Configurer le compte vManage multicloud AWS avec IAM

Table des matières

Introduction

Fond

Problème

Solution

Référence

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. Cela est dû au fait que la société unique **Account ID** est différente de l'**vManage EC2**instance dans AWS.

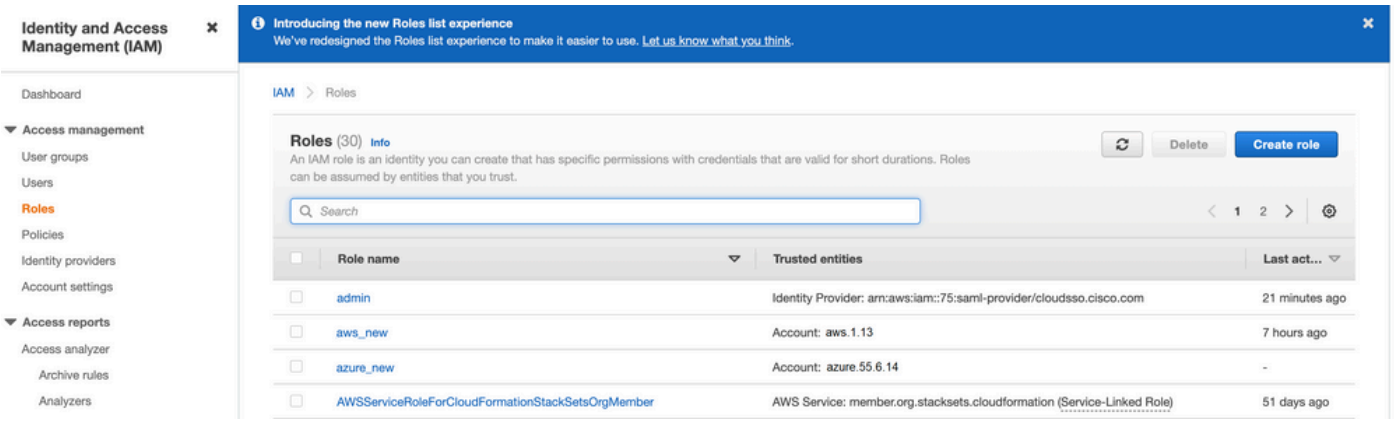
Problème

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

Solution

Voici la marche à suivre pour résoudre ce problème :

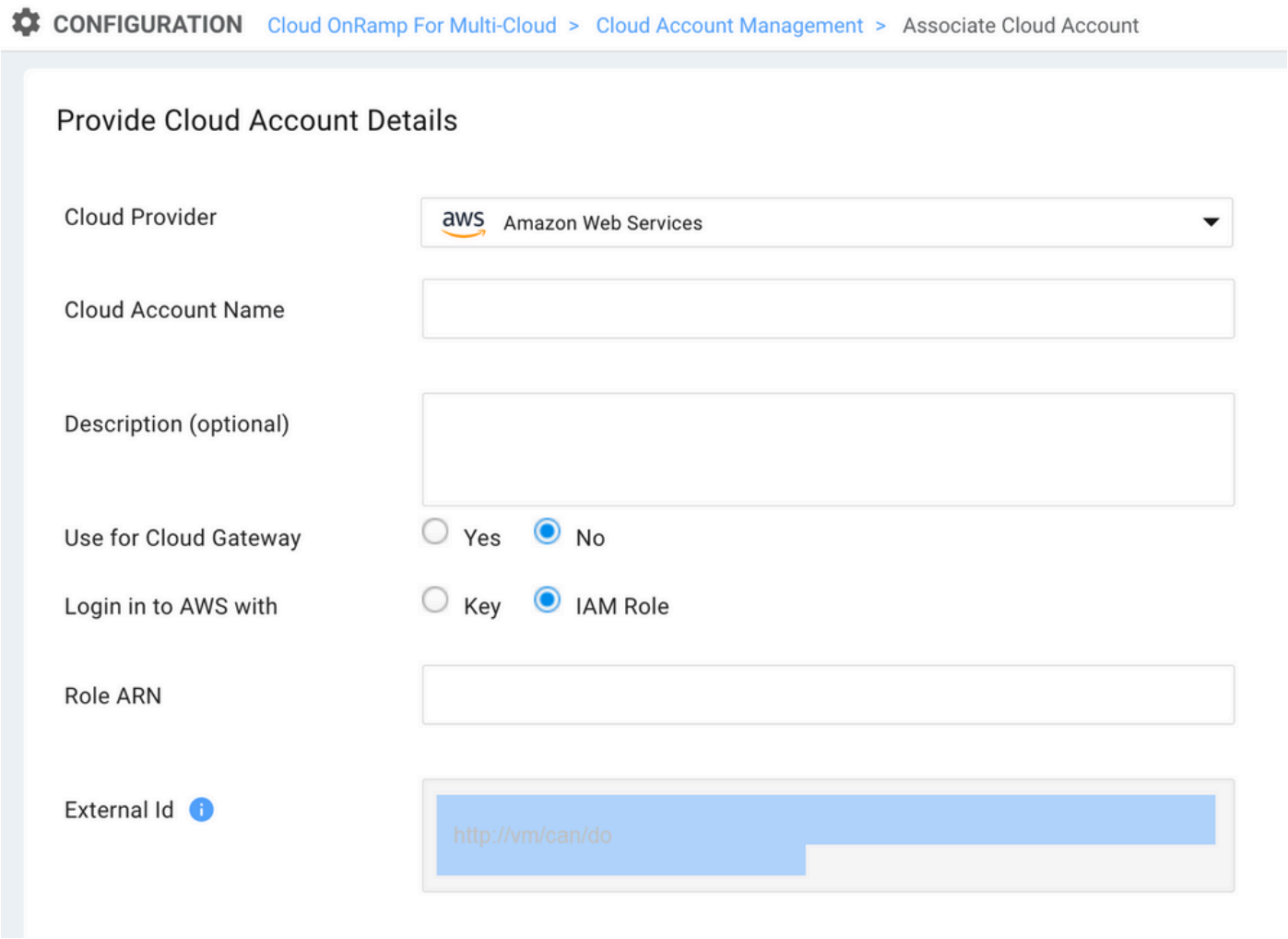
1. Naviguez jusqu'à **AWS** > **Identity and Access Management (IAM)** et créez un nouveau **ROLE** ou un autre élément répertorié **ROLE.**
2. Sur le **AWS** portail, entrez **IAM** dans la barre de recherche. Le **IAM** s'ouvre.
3. Dans le panneau latéral, accédez à **Roles** , puis sélectionnez **Create New.**



4. Sélectionnez l' **Another AWS Account** en tant qu'option.

5. L'**Account ID**instance est la **AWS Account** et l'**vManage EC2**instance est construite. 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 pour **"External ID"** et entrez une valeur sous **vManage** > **Cloud onRamp for multi-cloud** > **Account Management** > **Add AWS Account.**



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. Définissez les autorisations.

Create role

1 2 3 4

Attach permissions policies

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

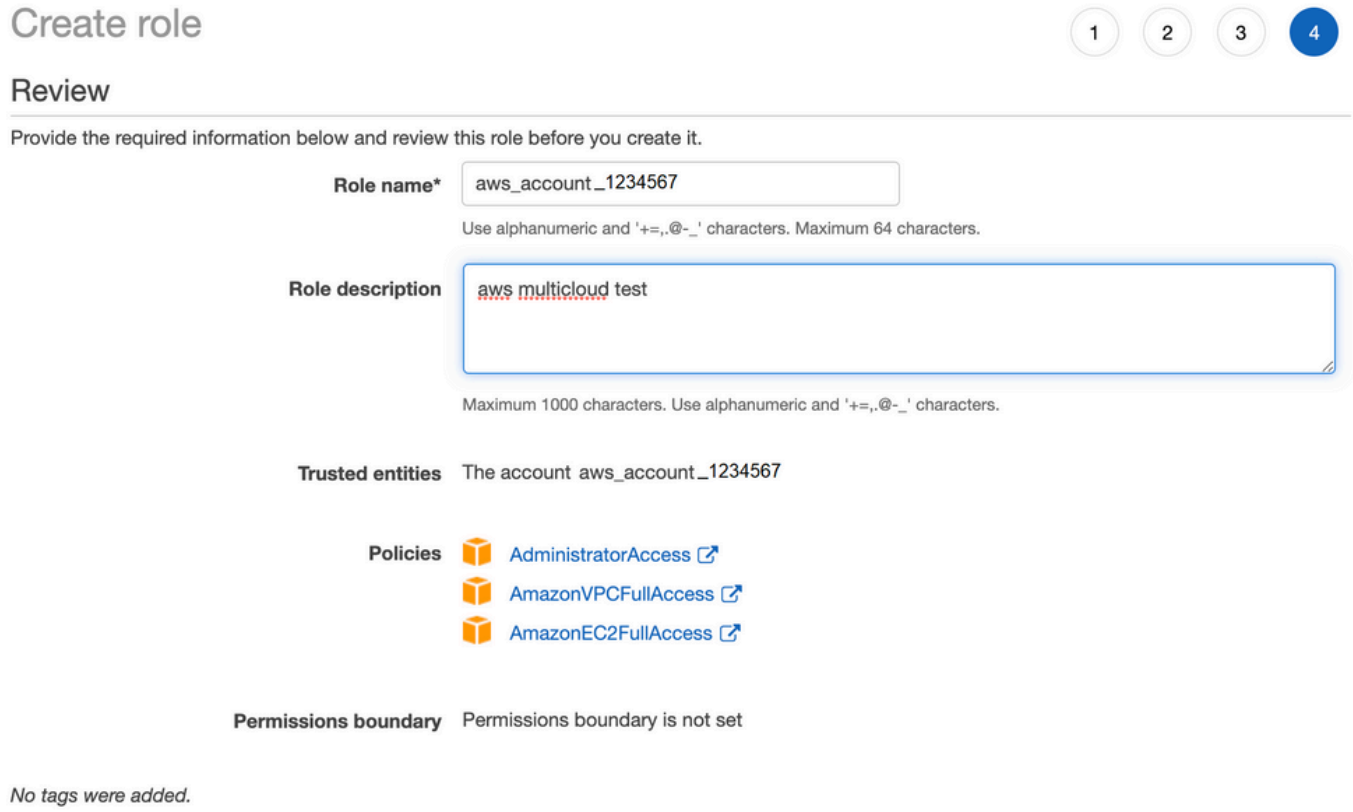
Create policy

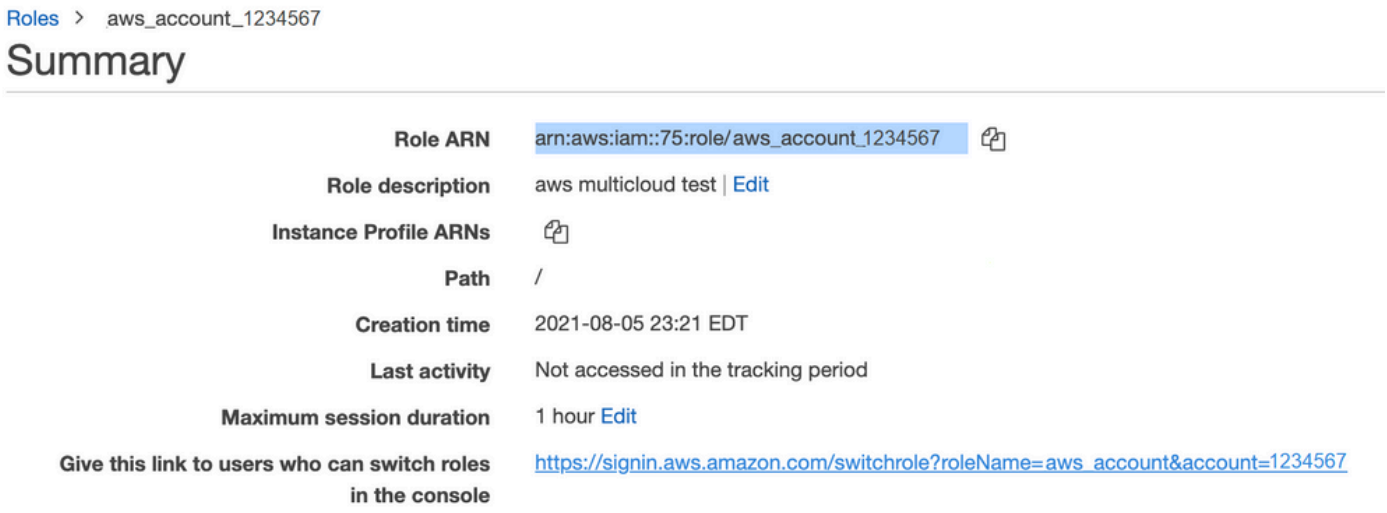
Filter policies EC2 Showing 32 results

	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. Ignorez les balises.
9. Vérifiez la dernière page et nommez le rôle. Publiez la création de ROLE et copiez le contenu ARN à partir du AWS portail.



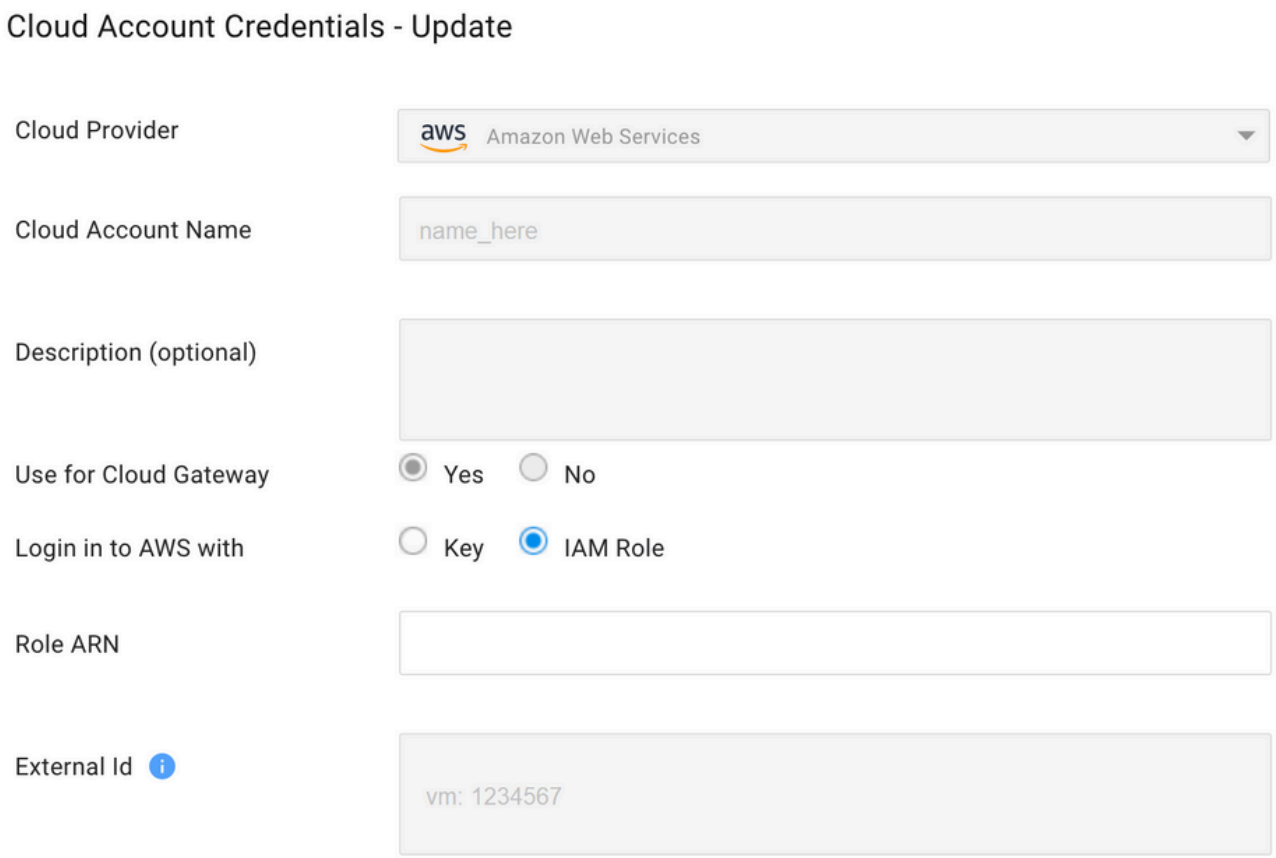


10. Assurez-vous que la syntaxe sous le "Trust Relationship > Edit Relationship"correspond à cet exemple JSON (avec les valeurs que vous définissez) :

```
{
  "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** de **AWS** et renseignez les détails sur la page **vManage** multi-cloud.



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

```
[2021-08-06T02:47:07UTC+0000:140360670770944:INFO:ca-v2:grpc_service.py:432] Returning ValidateAccountI
  "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+2GkdeyOIyTU
```


Référence

[Cisco_Cloud_onRamp_for_IaaS_AWS_Version2.html]

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d’un service mondial permettant à nos utilisateurs d’obtenir le contenu d’assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.