Configurare l'account AWS Multi-cloud vManage con IAM

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi di attendibilità che si verificano quando si tenta di utilizzare l'account IAM per l'automazione multiscloud.

Sfondo

Quando si utilizza la funzionalità multi-cloud Cisco con AWS TGW e l'account AWS della società, si verificano problemi di attendibilità. Questo perché l'azienda unica **Account ID** è diverso dal **vManage EC2** in AWS.

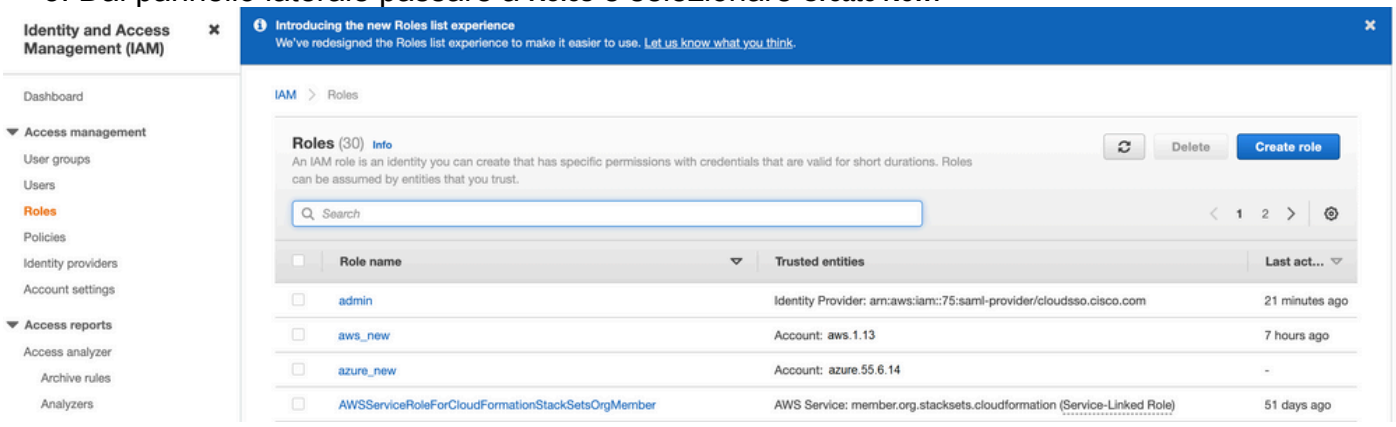
Problema

Quando si utilizza l'account IAM per l'automazione di più cloud, si verifica un problema di attendibilità.

Soluzione

Per risolvere il problema:

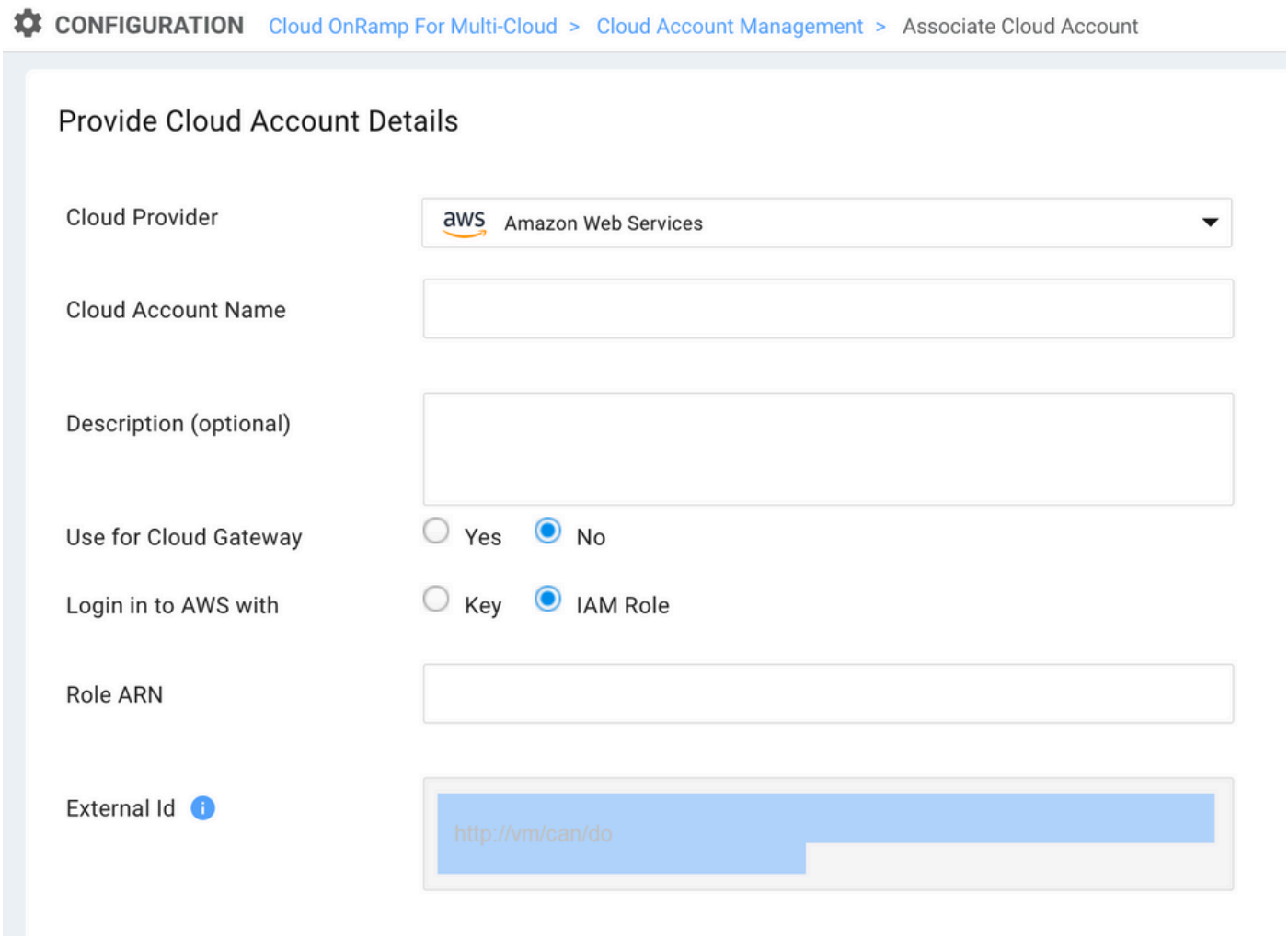
1. Passa a **AWS > Identity and Access Management (IAM)** e creare un nuovo **ROLE** o un altro **ROLE.**
2. Nella scheda **AWS** portale, immettere **IAM** nella barra di ricerca. Il **IAM** si apre.
3. Dal pannello laterale passare a **Roles** e selezionare **Create New.**

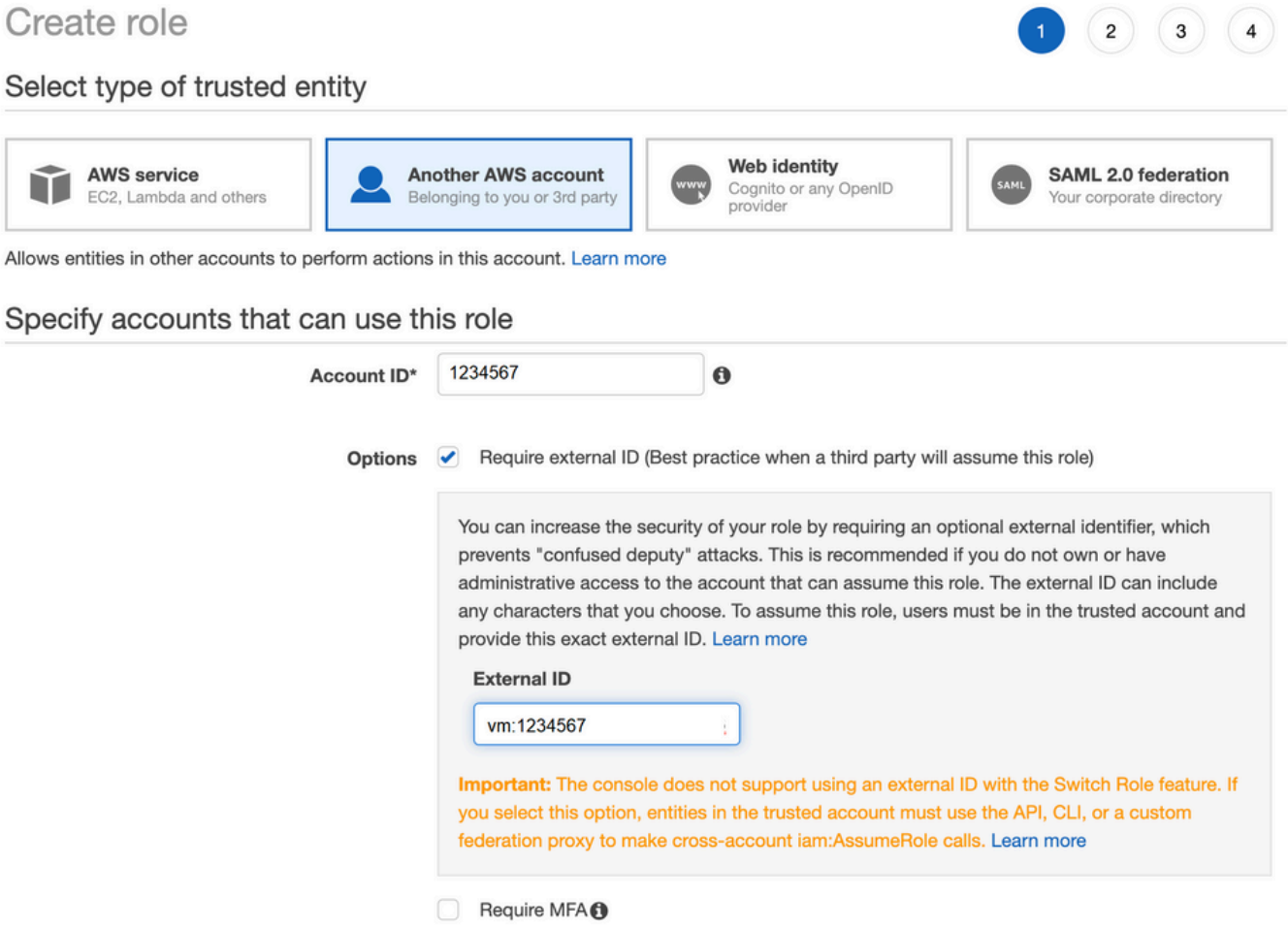


4. Selezionare il **Another AWS Account** come opzione.

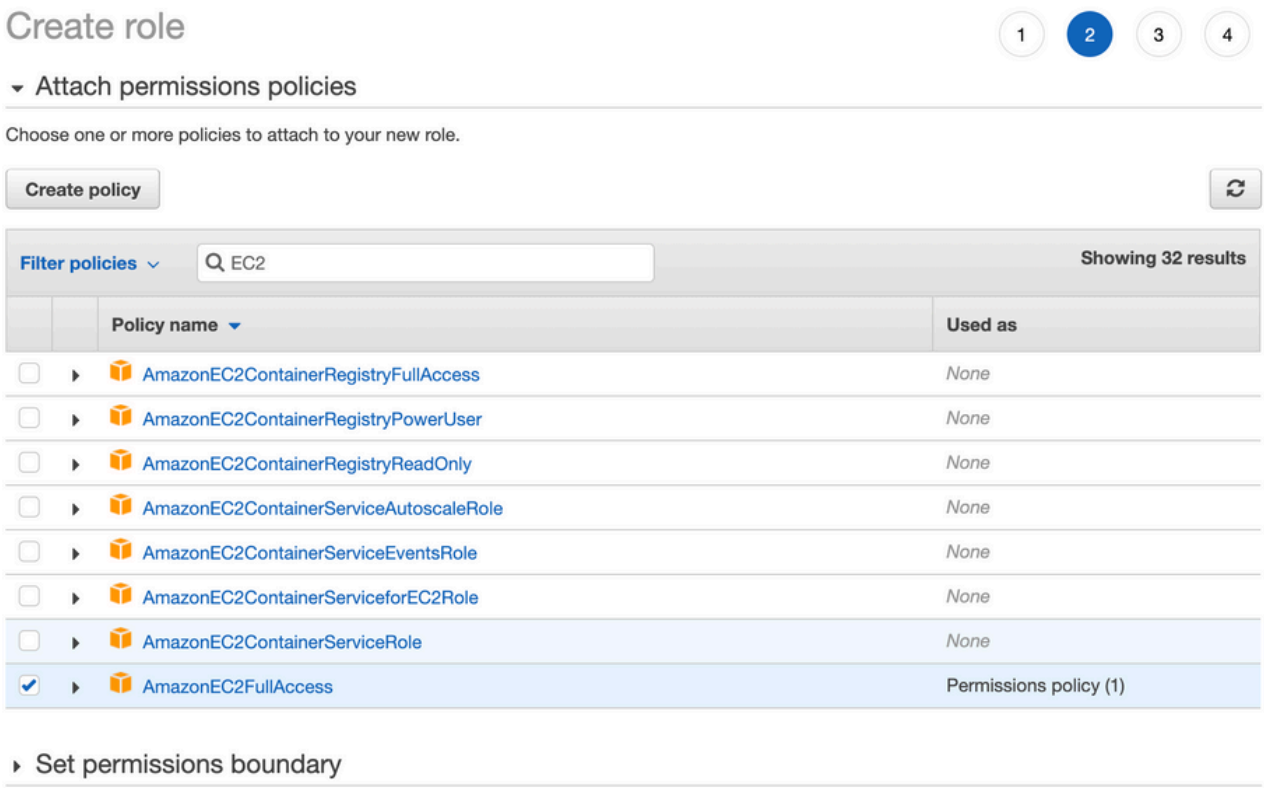
5. Il **Account ID** è il **AWS Account** e ha il **vManage EC2** istanza creata. Per gli account Cisco Hosted, l'ID account è "200238880647". (NON è il tuo) **AWS Account ID**.) Fare riferimento alla fine di questo articolo.

6. Selezionare la casella per **"External ID"** e immettere un valore in **vManage > Cloud onRamp for multi-cloud > Account Management > Add AWS Account.**



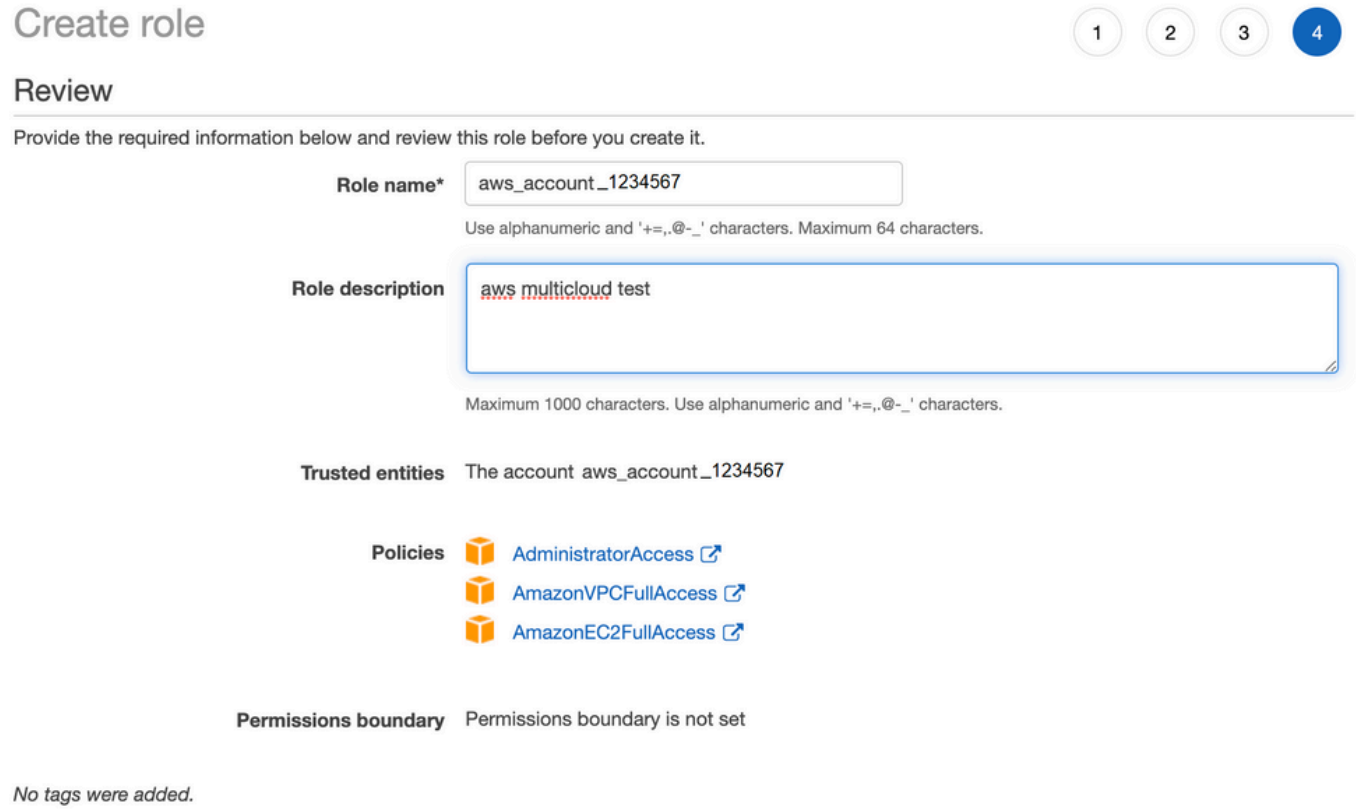


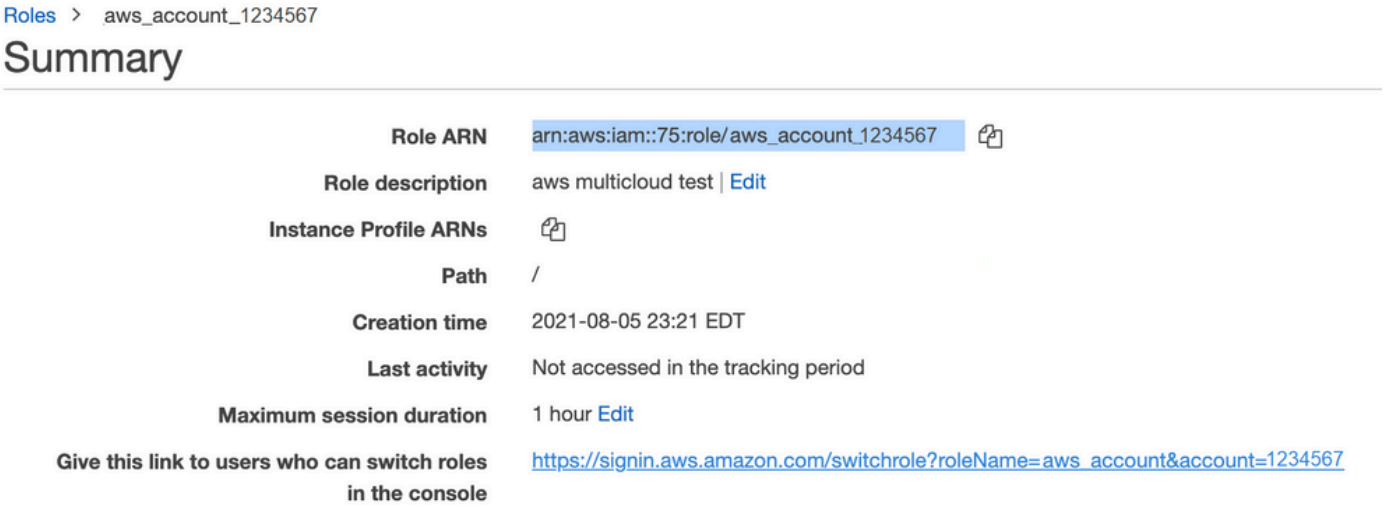
7. Impostare le autorizzazioni.



8. Ignora i tag.

9. Controllare l'ultima pagina e assegnare un nome al ruolo. Post la creazione di **ROLE** e copiare **ARN** dal **AWS** portale.

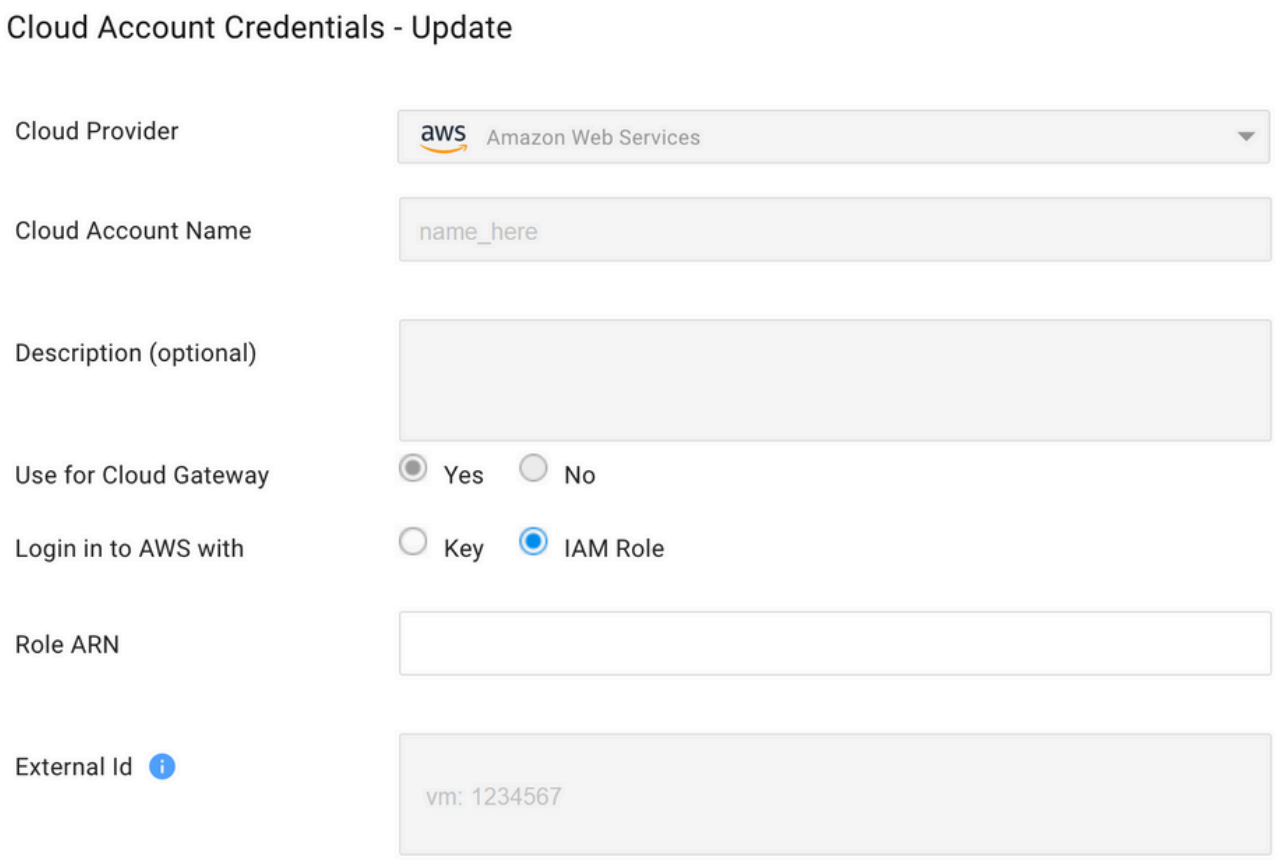




10. Assicurarsi che la sintassi in **"Trust Relationship > Edit Relationship"**corrisponde al seguente esempio JSON (con i valori impostati):

```
{ "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. Copia **ARN** da **AWS** e compilare i dettagli sul **vManage** pagina con più cloud.



Il "**/var/log/nms/containers/cloudagent-v2/cloudagent-v2.log**" contiene messaggi importanti (con i valori impostati):

```
[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==",
```

Riferimento

[Cisco_Cloud_onRamp_for_IaaS_AWS_Version2.html]