

使用IAM配置AWS多云vManage帐户

目录

- [简介](#)
- [背景](#)
- [问题](#)
- [解决方案](#)
- [参考](#)

简介

本文档介绍如何解决尝试使用IAM帐户实现多云自动化时出现的信任问题。

背景

当您在AWS TGW和您的公司AWS账户中使用思科多云功能时，存在信任问题。这是因为唯一的Account ID与vManage EC2实例。

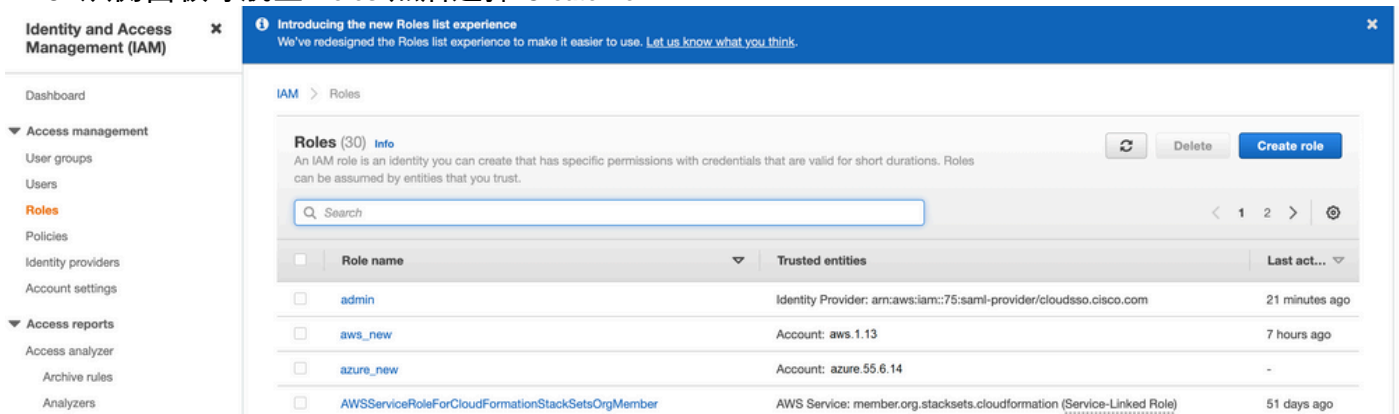
问题

当您使用IAM帐户进行多云自动化时，会引起信任问题。

解决方案

要解决此问题：

1. 导航至 **AWS > Identity and Access Management (IAM)** 并创建新的 **ROLE** 或列出的 **ROLE**。
2. 在 **AWS** 门户，输入 **IAM** 搜索栏中的 **IAM** 打开。
3. 从侧面板导航至 **Roles** 然后选择 **Create New**。




4. 选择 **Another AWS Account** 作为选项。

5. **Account ID** 是 **AWS Account** 并拥有 **vManage EC2** 实例已生成。对于思科托管帐户，帐户ID为“2002388880647”。(这不是您自己的 **AWS Account ID**.)请参阅本文结尾的参考资料。

6.选中此框 "External ID" 并在 vManage > Cloud onRamp for multi-cloud > Account Management > Add AWS Account.

Provide Cloud Account Details

Cloud Provider

 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 

<http://vm/can/do>

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. 设置权限。

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. 跳过标记。

9. 查看最后一页并为角色命名。发布创建 **ROLE** 并复制 **ARN** 从 **AWS** 门户。

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. 确保 "Trust Relationship > Edit Relationship" 匹配此JSON示例 (使用您设置的值) :

```
{ "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. 复制 **ARN** 从 **AWS** 并填写 **vManage** 多云页面。

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"/>

此"/var/log/nms/containers/cloudagent-v2/cloudagent-v2.log" 文件包含有价值的消息 (带有您设置的值) :

```
[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+EfSdKS8kaMpWCFE7W3vLjqaJCPgmSP1D61RsdlyrIldmQsf9bW7OFNhUKH5LQg+2Gkdey0IyTUg==" ,
```

参考

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