamp_for_IaaS_AWS_Version2.html