Configure AWS Multi-cloud vManage Account with IAM

Contents

Introduction

This document describes how to resolve trust issues that occur when you try to use the IAM account for multi-cloud automation.

Background

When you use the Cisco multi-cloud feature with AWS TGW and your company AWS account, there are trust issues. That is because the unique company **Account ID** is different from the **vManage EC2** instance in AWS.

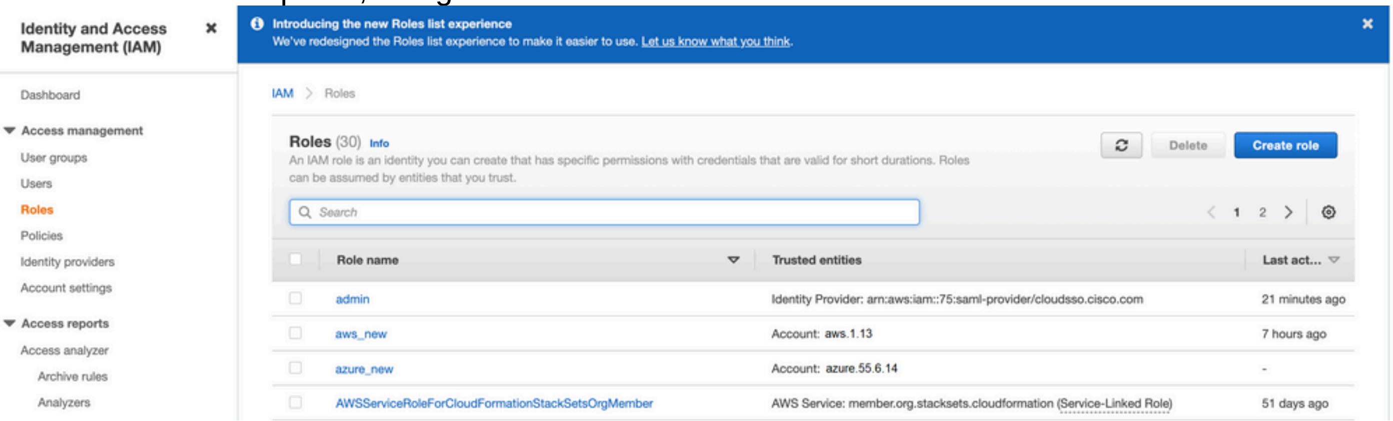
Problem

When you use the IAM account for multi-cloud automation, it causes a trust issue.

Solution

To resolve this problem:

1. Navigate to **AWS > Identity and Access Management (IAM)** and create a new **ROLE** or another listed **ROLE.**
2. On the **AWS** portal, enter **IAM** in the search bar. The **IAM** opens.
3. From the side panel, navigate to **Roles** and then select **Create New.**



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.

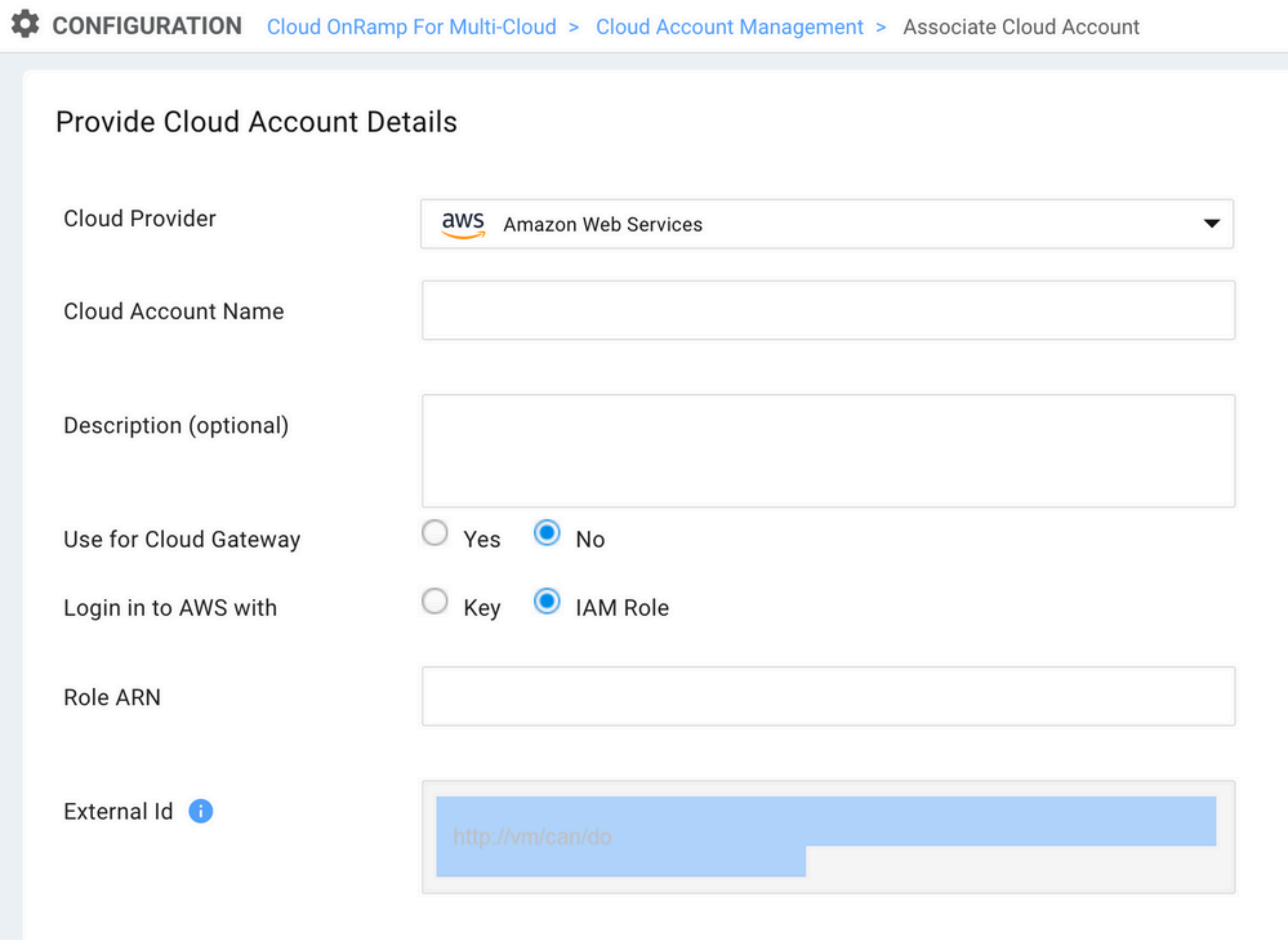
Roles (30) Info
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

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. Select the **Another AWS Account** as an option.

5. The **Account ID** is the **AWS Account** and has the **vManage EC2** instance built. For Cisco Hosted accounts, the account ID is "200238880647". (This is NOT your own **AWS Account ID**.) See Reference at the end of this article.

6. Check the box for **"External ID"** and enter a value under **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: aws Amazon Web Services

Cloud Account Name:

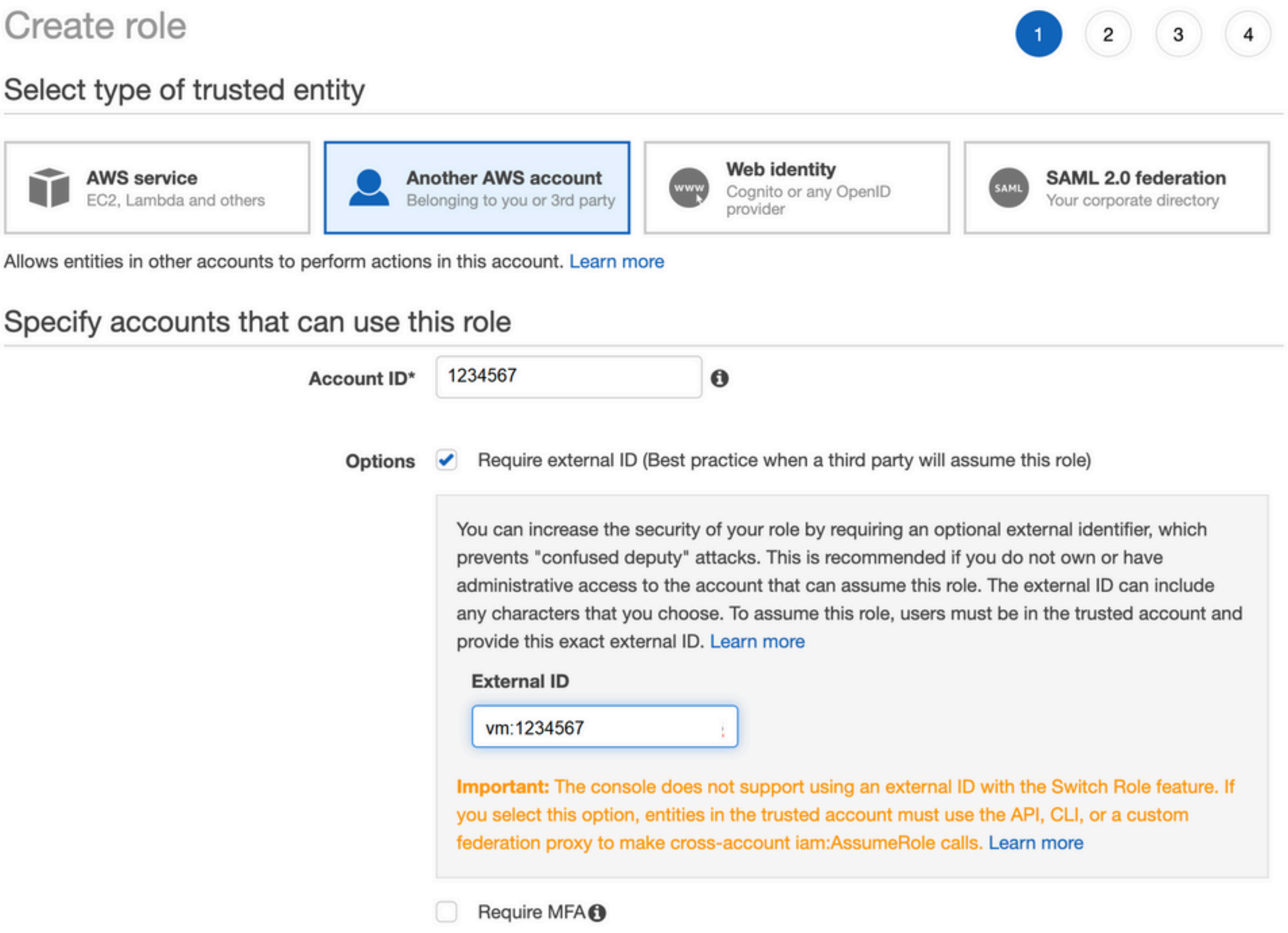
Description (optional):

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)

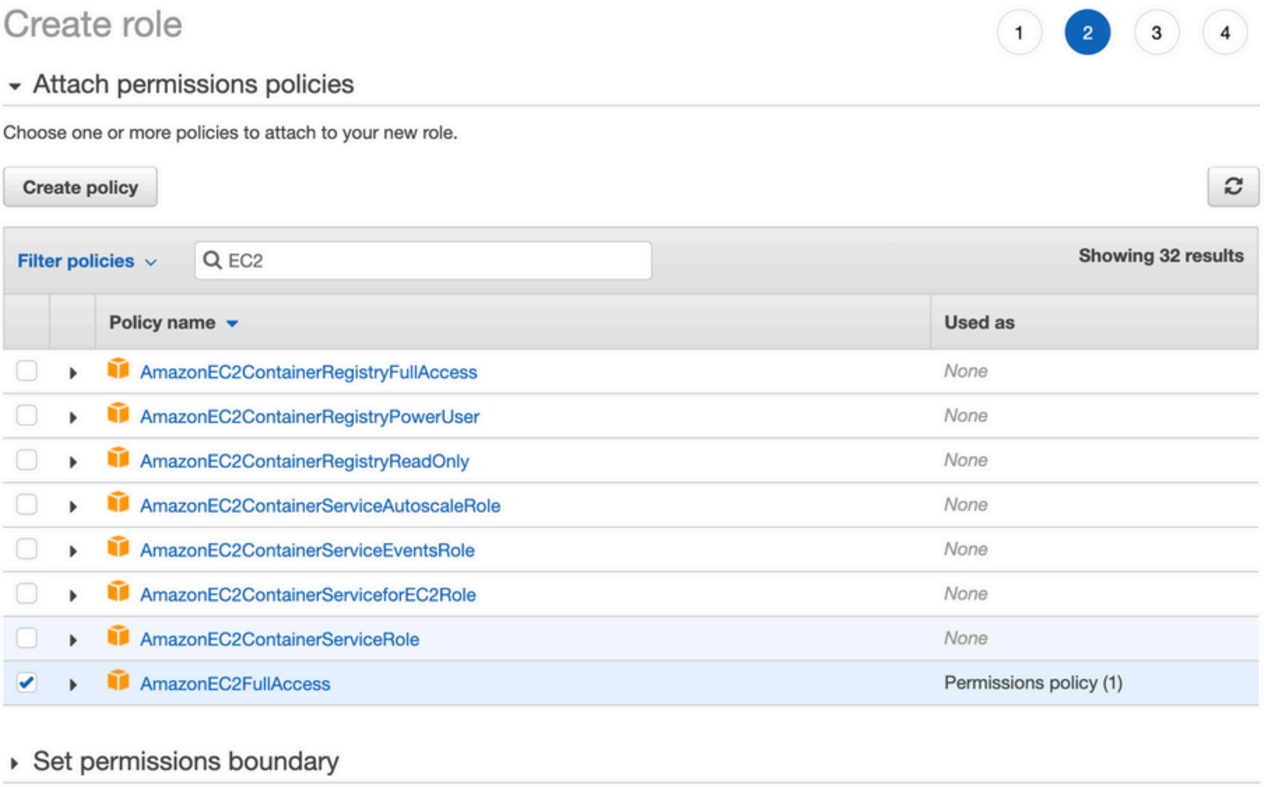
You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. 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. Set permissions.



Create role

Attach permissions policies

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

EC2

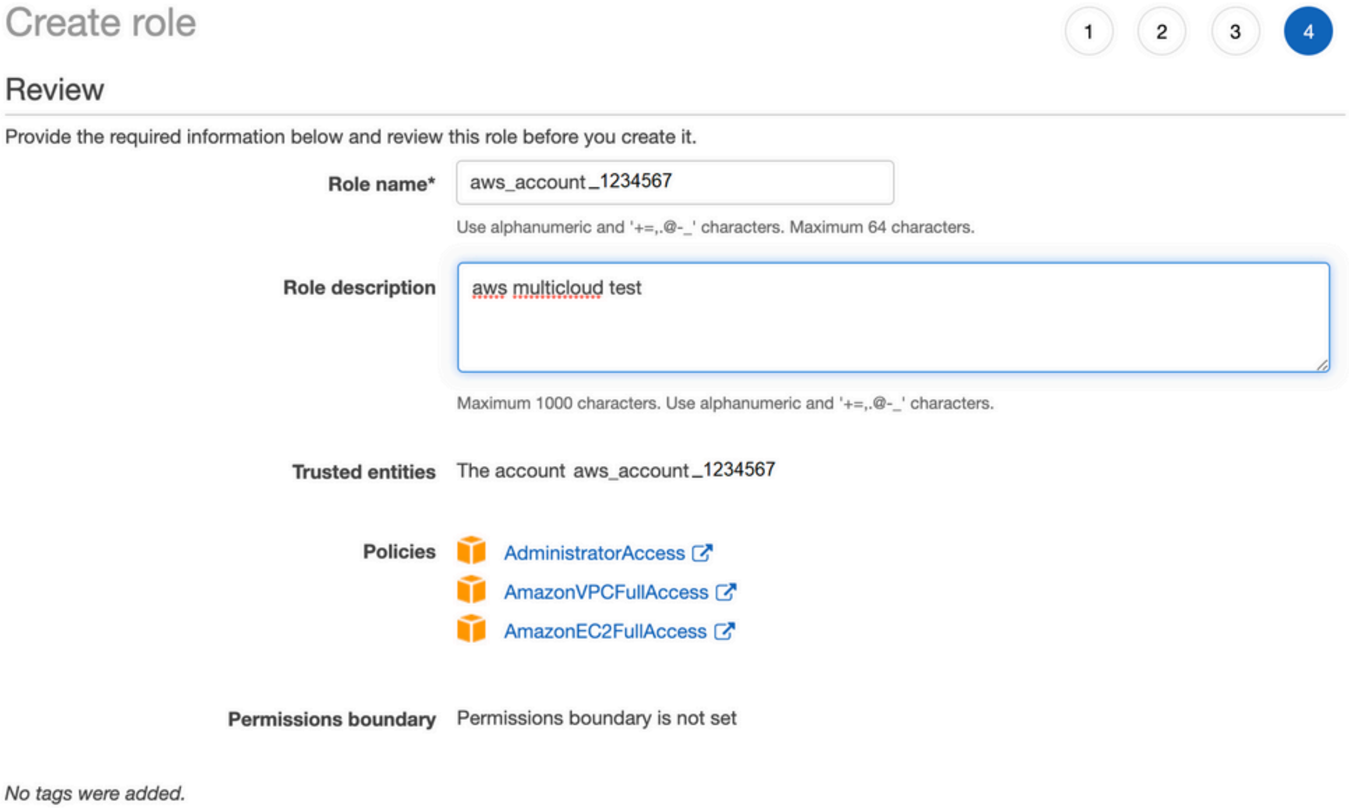
Showing 32 results

		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. Skip the tags.

9. Review the last page and name the role. Post the creation of **ROLE** and copy the **ARN** from the **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

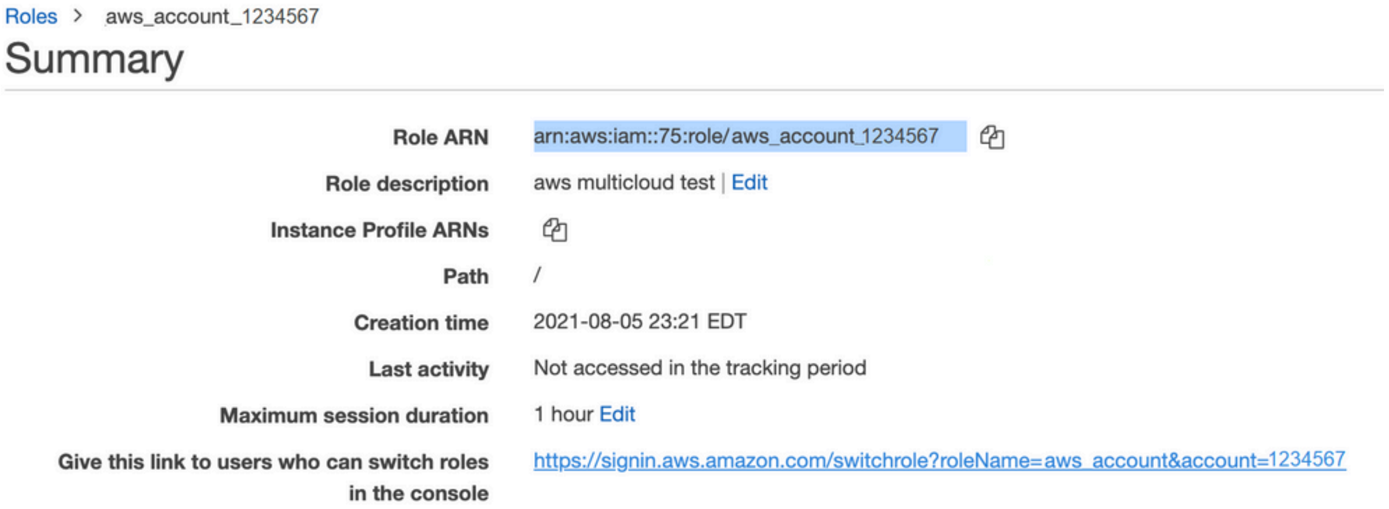
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Trusted entities The account aws_account_1234567

Policies AdministratorAccess
AmazonVPCFullAccess
AmazonEC2FullAccess

Permissions boundary Permissions boundary is not set

No tags were added.



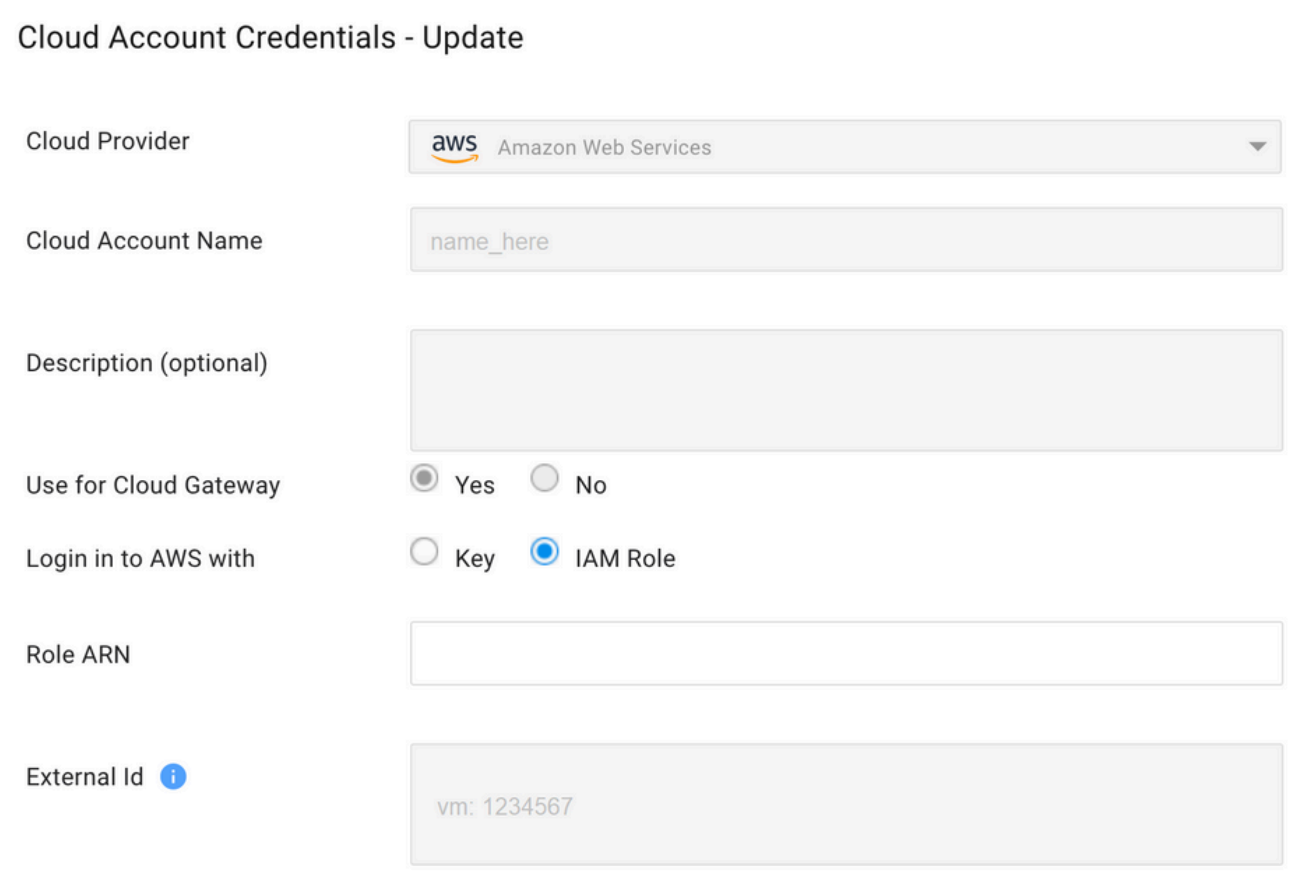
Summary

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. Ensure that the syntax under the **"Trust Relationship > Edit Relationship"**matches this JSON example (with the values you set):

```
{ "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. Copy the **ARN** from **AWS** and fill in the details on the **vManage** multi-cloud page.



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

The "**/var/log/nms/containers/cloudagent-v2/cloudagent-v2.log**" file has valuable messages (with the values you set):

```
[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==",
```

Reference

Cisco_Cloud_onRamp_for_IaaS_AWS_Version2.html