Configurer le compte vManage multicloud AWS avec IAM

Contenu

Introduction

Ce document décrit comment résoudre les problèmes de confiance qui se produisent lorsque vous essayez d'utiliser le compte IAM pour l'automatisation multi-cloud.

Fond

Lorsque vous utilisez la fonctionnalité multicloud de Cisco avec AWS TGW et votre compte AWS d'entreprise, il y a des problèmes de confiance. C'est parce que la société unique **Account ID** est différent de la **vManage EC2** dans AWS.

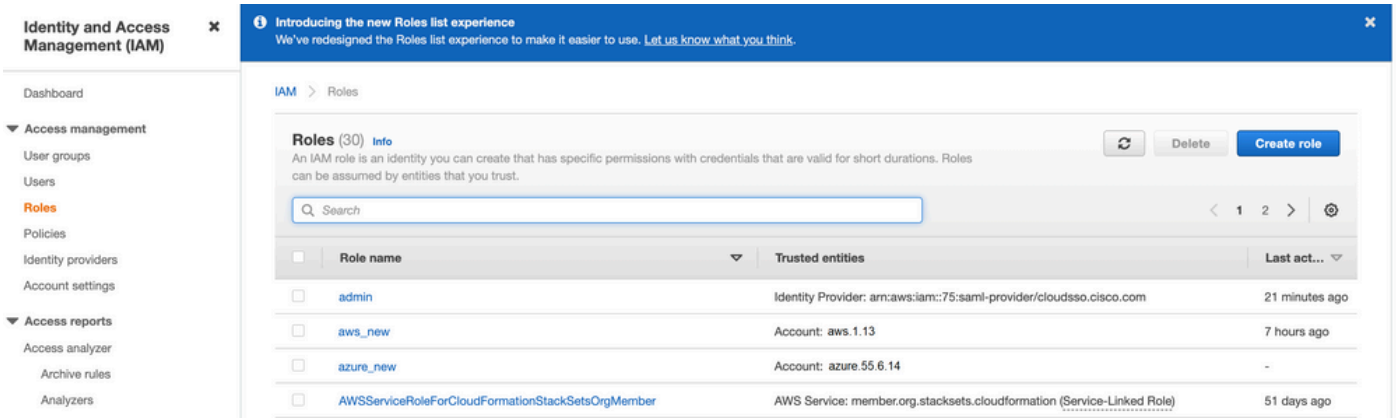
Problème

Lorsque vous utilisez le compte IAM pour l'automatisation multi-cloud, cela entraîne un problème de confiance.

Solution

Pour résoudre ce problème :

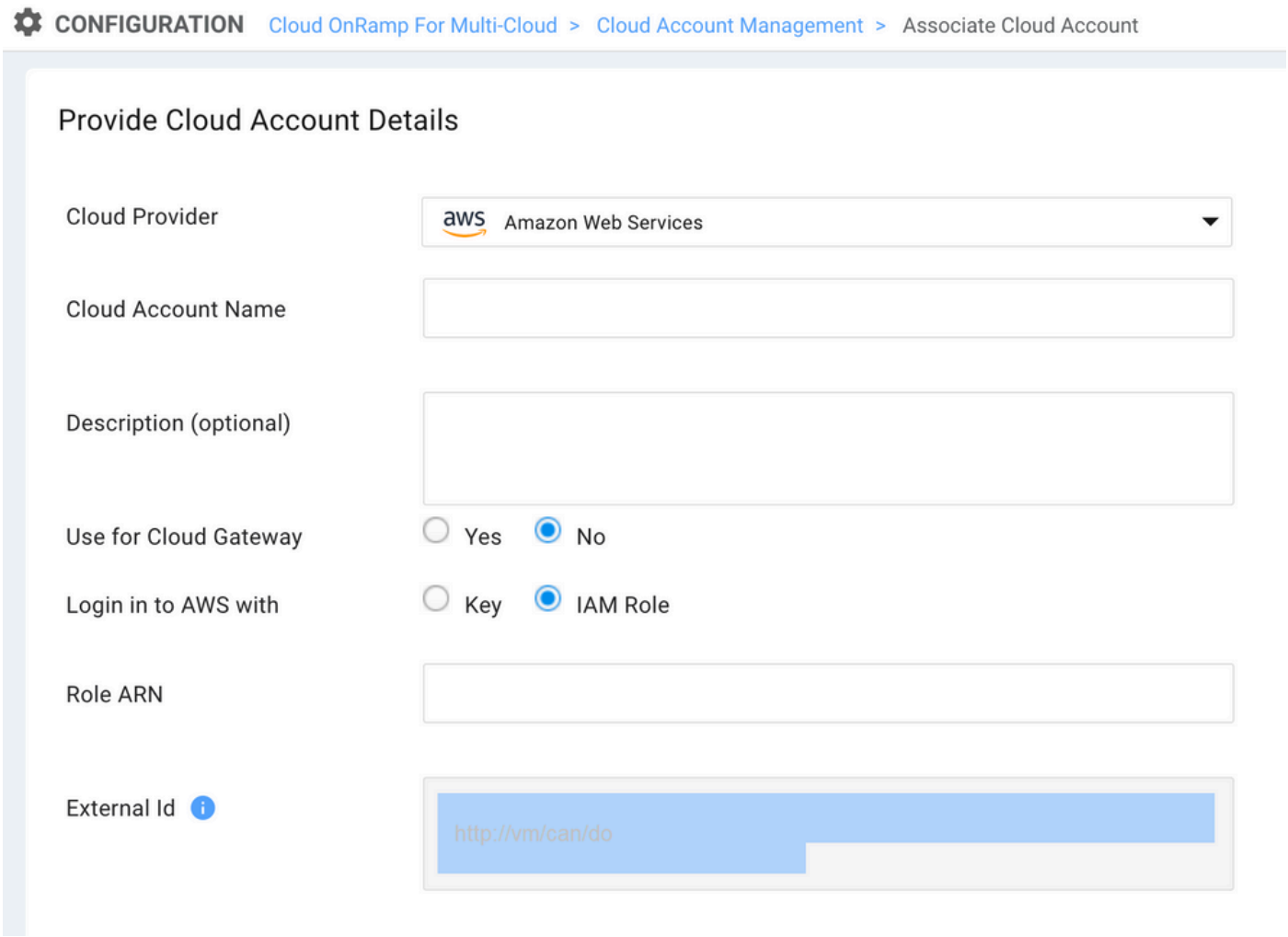
1. Naviguez jusqu'à **AWS > Identity and Access Management (IAM)** et créer un nouveau **ROLE** ou une autre liste **ROLE.**
2. Sur le **AWS** portail, saisissez **IAM** dans la barre de recherche. **IAM** s'ouvre.
3. Àpartir du panneau latéral, accédez à **Roles** puis sélectionnez **Create New.**

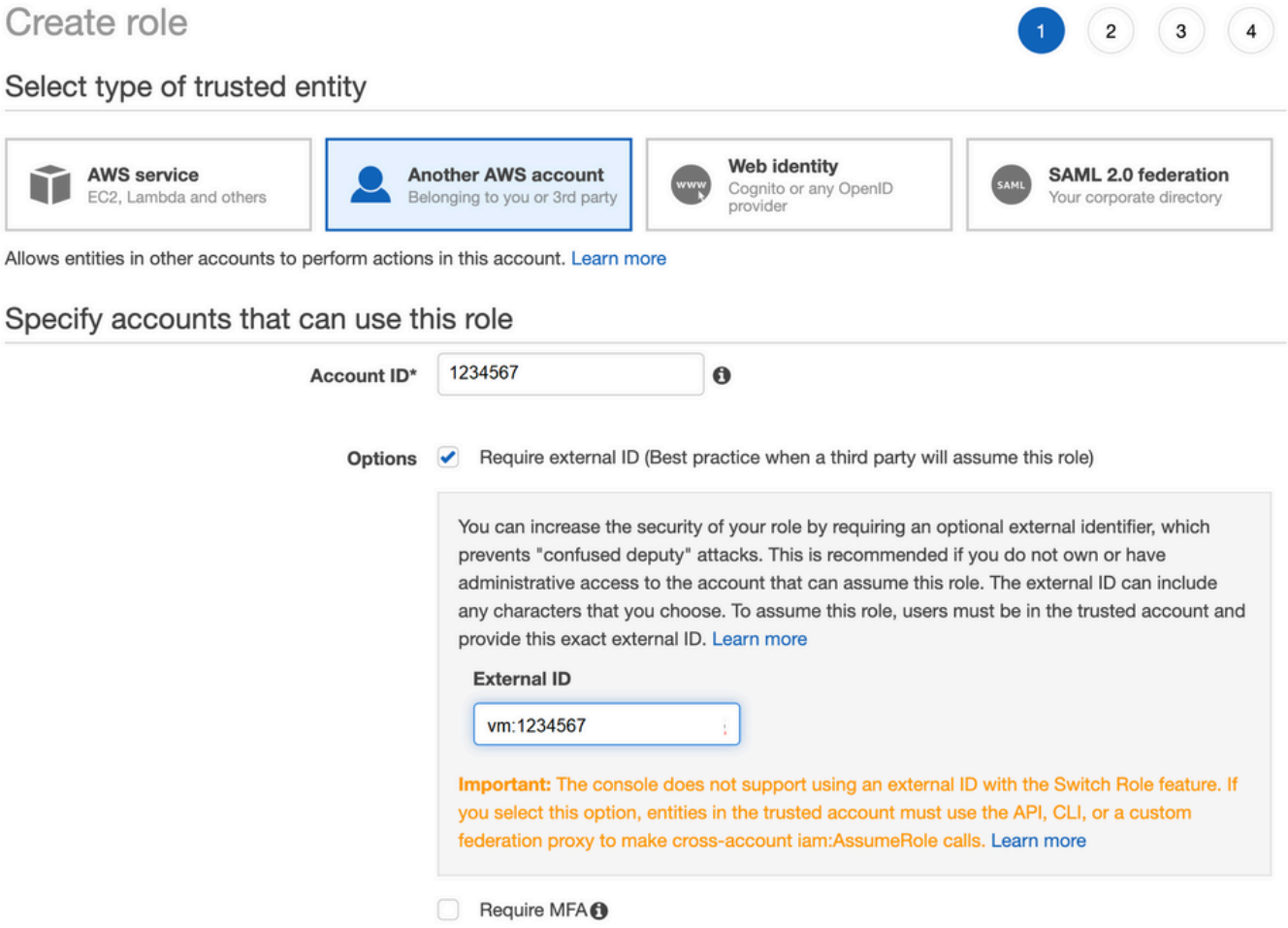


4. Sélectionnez le **Another AWS Account** en option.

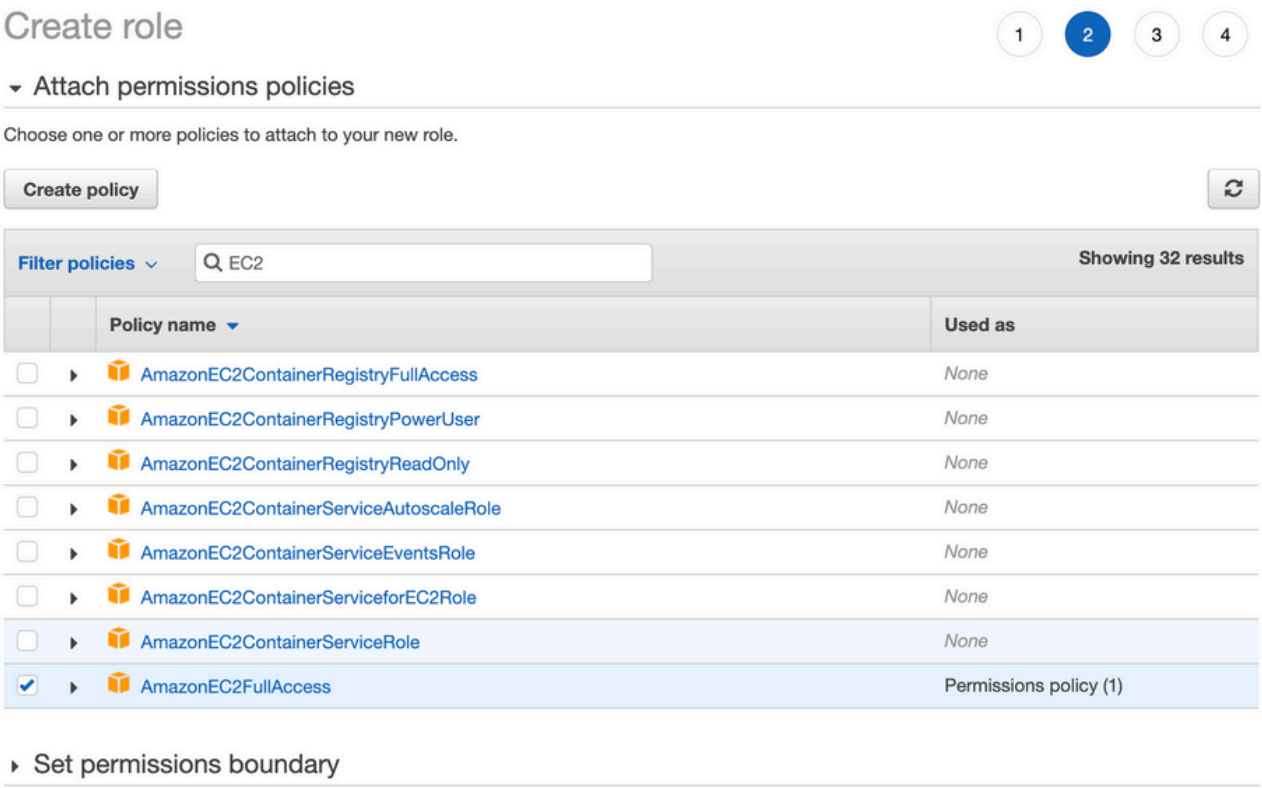
5. La **Account ID** est le **AWS Account** et dispose de la **vManage EC2** instance créée. Pour les comptes hébergés Cisco, l'ID de compte est « 2002388880647 ». (Ce n'est PAS le vôtre **AWS Account ID**.) Voir la référence à la fin de cet article.

6. Cochez la case correspondant à **"External ID"** et saisissez une valeur sous **vManage > Cloud onRamp for multi-cloud > Account Management > Add AWS Account.**



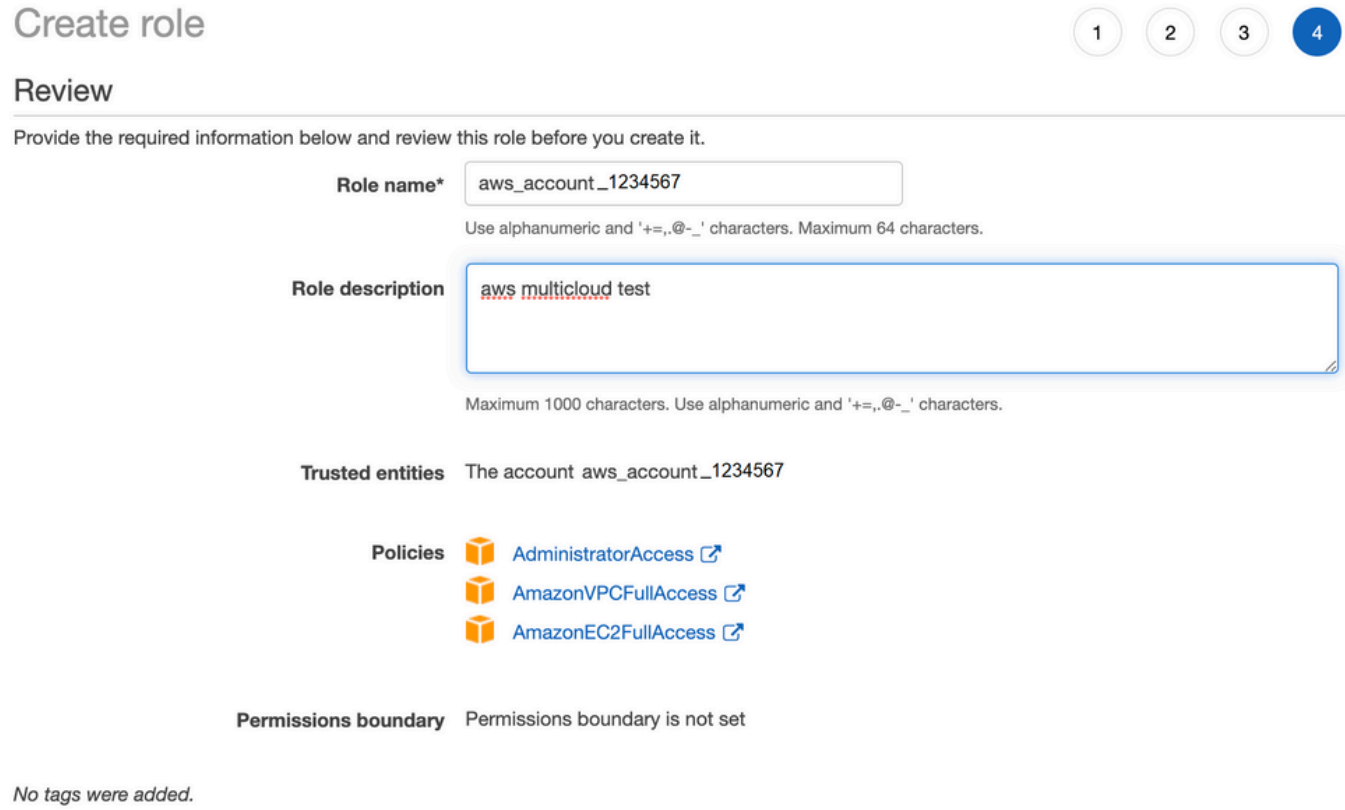


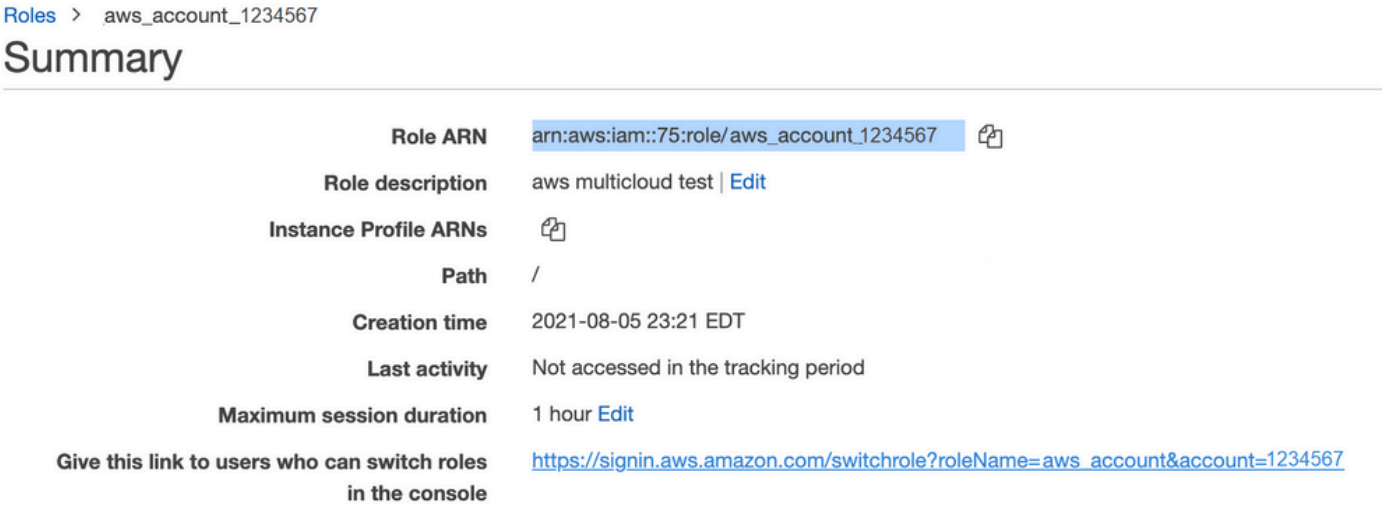
7. Définissez les autorisations.



8. Ignorez les balises.

9. Vérifiez la dernière page et nommez le rôle. Publier la création de **ROLE** et copiez le **ARN** a partir des versions **AWS** portail.

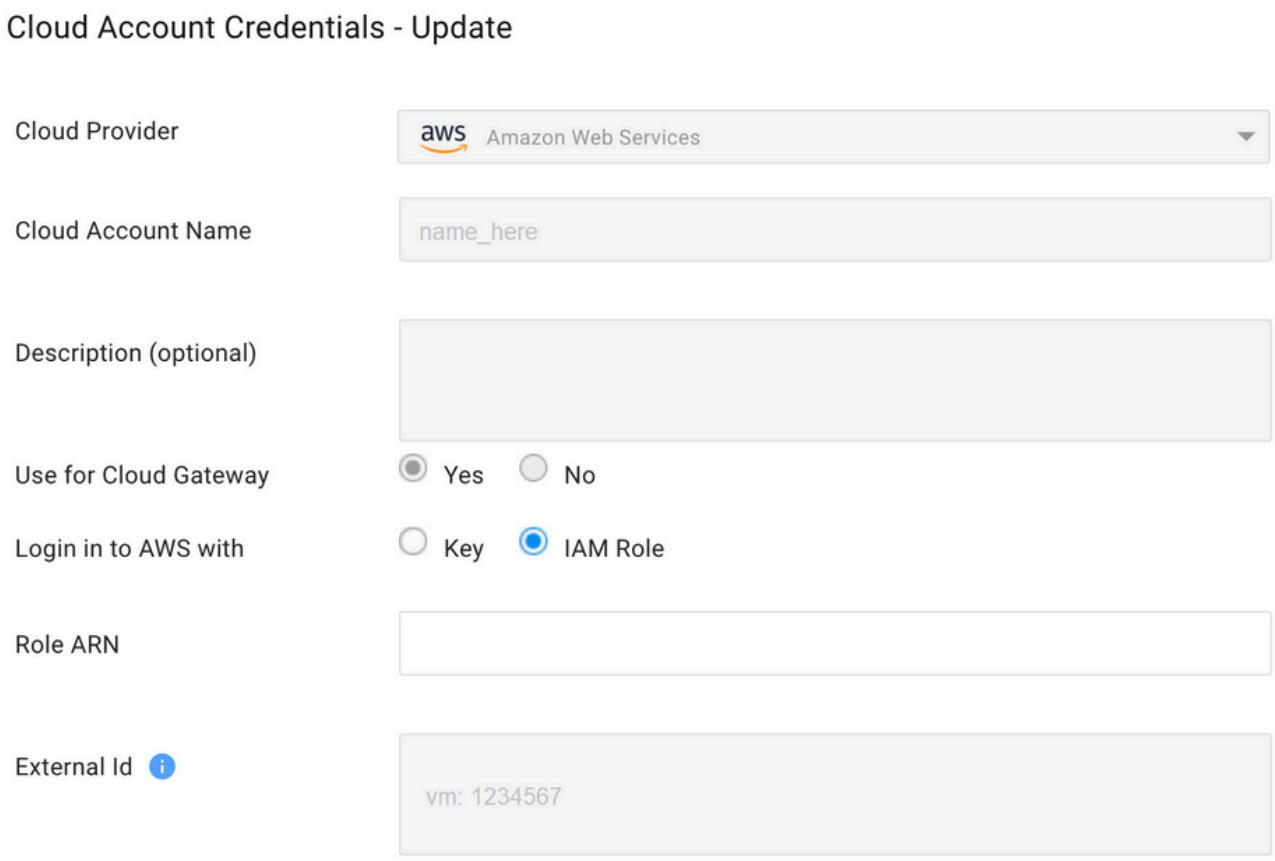




10. Vérifiez que la syntaxe sous le **"Trust Relationship > Edit Relationship"**correspond à cet exemple JSON (avec les valeurs que vous avez définies) :

```
{ "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. Copiez le **ARN** expéditeur **AWS** et renseignez les détails sur la **vManage** page multi-cloud.



Les"**/var/log/nms/containers/cloudagent-v2/cloudagent-v2.log**" contient des messages précieux (avec les valeurs que vous définissez) :

```
[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==",
```

Référence

[Cisco_Cloud_onRamp_for_IaaS_AWS_Version2.html]