

# Configurare l'account AWS Multi-cloud vManage con IAM

## Sommario

[Introduzione](#)

[Sfondo](#)

[Problema](#)

[Soluzione](#)

[Riferimento](#)

## Introduzione

In questo documento viene descritto come risolvere i problemi di attendibilità che si verificano quando si tenta di utilizzare l'account IAM per l'automazione multiscudo.

## Sfondo

Quando si utilizza la funzionalità multi-cloud Cisco con AWS TGW e l'account AWS della società, si verificano problemi di attendibilità. Questo perché l'azienda unica Account ID è diverso dal vManage Ec2 in AWS.

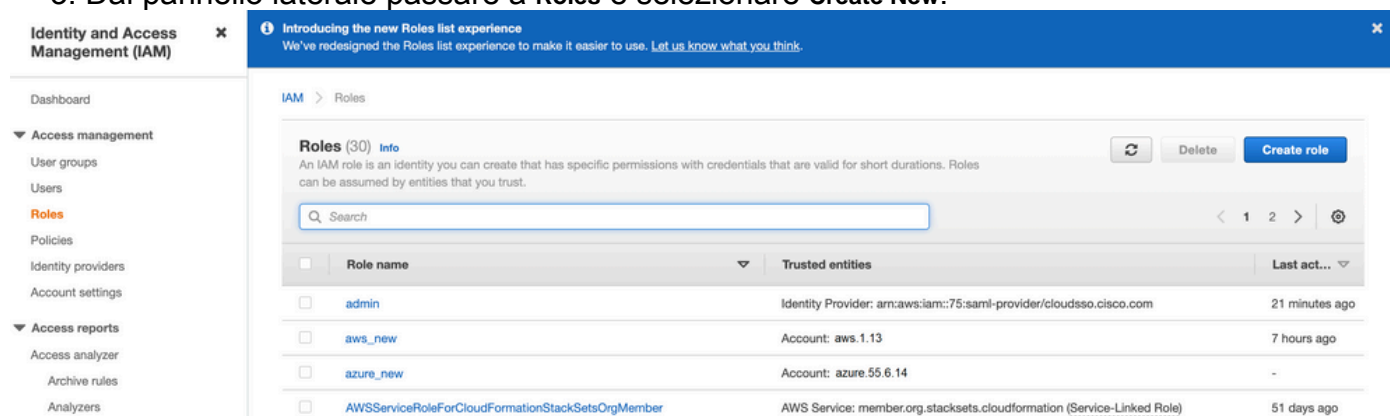
## Problema

Quando si utilizza l'account IAM per l'automazione di più cloud, si verifica un problema di attendibilità.

## Soluzione

Per risolvere il problema:

1. Passa a **AWS > Identity and Access Management (IAM)** e creare un nuovo **ROLE** o un altro **ROLE**.
2. Nella scheda **AWS** portale, immettere **IAM** nella barra di ricerca. Il **IAM** si apre.
3. Dal pannello laterale passare a **Roles** e selezionare **Create New**.




The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with 'Identity and Access Management (IAM)' selected. The main content area displays the 'Roles (30)' list. At the top of the main area, there is a blue notification banner: '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.' Below this, the 'Roles' section includes a search bar, a refresh button, a 'Delete' button, and a 'Create role' button. The roles list is a table with columns for 'Role name', 'Trusted entities', and 'Last act...'. The roles listed are:

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. Selezionare il **Another AWS Account** come opzione.

5. Il **Account ID** è il **AWS Account** e ha il **vManage EC2** istanza creata. Per gli account Cisco Hosted, l'ID account è "200238880647". (NON è il tuo) **AWS Account ID**.) Fare riferimento alla fine di questo articolo.

6. Selezionare la casella per "External ID" e immettere un valore in **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. Impostare le autorizzazioni.









## 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. Ignora i tag.

9. Controllare l'ultima pagina e assegnare un nome al ruolo. Post la creazione di **ROLE** e copiare **ARN** dal **AWS** portale.

## Create role

1 2 3 4

### 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


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

10. Assicurarsi che la sintassi in "Trust Relationship > Edit Relationship" corrisponde al seguente esempio JSON (con i valori impostati):

```
{ "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. Copia **ARN** da **AWS** e compilare i dettagli sul **vManage** pagina con più cloud.

## 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"/>

Il `"/var/log/nms/containers/cloudagent-v2/cloudagent-v2.log"` contiene messaggi importanti (con i valori impostati):

```
[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==" ,
```

### Riferimento

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