

ل ةبإحسلا ددعتم vManage باسح نيوكت IAM مادختساب AWS

تايوتحمل

[ةمدقملا](#)

[ةيفلخلا](#)

[ةلكشملا](#)

[لحلا](#)

[عجرملا](#)

ةمدقملا

IAM باسح مادختساب ةلواحم دنع ثدحت يتلا ةقثلا لكاشم لح ةيفي ك دننتسملا اذه حضوي ةبإحسلا ةددعتم ةتمتألل.

ةيفلخلا

لكتكرشب صإخلا AWS باسحو AWS TGW عم ةبإحسلا ةددعتم Cisco ةزيم مدختست ام دنع vManage EC2 نع فللختم Account ID ةديرفلا ةكرشلا ببسب لك لذ. ةقثلا يف لكاشم كانه AWS يف ليثملا.

ةلكشملا

ةقث ةلكشم يف ببستتي هنإف، ةبإحسلا ةددعتم ةتمتألل IAM باسح مادختساب دنع.

لحلا

ةلكشملا هذه لحلا:

1. ROLE رخآ جاردا وأ ROLE دي دج عاشنإو AWS > Identity and Access Management (IAM) ىلإ لقتنا.
2. حتف يف IAM رمأل ضرعي. شحبلا طيرش يف IAM لاخدا، لخدم AWS ىلع.
3. Create New ددح مث Roles ىلإ لقتنا، ةببإجل ةحوللا نم.

Role name	Trusted entities	Last act...
admin	Identity Provider: arn:aws:iam::75:saml-provider/cloudsso.cisco.com	21 minutes ago
aws_new	Account: aws.1.13	7 hours ago
azure_new	Account: azure.55.6.14	-
AWSServiceRoleForCloudFormationStackSetsOrgMember	AWS Service: member.org.stacksets.cloudformation (Service-Linked Role)	51 days ago

4. رايخك Another AWS Account ددح .

5- حساب سحلل ةبس نلاب . لثم عاشن | م ت vManage EC2 هو دلو و AWS Account هو Account ID .
AWS Account ID.) (هذه "200238880647" وه باسحلا فرعم نوكي ، Cisco نم ةفاضت سمل
ةدامل هذه ةياهن ي ف دراوال عجرمل رظنا .

6. رايخالا ةناخ ددح . ل رايخالا ةناخ ددح .
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 


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. تان وذل ان يي عت .









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. تامال عل ي طخت .

9. قباوب AWS نم ARN آسنو ROLE ءاشنإ رشن . رودلا مسا ددحو ةريآال ءحفصلا عآار .

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. اذه JSON لاثم ةقباطم "Trust Relationship > Edit Relationship" بآومب ةآااصلا نأ نم دكأت (اهطبضب تمق يتلا ميقلاب):

```
{ "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. قباوصلا ةددعتم ءحفص vManage ب ةصاآلا لاصاافتلا اولماو AWS نم ARN آسنا .

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"/>

ميرق لئاسر لى ع فللملا يوتحي `"var/log/nms/containers/cloudagent-v2/cloudagent-v2.log"` رمألا ضرعي
(اهني يعتب تمق يتلا ميقلاب):

```
[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==" ,
```

عجرملا

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

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا