

AWS Multi-cloud vManager-account met IAM configureren

Inhoud

[Inleiding](#)

[Achtergrond](#)

[Probleem](#)

[Oplossing](#)

[Referentie](#)

Inleiding

Dit document beschrijft hoe u vertrouwenskwesaties kunt oplossen die zich voordoen wanneer u de IAM-account voor multi-cloud automatisering probeert te gebruiken.

Achtergrond

Wanneer u de Cisco multi-cloud optie met AWS TGW en uw AWS-account van het bedrijf gebruikt, zijn er vertrouwensproblemen. Dat komt omdat het unieke bedrijf Account ID verschilt van de vManage EC2 Bijvoorbeeld in AWS.

Probleem

Wanneer u de IAM-account gebruikt voor multi-cloud automatisering, veroorzaakt het een vertrouwenskwesatie.

Oplossing

U lost dit probleem als volgt op:

1. Navigeren in om **AWS > Identity and Access Management (IAM)** en een nieuw **ROLE** of een andere **ROLE**.
2. Op het **AWS** portaal, invoeren **IAM** in de zoekbar. **IAM** geopend.
3. Van het zijpaneel, navigeer naar **Roles** en selecteer vervolgens **Create New**.

Identity and Access Management (IAM)

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.](#)

IAM > Roles

Roles (30) Info Refresh Delete Create role

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.

Search

<input type="checkbox"/>	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. Selecteer de **Another AWS Account** als optie.

5. De **Account ID** de **AWS Account** en de **vManage EC2 Instantie** gebouwd. Voor Cisco Hosted-accounts is de account-ID "20023880647". (Dit is NIET uw eigen account) **AWS Account ID.**) Zie Referentie aan het einde van dit artikel.

6. Controleer het vakje voor "**External ID**" en voer een waarde in onder **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

Cloud Account Name

Description (optional)

Use for Cloud Gateway Yes No

Login in to AWS with Key IAM Role

Role ARN

External ID i

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. Stel permissies in.

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. Naar de tags.

9. Bekijk de laatste pagina en noem de rol. De oprichting van **ROLE** en kopieert het **ARN** van **AWS** portaal.

Create role



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

Role ARN	arn:aws:iam::75:role/aws_account_1234567 ↗
Role description	aws multcloud 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. Zorg ervoor dat de syntaxis onder de "Trust Relationship > Edit Relationship" Past dit JSON voorbeeld aan (met de waarden die u instelt):

```
{ "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. Het bestand kopiëren **ARN** van **AWS** en de gegevens op de **vManage** pagina met meerdere wolken.

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"/>

Het "/var/log/nms/containers/cloudagent-v2/cloudagent-v2.log" bestand bevat waardevolle berichten (met de door u ingestelde waarden):

```
[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==" ,
```

Referentie

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