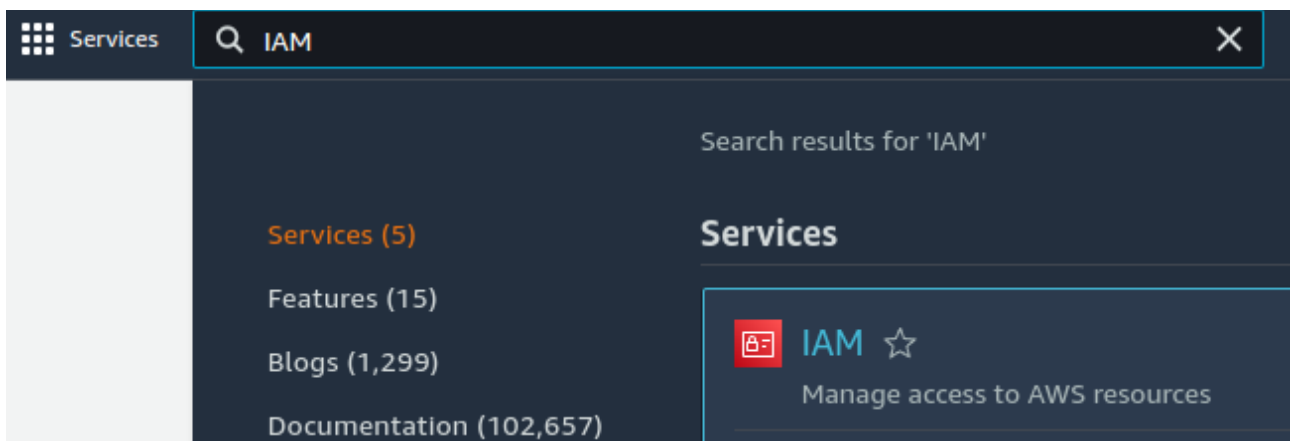




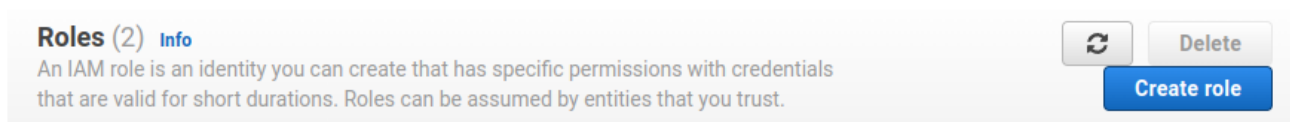
Allowing IDI EIKON to administer your AWS resources

This guide shows how to give IDI EIKON administrative access to your AWS account for creating and managing servers for dRural project. This administrator access don't give access to IDI EIKON to AWS billing so your payment information it's safe.

1.- **Go to IAM** Service, searching in the top search bar.



2.- Go to Roles and “Create role”





3.- Select “AWS account” and “Another AWS account”. Put 114849655608 in Account ID. Additional options must be unchecked. Click Next.

Select trusted entity

Trusted entity type

☐ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☒ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

An AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ This account (772221544737)

☒ **Another AWS account**

Account ID

Identifier of the account that can use this role

Account ID is a 12-digit number.

Options

- ☐ Require external ID (Best practice when a third party will assume this role)
- ☐ Require MFA
Requires that the assuming entity use multi-factor authentication.

[Cancel](#)

[Next](#)

4.- Add permissions to the account. Search for “AdministratorAccess” and press Enter

Add permissions

Permissions policies (Selected 1/751)

Choose one or more policies to attach to your new role.



5.- Select “AdministratorAccess” with type “AWS managed – job function” and click “Next”

"AdministratorAccess" X		Clear filters	
<input checked="" type="checkbox"/>	Policy name ↗	Type	Description
<input checked="" type="checkbox"/>	AdministratorAccess	AWS managed - job function	Provides full access to AWS services and resources.

6.- Give role a name and a description. Name needs to be “**druraleikon**” and as description we suggest “dRural administration role for IDI EIKON”. Click in “Create role” at the bottom of the page. Role will be created and page redirected to roles page again.

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

druraleikon

Maximum 64 characters. Use alphanumeric and '+,=,@-_' characters.

Description

Add a short explanation for this policy.

dRural administration role for IDI EIKON

Maximum 1000 characters. Use alphanumeric and '+,=,@-_' characters.



7.- Enter in the new druraleikon created role clicking the name, go to “Trust relationships” and click “Edit trust policy”

IAM > Roles > druraleikon

druraleikon Delete

dRural administration role for IDI EIKON

Summary Edit

Creation date May 09, 2022, 09:08 (UTC+02:00)	ARN arn:aws:iam::772221544737:role/druraleikon	Link to switch roles in console https://signin.aws.amazon.com/switchrole?roleName=druraleikon&account=772221544737
Last activity None	Maximum session duration 1 hour	

Permissions **Trust relationships** Tags Access Advisor Revoke sessions

Trusted entities Edit trust policy

Entities that can assume this role under specified conditions.

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "AWS": "arn:aws:iam::114849655608:root"  
8       },  
9       "Action": "sts:AssumeRole",  
10      "Condition": {}  
11    }  
12  ]  
13 }
```

8.- Edit trust policy and paste this full text (or change “/root” for “user/drural”):

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": "arn:aws:iam::114849655608:user/drural"  
      },  
      "Action": "sts:AssumeRole",  
      "Condition": {}  
    }  
  ]  
}
```



8.- Click in “Update policy” and we are done.

[IAM](#) > [Roles](#) > [druraleikon](#) > [Edit trust policy](#)

Edit trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "AWS": "arn:aws:iam::114849655608:user/drural"  
8       },  
9       "Action": "sts:AssumeRole",  
10      "Condition": {}  
11    }  
12  ]  
13 }
```

[Add new statement](#)

JSON Ln 7, Col 61

Cancel

Update policy

Revoking access to IDI EIKON to your account.

Simply delete “druraleikon” role.