

IAMを使用したAWS Multi-cloud vManageアカウントの設定

内容

[概要](#)

[背景](#)

[問題](#)

[解決方法](#)

[参考](#)

概要

このドキュメントでは、マルチクラウド自動化にIAMアカウントを使用するときに発生する信頼の問題を解決する方法について説明します。

背景

AWS TGWと会社のAWSアカウントでシスコのマルチクラウド機能を使用すると、信頼の問題が発生します。それは、ユニークな企業だからです Account ID は、vManage EC2 AWSのインスタンスです。

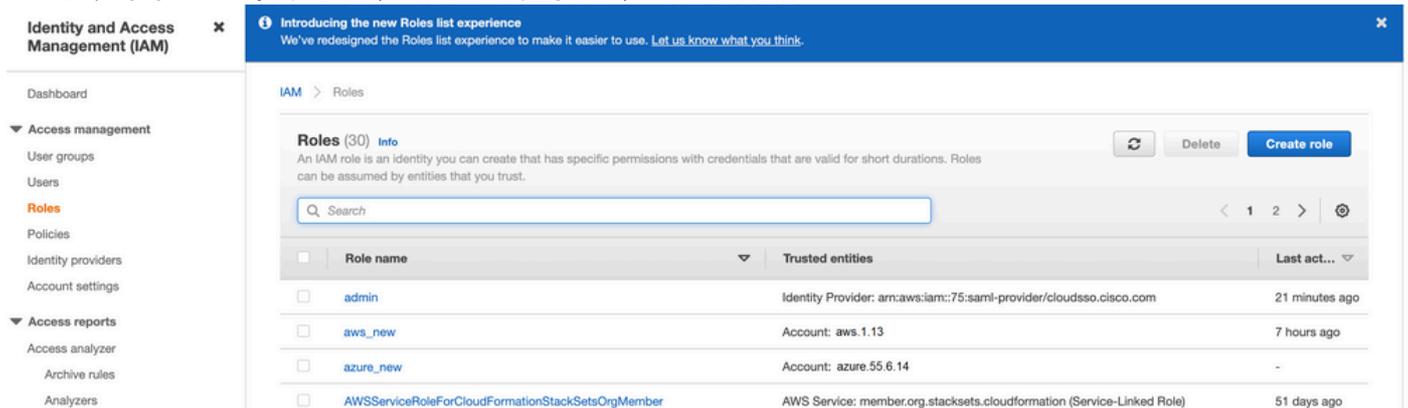
問題

マルチクラウドの自動化にIAMアカウントを使用すると、信頼問題が発生します。

解決方法

この問題を解決するには：

1. 移動先 AWS > Identity and Access Management (IAM) 新しい ROLE その他のリスト ROLE.
2. Cisco IOSソフトウェア AWS ポータル、入力 IAM をクリックします。IAM が開きます。
3. サイド・パネルから、Roles を選択し、Create New.



The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with 'Roles' highlighted. The main content area displays a list of roles. At the top, there is a notification banner about the new Roles list experience. Below that, the 'Roles (30)' section includes a search bar and a table of roles.

<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. Another AWS Account オプションとして使用できます。

5. Account ID は AWS Account また、 vManage EC2 インスタンスが構築されました。Cisco Hostedアカウントの場合、アカウントIDは「2002388880647」です（お客様のアカウントではありません）。AWS Account ID.)この記事の最後にある「参考資料」を参照してください。

6. チェックボックスをオンにして、"External ID" の下に値を入力します。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 ℹ️

http://vm/can/do

Create role

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. アクセス許可を設定します。

Create role

▼ 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. タグをスキップします。

9. 最後のページを確認し、ロールに名前を付けます。~の作成を投稿する **ROLE** をコピーし、ARN AWS ポータル。

Create role

1 2 3 4

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. 次の構文を確認してください。 "Trust Relationship > Edit Relationship" 次のJSONの例に一致します (設定した値を使用)。

```
{ "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. コピー ARN 変更前 AWS 詳細を入力してください vManage マルチクラウドページ

Cloud Account Credentials - Update

Cloud Provider

 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

その"/var/log/nms/containers/cloudagent-v2/cloudagent-v2.log" ファイルに重要なメッセージがある (設定した値を含む) :

```
[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==" ,
```

参考

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