

Konfiguration eines AWS Multi-Cloud vManage-Kontos mit IAM

Inhalt

[Einleitung](#)

[Hintergrund](#)

[Problem](#)

[Lösung](#)

[Referenz](#)

Einleitung

In diesem Dokument wird beschrieben, wie Vertrauensprobleme behoben werden, die bei der Verwendung des IAM-Kontos für die Multi-Cloud-Automatisierung auftreten.

Hintergrund

Wenn Sie die Cisco Multi-Cloud-Funktion mit AWS TGW und Ihrem AWS-Konto in Ihrem Unternehmen nutzen, treten Vertrauensprobleme auf. Das liegt daran, dass das einzigartige Unternehmen `Account ID` unterscheidet sich von `vManage EC2` Instanz in AWS.

Problem

Wenn Sie das IAM-Konto für die Multi-Cloud-Automatisierung verwenden, führt dies zu einem Vertrauensproblem.

Lösung

So beheben Sie dieses Problem:

1. Navigieren Sie zu **AWS > Identity and Access Management (IAM)** und eine neue **ROLE** oder anderen aufgeführten **ROLE**.
2. Auf dem **AWS** Portal, eingeben **IAM** in der Suchleiste. Die **IAM** öffnet.
3. Navigieren Sie auf der Seitenleiste zu **Roles** und dann **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. Wählen Sie **Another AWS Account** als Option.

5. Die **Account ID** ist **AWS Account** und verfügt über die **vManage EC2 Instanz** erstellt. Für gehostete Cisco Kunden lautet die Konto-ID "2002388880647". (Dies ist NICHT Ihre eigene ID.) **AWS Account ID**.) Siehe Verweis am Ende dieses Artikels.

6. Aktivieren Sie das Kontrollkästchen für "**External ID**" und geben Sie einen Wert unter **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. Berechtigungen festlegen.









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. Überspringen Sie die Tags.

9. Überprüfen Sie die letzte Seite, und geben Sie der Rolle einen Namen. Nach der Erstellung **ROLE** und kopieren Sie **ARN** von **AWS Portal**.

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 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. Stellen Sie sicher, dass die Syntax unter "**Trust Relationship > Edit Relationship**" entspricht diesem JSON-Beispiel (mit den von Ihnen festgelegten Werten):

```
{ "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. Kopieren Sie **ARN** von **AWS** und geben Sie die Einzelheiten auf der **vManage Multi-Cloud**-Seite.

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"/> |

Die Fehlermeldung `/var/log/nms/containers/cloudagent-v2/cloudagent-v2.log` enthält nützliche Nachrichten (mit den von Ihnen festgelegten Werten):

```
[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==" ,
```

Referenz

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