使用IAM配置AWS多雲vManage帳戶

目錄

簡介

本文檔介紹如何解決嘗試使用IAM帳戶實現多雲自動化時出現的信任問題。

背景

當您在AWS TGW和您的公司AWS賬戶中使用思科多雲功能時，存在信任問題。這是因為唯一的 **Account ID** 與 **vManage EC2** 例項。

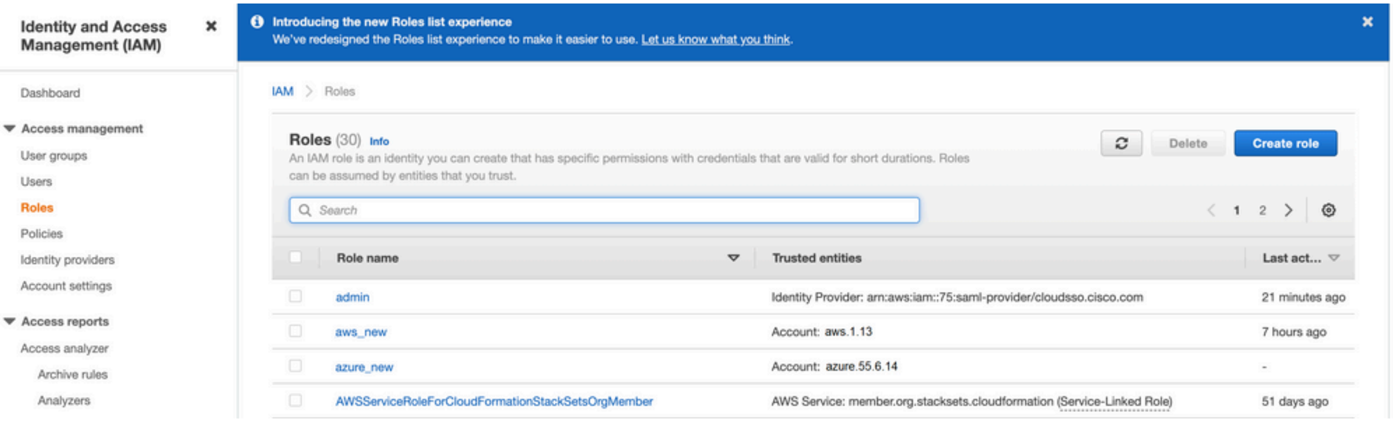
問題

當您將IAM帳戶用於多雲自動化時，它會導致信任問題。

解決方案

要解決此問題：

1. 導航至 **AWS > Identity and Access Management (IAM)** 並建立新的 **ROLE** 或列出的 **ROLE.**
2. 在 **AWS** 門戶，輸入 **IAM** 在搜尋欄中 **IAM** 開啟。
3. 從側面板導航到 **Roles** 然後選擇 **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.

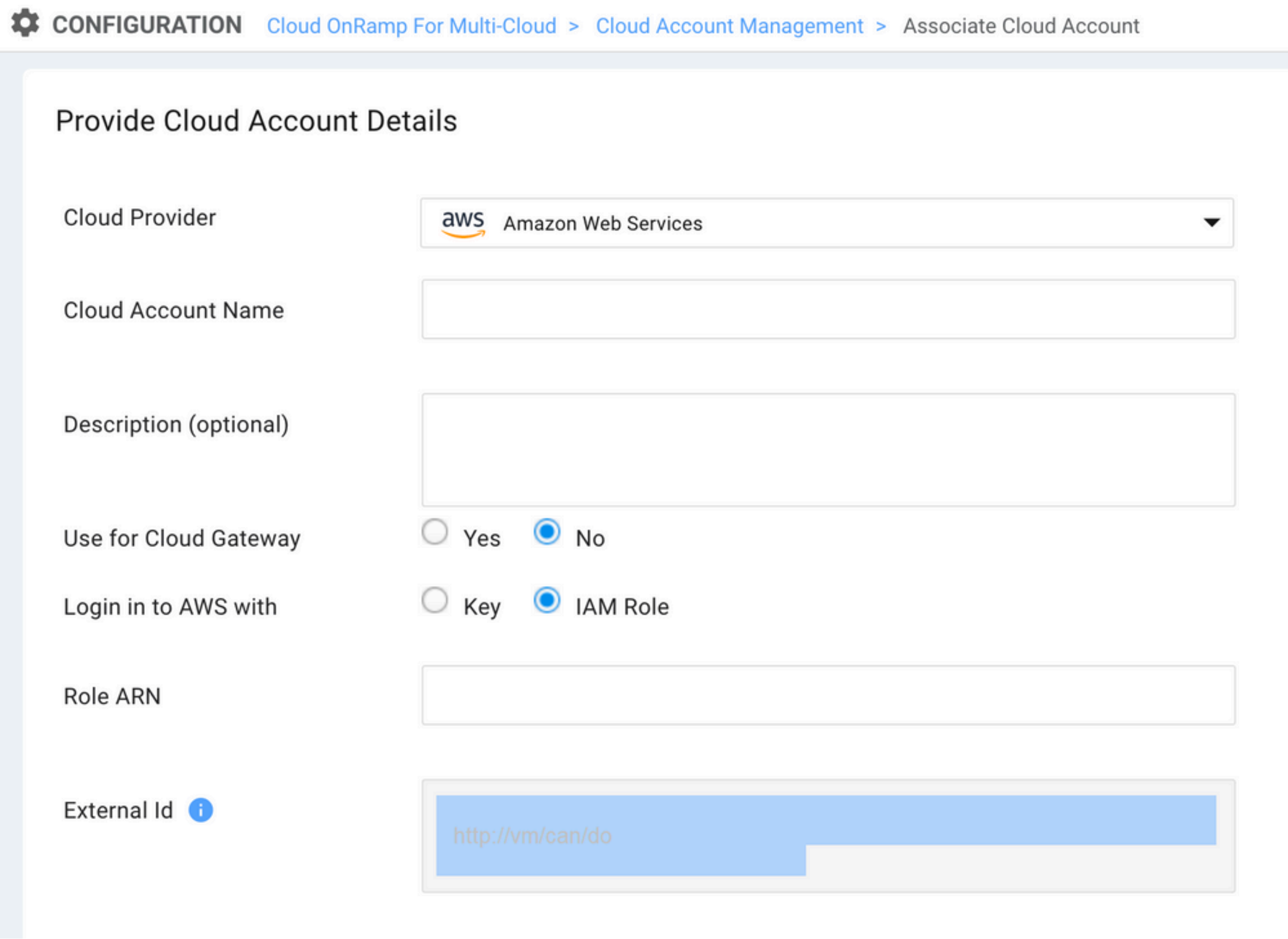
Roles (30)
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

	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.選擇 **Another AWS Account** 作為選項。

5. **Account ID** 是 **AWS Account** 擁有 **vManage EC2** 例項已生成。對於思科託管帳戶，帳戶ID為「2002388880647」。(這不是您自己的 **AWS Account ID.**)請參閱本文結尾的參考文獻。

6.選中覈取方塊 **"External ID"** 並在下面輸入一個值 **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:

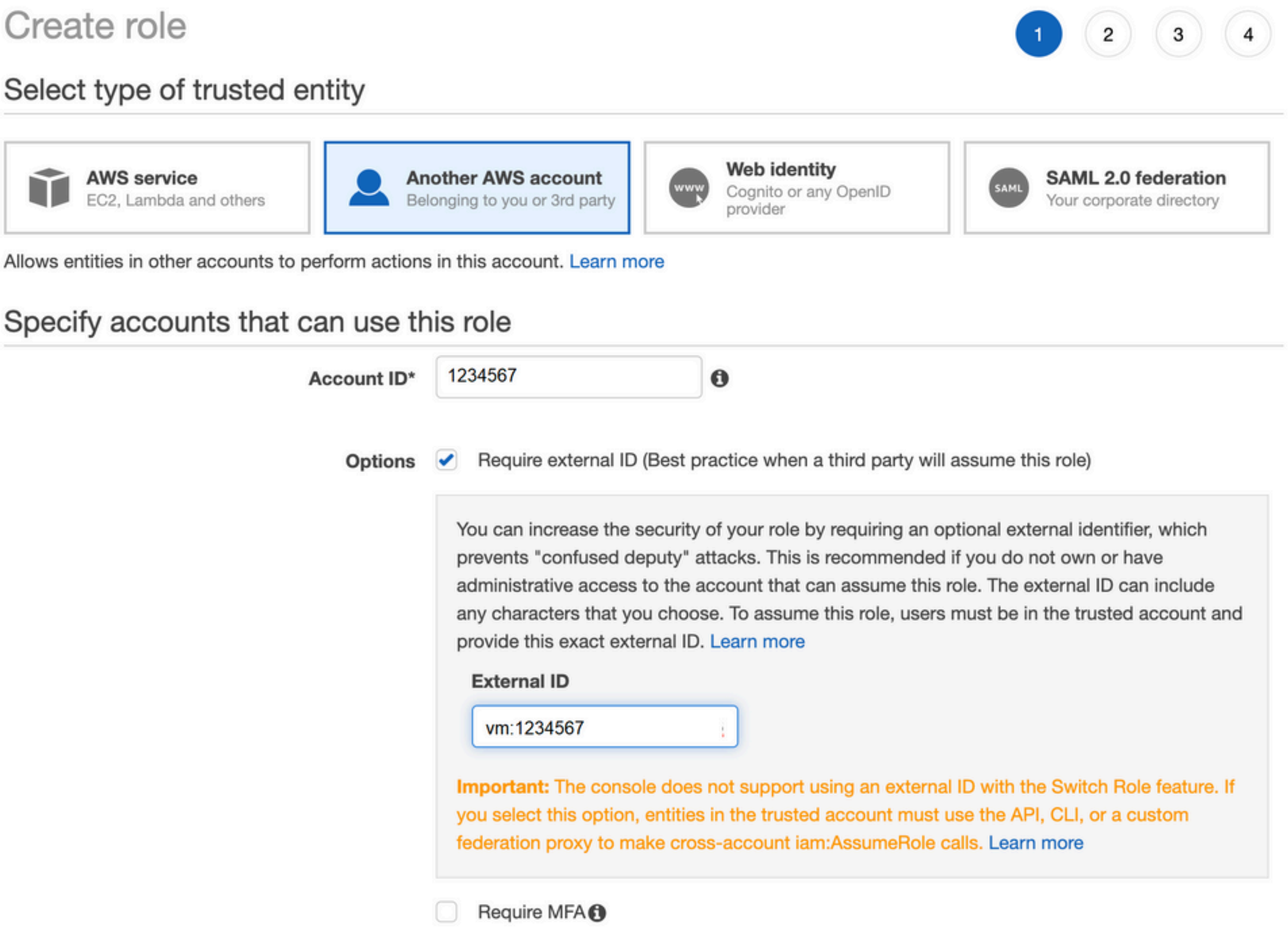
Description (optional):

Use for Cloud Gateway: ○ Yes ● No

Login in to AWS with: ○ Key ● IAM Role

Role ARN:

External Id: http://vm/can/do



Create role

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* 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

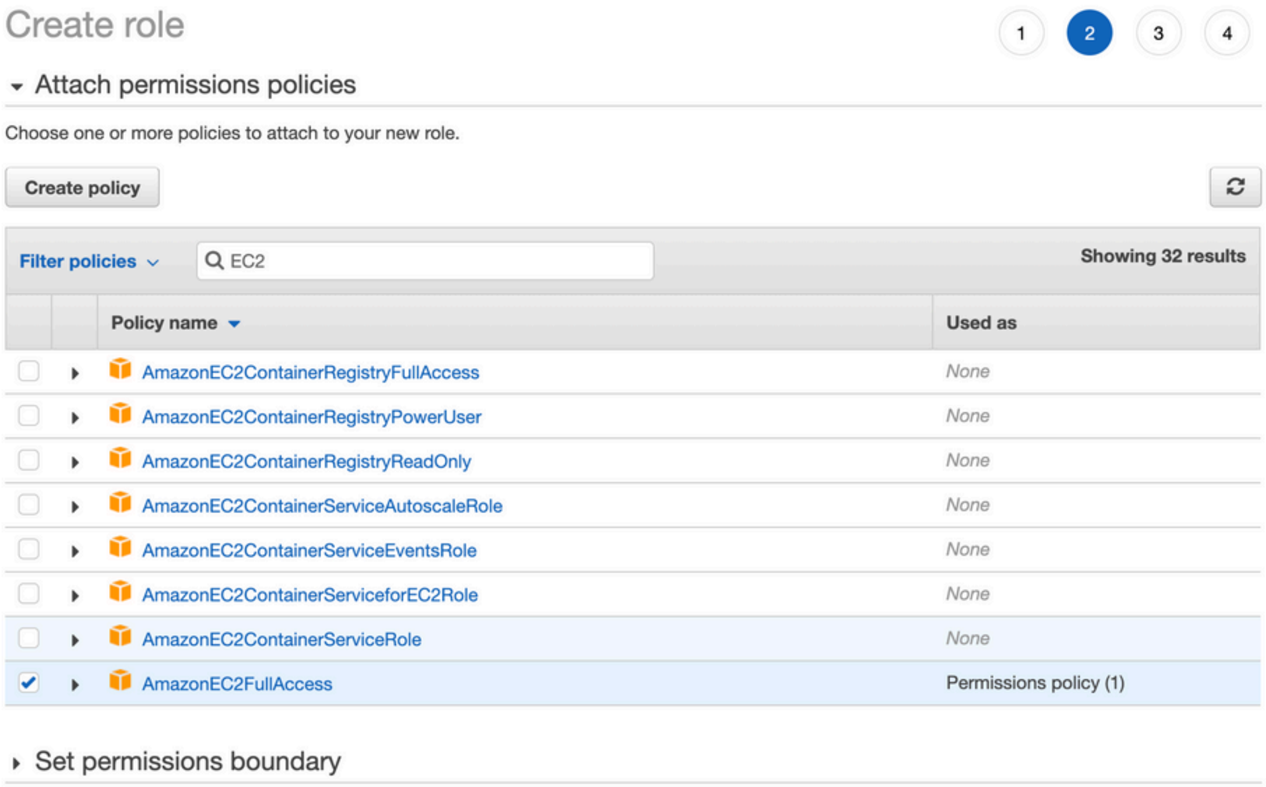
External ID

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.設定許可權。



Create role

1 2 3 4

Attach permissions policies

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

Create policy

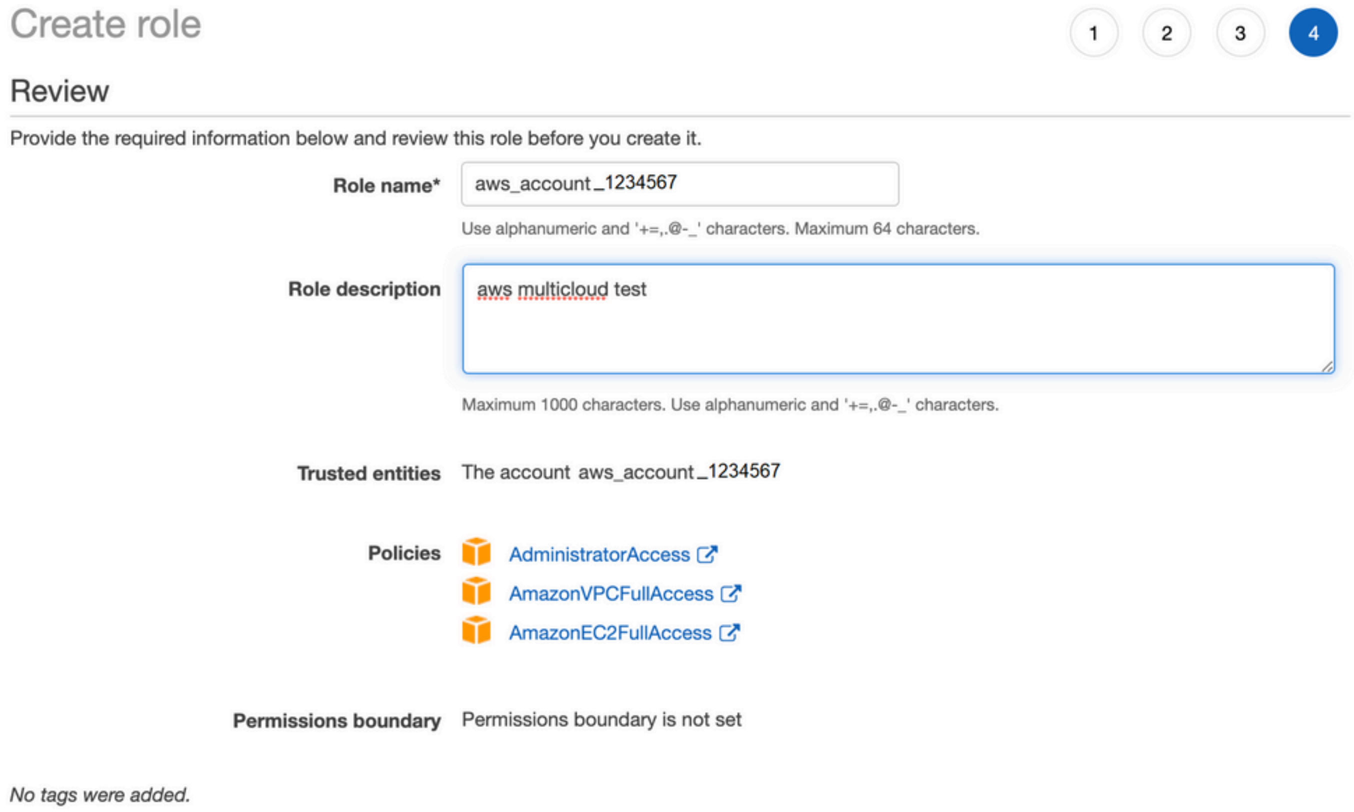
Filter policies EC2 Showing 32 results

		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. 跳過標籤。

9. 檢視最後一頁並命名角色。發佈建立 **ROLE** 並複製 **ARN** 從 **AWS** 門戶。



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

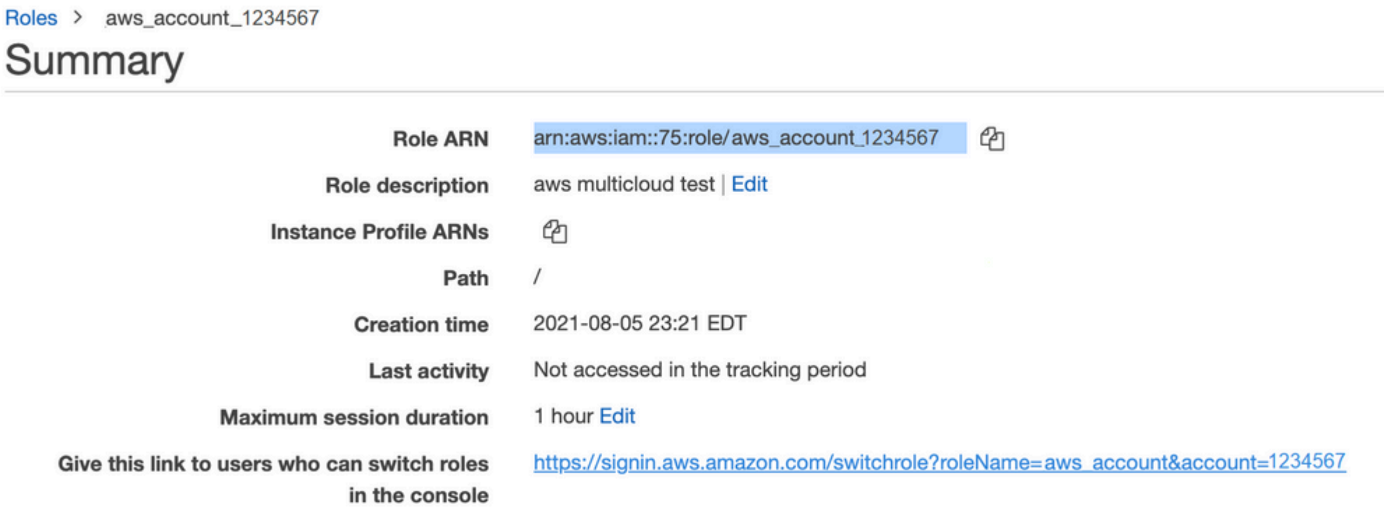
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

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

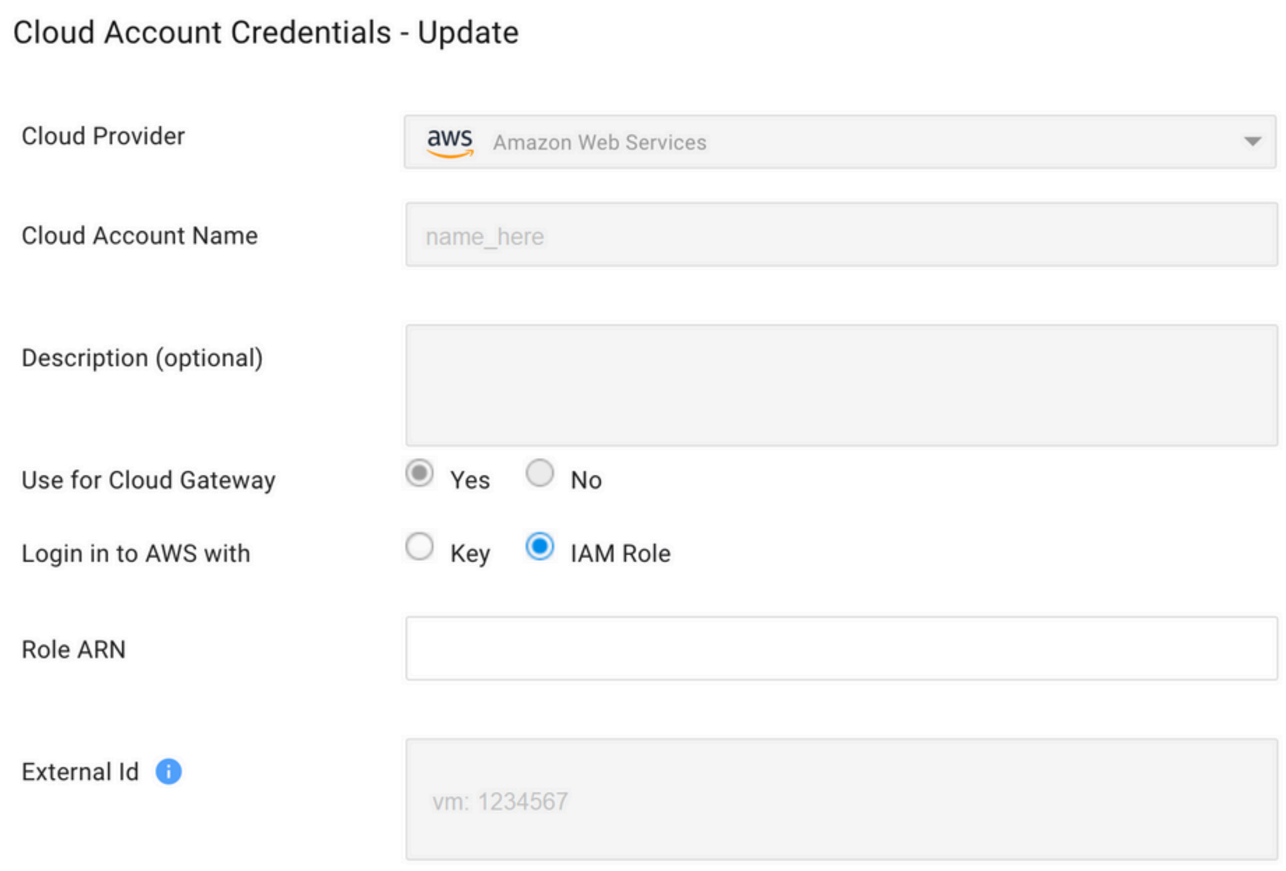
Maximum session duration 1 hour Edit

Give this link to users who can switch roles in the console https://signin.aws.amazon.com/switchrole?roleName=aws_account&account=1234567

10. 確保 **"Trust Relationship > Edit Relationship"**匹配此JSON示例（使用您設定的值）：

```
{ "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. 複製 **ARN** 自 **AWS** 並填寫 **vManage** 多雲頁面。



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

其"**/var/log/nms/containers/cloudagent-v2/cloudagent-v2.log**" 檔案包含有價值的消息（使用您設定的值）：

```
[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==",
```

參考

[Cisco_Cloud_onRamp_for_IaaS_AWS_Version2.html]