AWS Assume Role

=====================================================================================

1. Create one Iam user name:Security
2. Create one roles

* Choose service – EC2
* Select [AdministratorAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAdministratorAccess)
* Give role name
* Create Role

1. Enable Trust-relation for user under the role

* Edit code
* Paste arn of created user

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"sts:AssumeRole"

],

"Principal": {

"AWS":

"arn:aws:iam::182263511292:user/security"

"Service": [

"ec2.amazonaws.com"

]

}

}

]

}

In terminal if we already configure user then we have to change this

root@DESKTOP-DA2RDP0:~# aws sts assume-role --duration-seconds 900 --role-arn arn:aws:iam::112365962865:role/devops --role-session-name security-role-session

An error occurred (AccessDenied) when calling the AssumeRole operation: Roles may not be assumed by root accounts.

root@DESKTOP-DA2RDP0:~# aws sts get-caller-identity

{

"UserId": "112365962865",

"Account": "112365962865",

"Arn": "arn:aws:iam::112365962865:root"

}

root@DESKTOP-DA2RDP0:~# mv /root/.aws /opt

* move .aws in /opt

root@DESKTOP-DA2RDP0:~# aws sts get-caller-identity

Unable to locate credentials. You can configure credentials by running "aws configure".

* Now we are not able to locate credentials
* Adding user created access key credentials

root@DESKTOP-DA2RDP0:~# aws configure

AWS Access Key ID [None]: AKIARUKMIQZYTKBMLAL2

AWS Secret Access Key [None]: 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

Default region name [None]: us-east-1

Default output format [None]: json

root@DESKTOP-DA2RDP0:~#

root@DESKTOP-DA2RDP0:~# aws sts get-caller-identity

{

"UserId": "AIDARUKMIQZYSSHL7MFER",

"Account": "112365962865",

"Arn": "arn:aws:iam::112365962865:user/security"

}

root@DESKTOP-DA2RDP0:~# aws s3 ls

* Add arn of roles here so we can get credentials

root@DESKTOP-DA2RDP0:~# aws sts assume-role --duration-seconds 900 --role-arn arn:aws:iam::112365962865:role/devops --role-session-name security-role-session

{

"Credentials": {

"AccessKeyId": "ASIARUKMIQZY2KKBX2V3",

"SecretAccessKey": "nD8+NMdy3326rux7vd0/RDuEEmKEDNT9o3dZvHe+",

"SessionToken": "FwoGZXIvYXdzEO///////////wEaDJhzCvWqD92lMIO4eCK5AYpc5C3ZVLUAUlPaZeJ9MikZkLvNRQKHZXnwmUd6vSGnsogkw/7vdjh3zOKiO5I4eP6A/HIXPE+AMkSL96sxieDuwKg9nNJEjyvdV6bOD/yxLaHOLvvRqfGRYDcuZ1uO2xhn4/Eyq6eOmGjH6g5h0+NxY+gLTuJhPGVJOyCbeC+o3z0pXm0zmj/xbZYHm+I47j5kTBIQDa8KB+eK+XatUK1HX2fNuWXTmT1vt8xfGtKLYE2elQrz+uq6KMPVg64GMi16su4GU2fevZ2BzRCWjC3tFZbuvmU/DBa3LXeFOXaK/DPP4cO5BjEq6cqBn7U=",

"Expiration": "2024-02-05T14:18:47Z"

},

"AssumedRoleUser": {

"AssumedRoleId": "AROARUKMIQZY674VXDHZP:security-role-session",

"Arn": "arn:aws:sts::112365962865:assumed-role/devops/security-role-session"

}

}

* Export

root@DESKTOP-DA2RDP0:~# export AWS\_ACCESS\_KEY\_ID="ASIARUKMIQZY2KKBX2V3"

root@DESKTOP-DA2RDP0:~# export AWS\_SECRET\_ACCESS\_KEY="nD8+NMdy3326rux7vd0/RDuEEmKEDNT9o3dZvHe+"

root@DESKTOP-DA2RDP0:~# export AWS\_SESSION\_TOKEN="FwoGZXIvYXdzEO///////////wEaDJhzCvWqD92lMIO4eCK5AYpc5C3ZVLUAUlPaZeJ9MikZkLvNRQKHZXnwmUd6vSGnsogkw/7vdjh3zOKiO5I4eP6A/HIXPE+AMkSL96sxieDuwKg9nNJEjyvdV6bOD/yxLaHOLvvRqfGRYDcuZ1uO2xhn4/Eyq6eOmGjH6g5h0+NxY+gLTuJhPGVJOyCbeC+o3z0pXm0zmj/xbZYHm+I47j5kTBIQDa8KB+eK+XatUK1HX2fNuWXTmT1vt8xfGtKLYE2elQrz+uq6KMPVg64GMi16su4GU2fevZ2BzRCWjC3tFZbuvmU/DBa3LXeFOXaK/DPP4cO5BjEq6cqBn7U="

root@DESKTOP-DA2RDP0:~# aws sts get-caller-identity

{

"UserId": "AROARUKMIQZY674VXDHZP:security-role-session",

"Account": "112365962865",

"Arn": "arn:aws:sts::112365962865:assumed-role/devops/security-role-session"

}

- Create s3 bucket name = myawsbucket7777890007

root@DESKTOP-DA2RDP0:~# aws s3 ls

2024-02-05 19:39:26 myawsbucket7777890007

* Delete root file of .aws

root@DESKTOP-DA2RDP0:~# rm -rf /root/.aws/

* Move back our old configure

root@DESKTOP-DA2RDP0:~# mv /opt/.aws /root

root@DESKTOP-DA2RDP0:~# cd /root/.aws/

root@DESKTOP-DA2RDP0:.aws# ll

total 16

drwxr-xr-x 2 root root 4096 Dec 28 11:13 ./

drwx------ 16 root root 4096 Feb 5 19:42 ../

-rw------- 1 root root 43 Jan 23 11:48 config

-rw------- 1 root root 116 Jan 23 11:48 credentials

root@DESKTOP-DA2RDP0:.aws# cat credentials

[default]

aws\_access\_key\_id = AKIARUKMIQZY4OQ4WPAN

aws\_secret\_access\_key = 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

root@DESKTOP-DA2RDP0:.aws#