

IAM으로 AWS Multi-cloud vManage 계정 구성

목차

- [소개](#)
- [배경](#)
- [문제](#)
- [솔루션](#)
- [참조](#)

소개

이 문서에서는 멀티 클라우드 자동화를 위해 IAM 계정을 사용하려고 할 때 발생하는 트러스트 문제를 해결하는 방법에 대해 설명합니다.

배경

Cisco 멀티 클라우드 기능을 AWS TGW 및 회사 AWS 계정과 함께 사용하면 신뢰에 문제가 있습니다. 그 이유는 Account ID 이(가) vManage EC2 AWS의 인스턴스입니다.

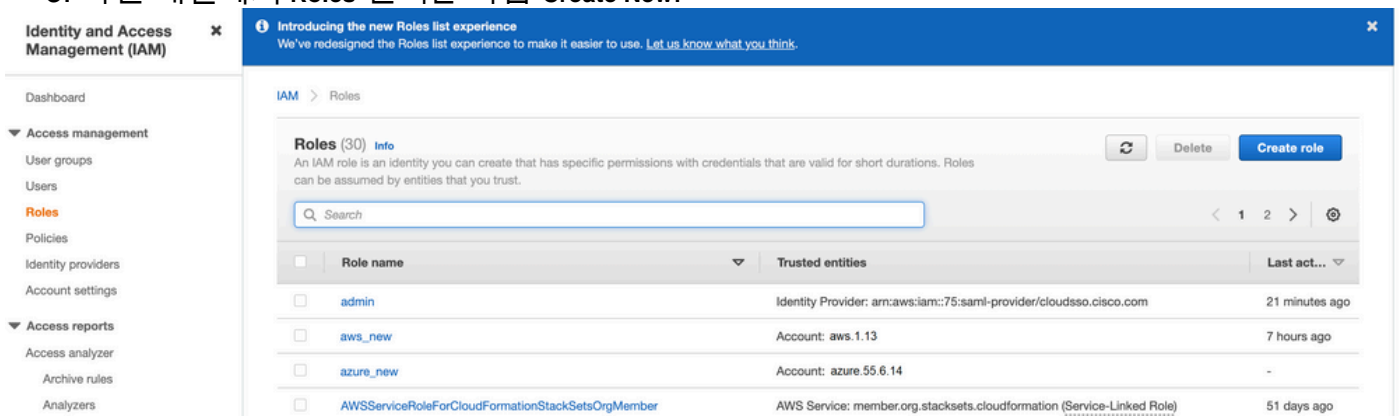
문제

멀티 클라우드 자동화를 위해 IAM 계정을 사용할 경우 트러스트 문제가 발생합니다.

솔루션

이 문제를 해결하려면

1. 탐색 AWS > Identity and Access Management (IAM) 새로운 ROLE 또는 ROLE.
2. 에 AWS 포털, 입력 IAM 검색 막대에서 IAM 를 엽니다.
3. 측면 패널에서 Roles 선택한 다음 Create New.



The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with 'Identity and Access Management (IAM)' selected. The main content area displays a list of roles under the heading 'Roles (30)'. The roles listed are:

<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 선택할 수 있습니다.

5. Account ID 은(는) AWS Account 및 vManage EC2 인스턴스를 빌드했습니다. Cisco Hosted Account의


경우 계정 ID는 "2002388880647"입니다. AWS Account ID.) 이 문서의 끝에 있는 참조를 참조하십시오

6. 다음에 대한 확인란을 선택합니다. "External ID" 다음 아래에 값을 입력합니다. 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

 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 

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. 권한을 설정합니다.

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. 태그를 건너뛵니다.

9. 마지막 페이지를 검토하고 역할 이름을 지정합니다. 작성 게시 ROLE 및 ARN 에서 AWS 포털 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 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. 아래의 구문이 "Trust Relationship > Edit Relationship"이 JSON 예와 일치(설정된 값 포함):

```
{ "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. 복사 ARN 발신 AWS 자세한 내용을 vManage 멀티 클라우드 페이지입니다.

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"/>

이 "/var/log/nms/containers/cloudagent-v2/cloudagent-v2.log" 파일에 다음과 같은 중요한 메시지가 있습니다 (사용자가 설정한 값 포함).

```
[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==" ,
```

참조

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