Configurar a conta do AWS Multi-cloud vManage com IAM

Contents

Introduction

Este documento descreve como resolver problemas de confiança que ocorrem quando você tenta usar a conta IAM para automação de várias nuvens.

Background

Quando você usa o recurso de várias nuvens da Cisco com o AWS TGW e a conta AWS da sua empresa, há problemas de confiança. Isso porque a empresa única **Account ID** é diferente do **vManage EC2** instância no AWS.

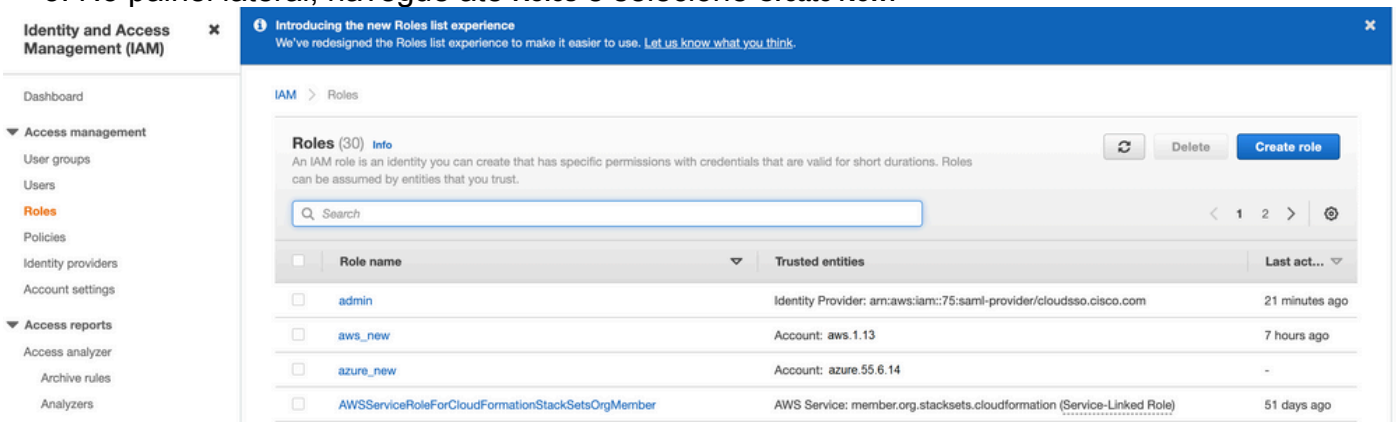
Problema

Quando você usa a conta IAM para automação de várias nuvens, isso causa um problema de confiança.

Solução

Para resolver esse problema:

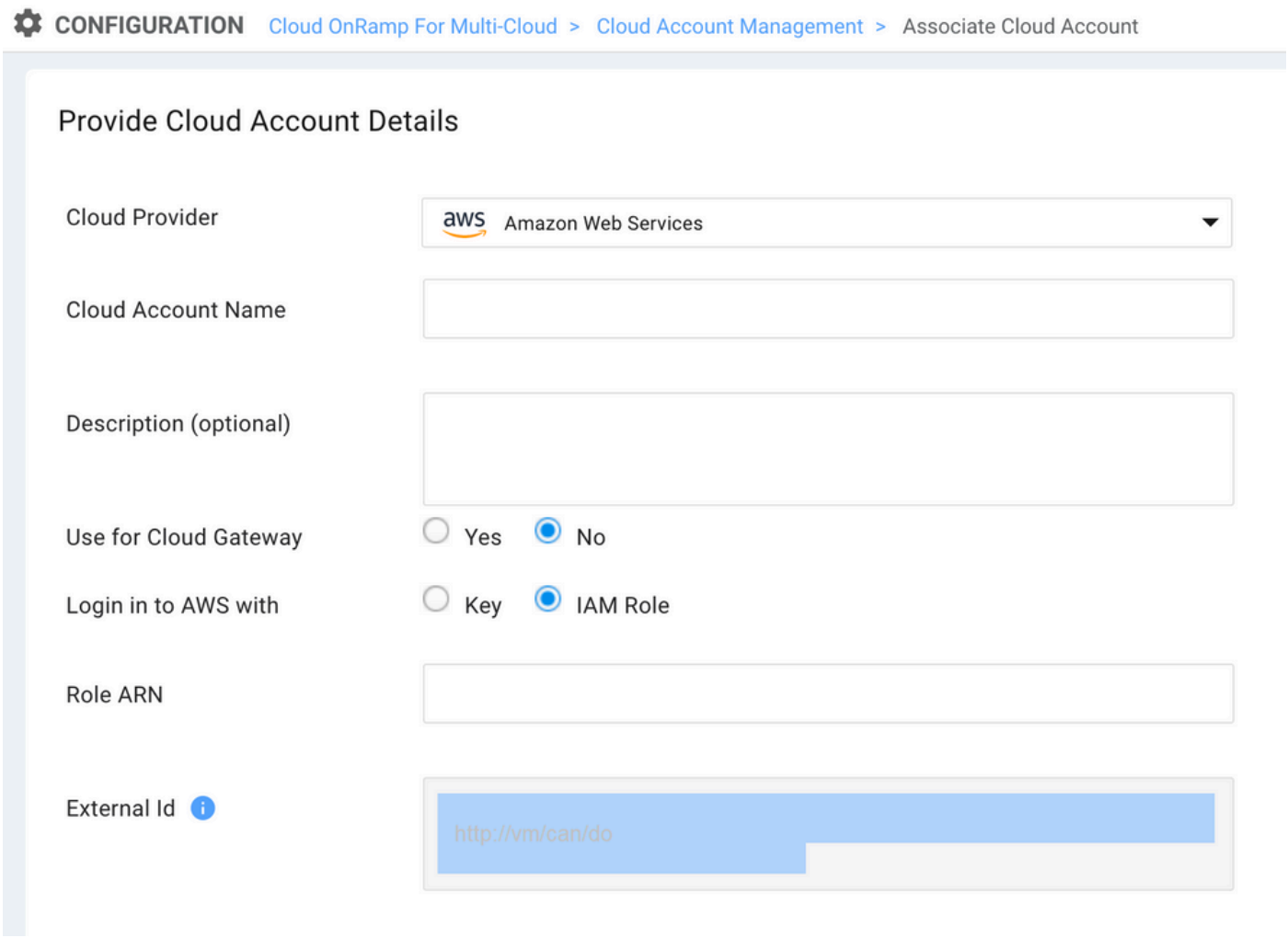
1. Navegue até **AWS > Identity and Access Management (IAM)** e criar uma nova **ROLE** ou outro **ROLE.**
2. Na guia **AWS** portal, insira **IAM** na barra de pesquisa. O **IAM** abre.
3. No painel lateral, navegue até **Roles** e selecione **Create New.**

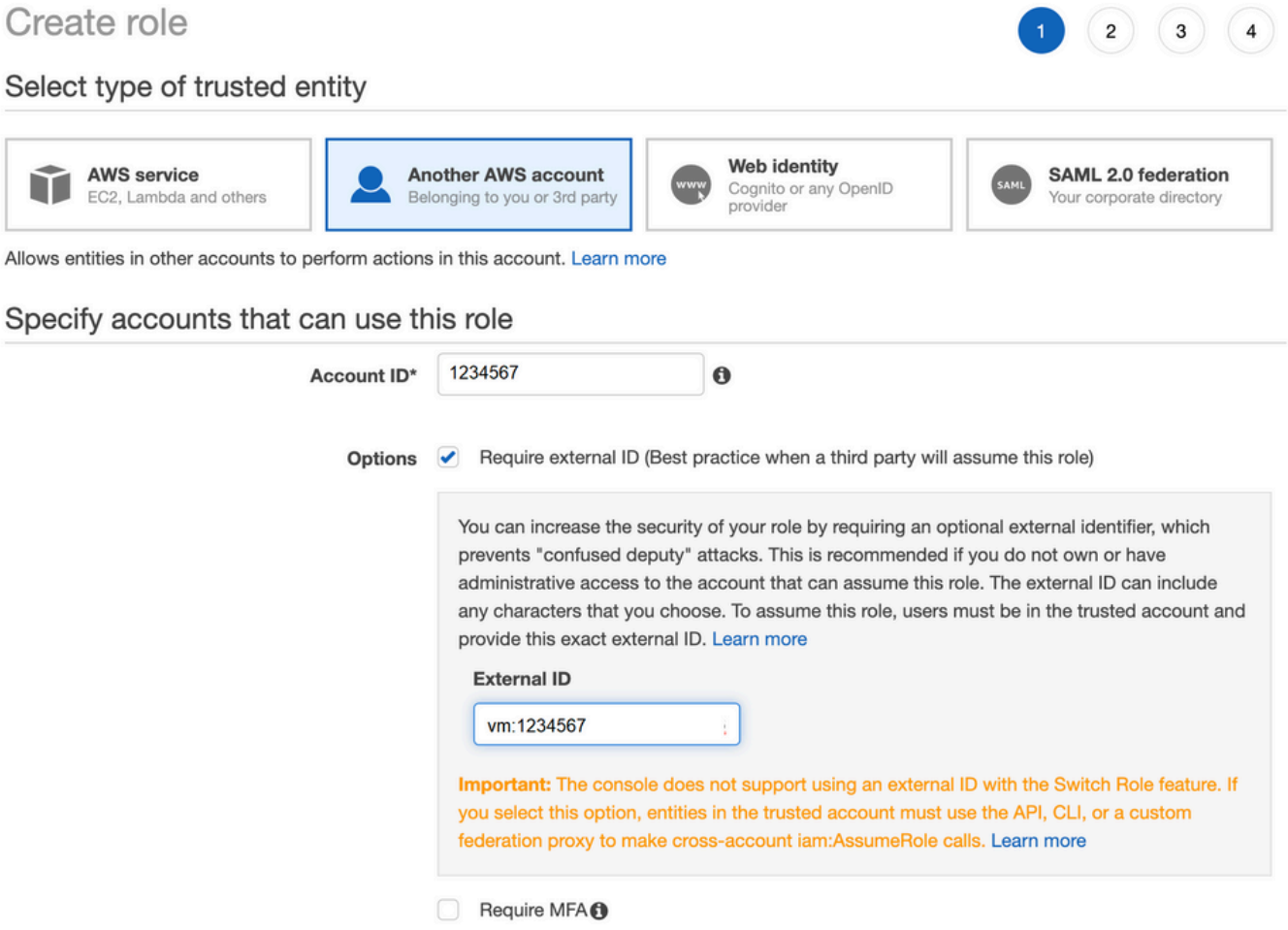


4. Selecione a opção **Another AWS Account** como uma opção.

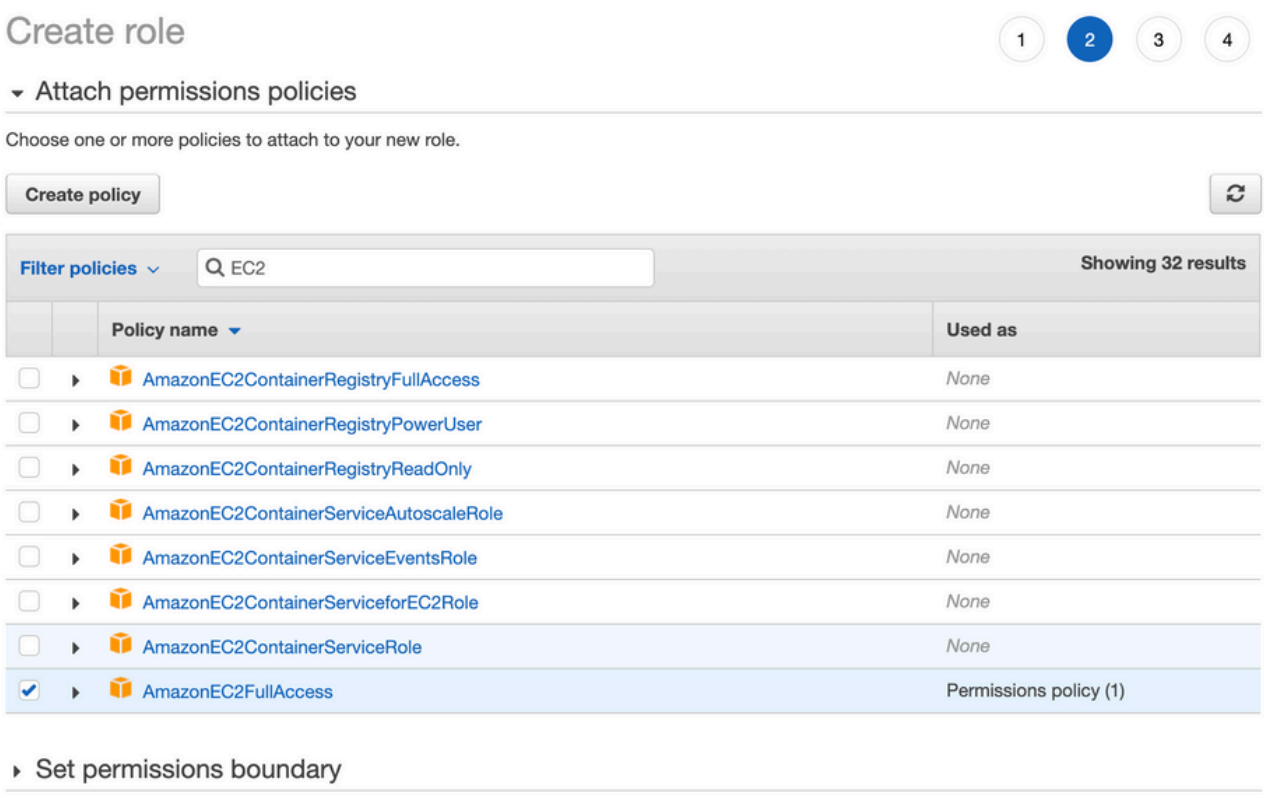
5. O **Account ID** é o **AWS Account** e tem o **vManage EC2** instância criada. Para contas Cisco Hosted, a ID da conta é "2002388880647". (Não é sua própria **AWS Account ID**.) Consulte Referência no final deste artigo.

6. Marque a caixa para **"External ID"** e insira um valor em **vManage > Cloud onRamp for multi-cloud > Account Management > Add AWS Account.**



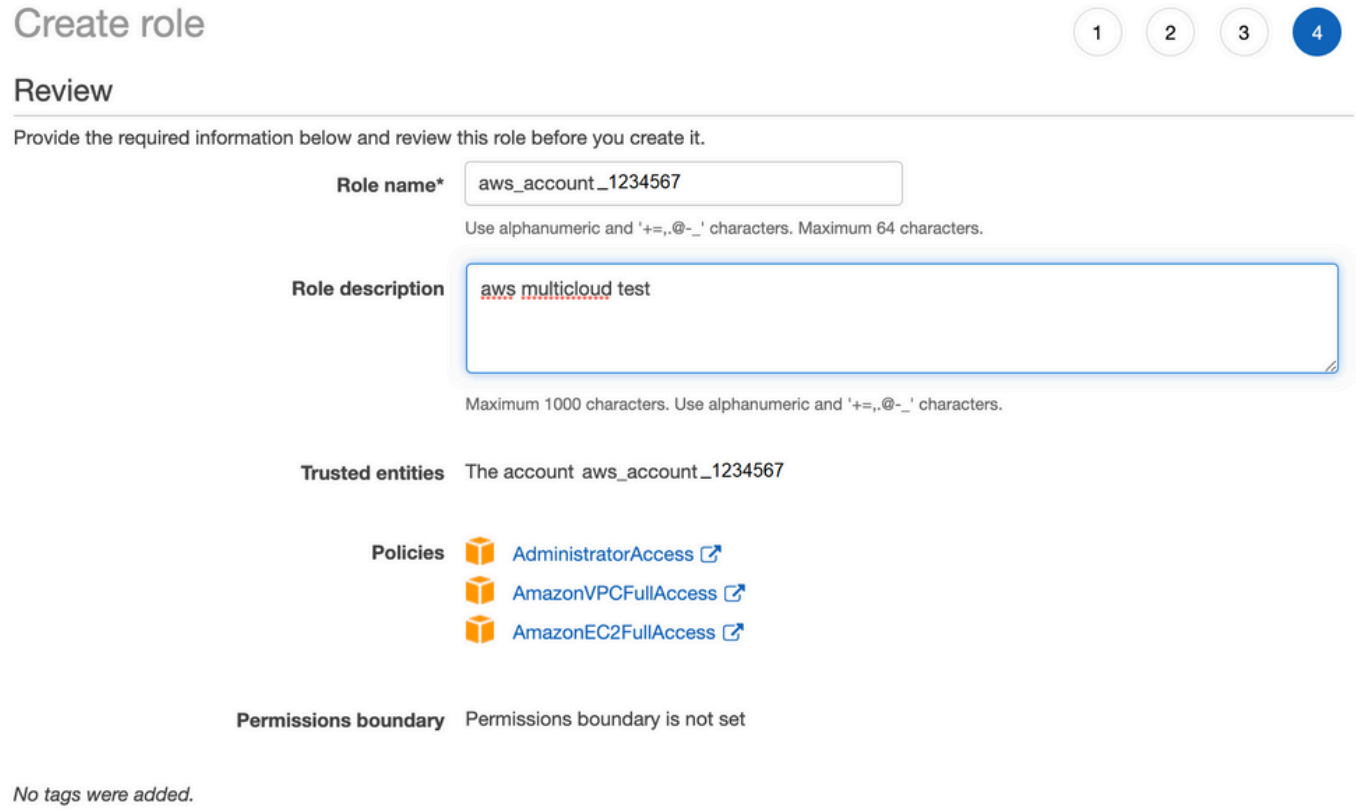


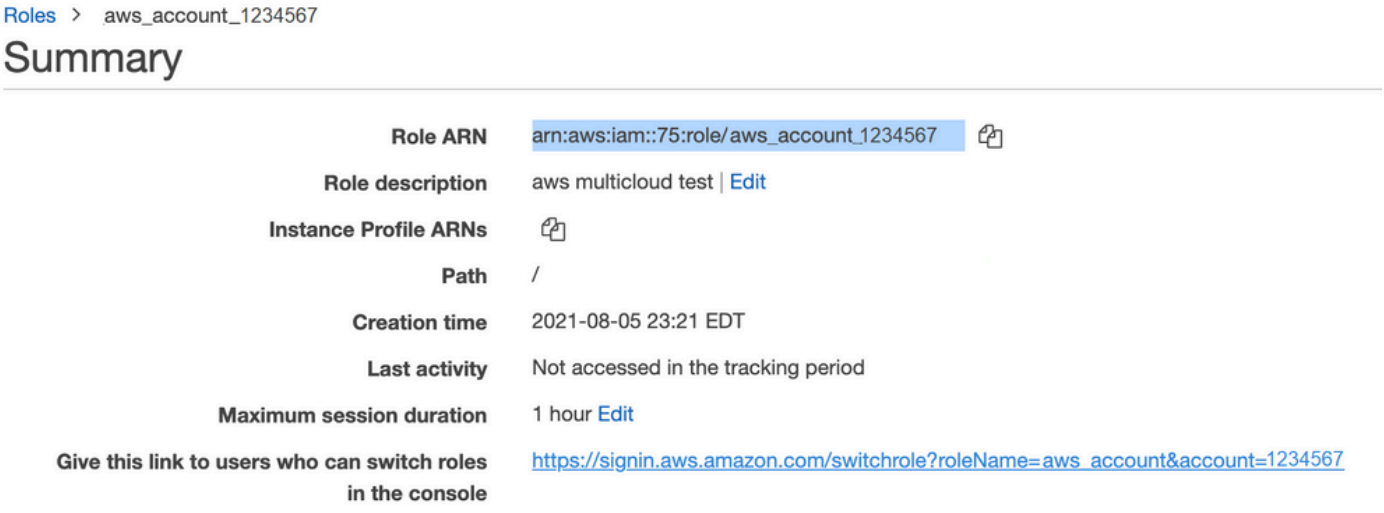
7. Defina permissões.



8. Ignore as marcas.

9. Revise a última página e nomeie a atribuição. Lançar a criação de **ROLE** e copiar o **ARN** nos **AWS** portal.

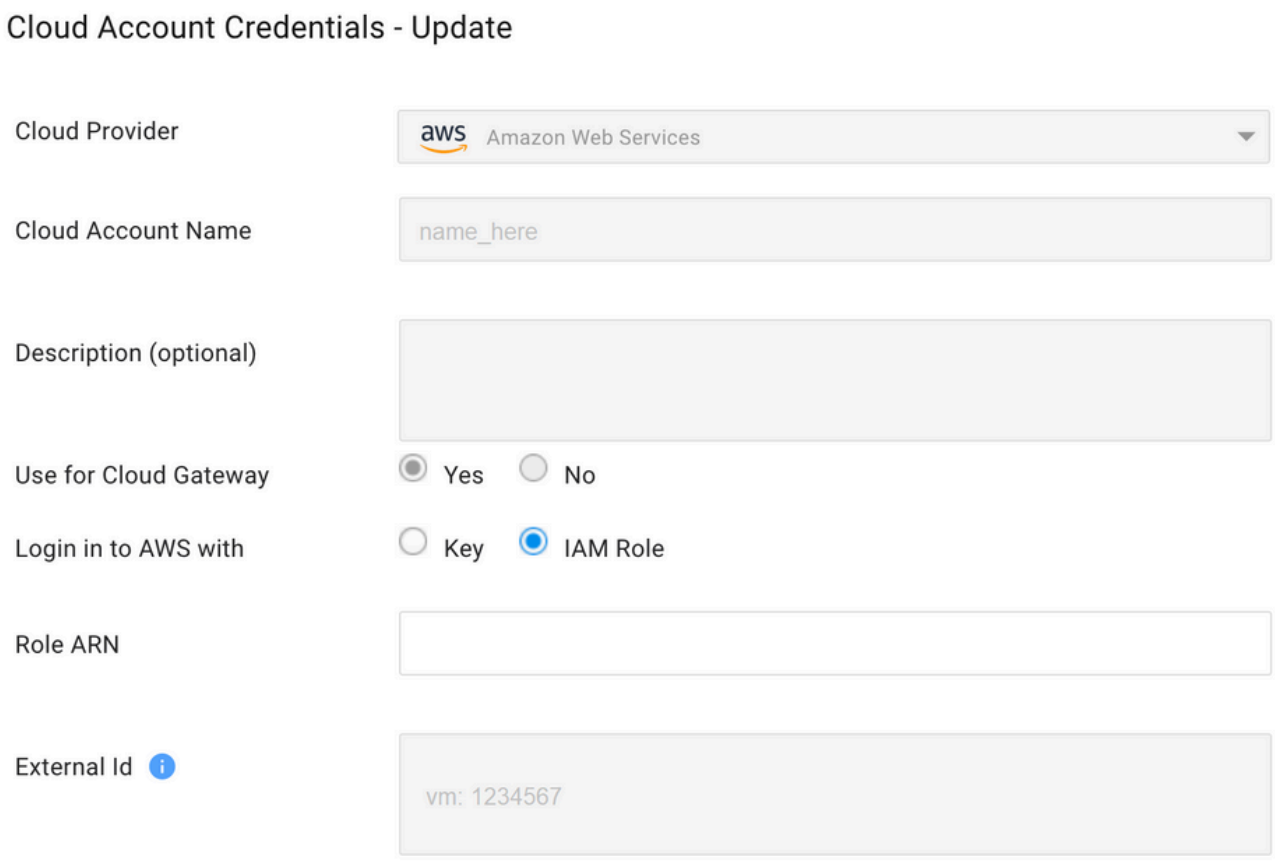




10. Verifique se a sintaxe sob o comando **"Trust Relationship > Edit Relationship"**corresponde a este exemplo JSON (com os valores definidos):

```
{ "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. Copie o **ARN** de **AWS** e preencha os detalhes no **vManage** página de várias nuvens.



O "**/var/log/nms/containers/cloudagent-v2/cloudagent-v2.log**" O arquivo tem mensagens valiosas (com os valores definidos por você):

```
[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==",
```

Referência

[Cisco_Cloud_onRamp_for_IaaS_AWS_Version2.html]