

Assignment 5 :: IAM- create group called as globallogic and assign permission to launch EC2 instance only in us-east-1(any available region) with specific duration in daytime.

Step 1 :: Create Custom Policy from AWS console

The screenshot shows the AWS IAM console 'Policies' page. A custom policy named 'Assignment-5' is being created. The policy document is displayed in a text editor, allowing for syntax highlighting and line numbers. The policy is a 'Customer managed' type with no 'Used as' dependencies. The policy document is as follows:

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": "ec2:*",
8       "Resource": "*",
9       "Condition": {
10        "StringEquals": {
11          "aws:RequestedRegion": "us-east-1"
12        },
13        "DateGreaterThan": {
14          "aws:CurrentTime": "2022-06-20T00:00:00Z"
15        },
16        "DateLessThan": {
17          "aws:CurrentTime": "2022-10-20T00:00:00Z"
18        }
19      }
20    ]
21  }
```

Step 2 :: Created User group named “globallogic” using custom policy “Assignment-5” created in step 1.

The screenshot shows the AWS IAM console 'User groups' page. A user group named 'globallogic' has been created and is selected. The table below shows the details of the user groups.

Group name	Users	Permissions	Creation time
<input checked="" type="checkbox"/> globallogic	⌚ Loading	✔ Defined	Now
<input type="checkbox"/> NL_DND_Niit_AWS_POC_Test_policy	⌚ Loading	⌚ Loading	11 days ago
<input type="checkbox"/> NL_DND_SSO	⌚ Loading	⌚ Loading	11 days ago
<input type="checkbox"/> NL_DND_StackRoute_IAM_Policy	⌚ Loading	⌚ Loading	11 days ago


Step 3 :: Creating a test username “globallogictestuser” with custom policy


While creating the user, adding it to group “globallogic” created in step 2.


## Add user

12345

Set permissions

 Add user to group

 Copy permissions from existing user

 Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

### Add user to group

Create group

Refresh

Search

Showing 4 results

Group	Attached policies
<input checked="" type="checkbox"/> globallogic	Assignment-5
<input type="checkbox"/> NL_DND_Niit_AWS_POC_Test_policy	Niit_AWS_POC_Test_policy
<input type="checkbox"/> NL_DND_SSO	SSO
<input type="checkbox"/> NL_DND_StackRoute_IAM_Policy	StackRoute_IAM_Policy

Set permissions boundary

Cancel

Previous

Next: Tags

## Add user

1 2 3 4 5

### Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

#### User details

User name	globallogictestuser
AWS access type	AWS Management Console access - with a password
Console password type	Autogenerated
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

#### Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	globallogic

#### Tags

The new user will receive the following tag

Key	Value
Name	TestUser

Cancel

Previous

Create user

## Add user

1 2 3 4 5



#### Users created but with errors

You successfully created the following users, but some problems remain. Expand the following section for details. View and download user's security credentials as well as email users instructions to log into the AWS Management Console. This will be the last time these credentials will be available to download. However, you can manage and recreate these credentials at any time.

Users with AWS Management Console access may sign-in at: <https://271697867512.signin.aws.amazon.com/console>

Download .csv

User
<div><div></div>globallogictestuser</div> <div><div><div><div> Created user globallogictestuser</div><div> Added user globallogictestuser to group globallogic</div><div> Could not create login profile for user globallogictestuser: User: arn:aws:iam::271697867512:user/hari.gopalakrishnan@globallogic.com is not authorized to perform: iam:CreateLoginProfile on resource: user globallogictestuser with an explicit deny in an identity-based policy</div></div></div></div>

Close

Step 4 :: Created AWS Access Key ID and secret access key

Create access key

Warning

Never post your secret access key on public platforms, such as GitHub. This can compromise your account security.

Success

This is the **only** time that the secret access keys can be viewed or downloaded. You cannot recover them later. However, you can create new access keys at any time.

Download .csv file

Access key ID	Secret access key
AKIAT6QTUOL4I57Z4GJA	b+aSAWjkgkfkQTPo9tPHtJLJEax9ZITrw90VTLH <a href="#">Hide</a>

Close

Step 5 :: aws configure using AWS Access Key ID for user “globallogictestuser”

AutoSave ☐ Off

globallogictestuser\_accessKeys.csv

	A	B	C	D
1	Access key ID	Secret access key		
2	AKIAT6QTUOL4I57Z4GJA	b+aSAWjkgkfkQTPo9tPHtJLJEax9ZITrw90VTLH		
3				
4				
5				

C:\ Administrator: Command Prompt

```
C:\Users\hari.gopalakrishnan>aws configure
AWS Access Key ID [*****LBVN]: AKIAT6QTUOL4I57Z4GJA
AWS Secret Access Key [*****vMkW]: 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
Default region name [us-east-1]: us-east-1
Default output format [None]:

C:\Users\hari.gopalakrishnan>
```

## Step 6 :: Creating EC2 instance via AWS CLI

```
C:\Users\hari.gopalakrishnan>aws ec2 run-instances --image-id ami-0cfff528ff583bf9a --count 1 --instance-type t2.micro --key-name DevOps --security-group-ids sg-0004c662da7a9e90 --subnet-id subnet-0b1da42a865748d33 --tag-specifications ResourceType=instance,Tags=[{Key=Name,Value=PolicyValidator}]
{
  "Groups": [],
  "Instances": [
    {
      "AmiLaunchIndex": 0,
      "ImageId": "ami-0cfff528ff583bf9a",
      "InstanceId": "i-0acdf94ad707664b3",
      "InstanceType": "t2.micro",
      "KeyName": "DevOps",
      "LaunchTime": "2022-06-21T10:34:58+00:00",
      "Monitoring": {
        "State": "disabled"
      },
      "Placement": {
        "AvailabilityZone": "us-east-1a",
        "GroupName": "",
        "Tenancy": "default"
      },
      "PrivateDnsName": "ip-192-168-0-14.ec2.internal",
      "PrivateIpAddress": "192.168.0.14",
      "ProductCodes": [],
      "PublicDnsName": "",
      "State": {
        "Code": 0,
        "Name": "pending"
      },
      "StateReason": {
        "Code": "pending",
        "Message": "pending"
      },
      "StateTransitionReason": "",
      "SubnetId": "subnet-0b1da42a865748d33",
      "VpcId": "vpc-84b8132b5469f9777",
      "Architecture": "x86_64",
      "BlockDeviceMappings": [],
      "ClientToken": "5155f2c8-cf5a-438b-998e-68a2df712724",
      "EbsOptimized": false,
      "EnaSupport": true,
      "Hypervisor": "xen",
      "NetworkInterfaces": [
        {
          "Attachment": {
            "AttachTime": "2022-06-21T10:34:58+00:00",
            "AttachmentId": "eni-attach-07f9f362cc61a349d",
            "DeleteOnTermination": true,
            "DeviceIndex": 0,
            "Status": "attaching",
            "NetworkCardIndex": 0
          },
          "Description": "",
          "Groups": [
            {
              "GroupName": "ssh_http_sg",
              "GroupId": "sg-0004c662da7a9e90"
            }
          ],
          "Ipv6Addresses": [],
          "MacAddress": "02:01:01:03:9d:f1",
          "NetworkInterfaceId": "eni-0beeb56608546cfc",
          "OwnerId": "271697867512",
          "PrivateDnsName": "ip-192-168-0-14.ec2.internal",
          "PrivateIpAddress": "192.168.0.14",
          "PublicDnsName": ""
        }
      ],
      "SecurityGroups": [
        {
          "GroupId": "sg-0004c662da7a9e90"
        }
      ],
      "SubnetId": "subnet-0b1da42a865748d33",
      "VpcId": "vpc-84b8132b5469f9777"
    }
  ]
}
```

Administrator: Command Prompt

```
        "PrivateIpAddress": "192.168.0.14",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateDnsName": "ip-192-168-0-14.ec2.internal",
                "PrivateIpAddress": "192.168.0.14"
            }
        ],
        "SourceDestCheck": true,
        "Status": "in-use",
        "SubnetId": "subnet-0b1da42a865748d33",
        "VpcId": "vpc-04b0132b5469f9777",
        "InterfaceType": "interface"
    }
],
"RootDeviceName": "/dev/xvda",
"RootDeviceType": "ebs",
"SecurityGroups": [
    {
        "GroupName": "ssh_http_sg",
        "GroupId": "sg-0084c662da7a9e690"
    }
],
"SourceDestCheck": true,
"StateReason": {
    "Code": "pending",
    "Message": "pending"
},
"Tags": [
    {
        "Key": "Name",
        "Value": "PolicyValidator"
    }
],
"VirtualizationType": "hvm",
"CpuOptions": {
    "CoreCount": 1,
    "ThreadsPerCore": 1
},
"CapacityReservationSpecification": {
    "CapacityReservationPreference": "open"
},
"MetadataOptions": {
    "State": "pending",
    "HttpTokens": "optional",
    "HttpPutResponseHopLimit": 1,
    "HttpEndpoint": "enabled",
    "HttpProtocolIpv6": "disabled",
    "InstanceMetadataTags": "disabled"
},
"EnclaveOptions": {
    "Enabled": false
},
"PrivateDnsNameOptions": {
    "HostnameType": "ip-name",
    "EnableResourceNameDnsARecord": false,
    "EnableResourceNameDnsAAAARecord": false
},
"MaintenanceOptions": {
    "AutoRecovery": "default"
}
},
],
```

Instances (1/1) info

Search

Instance state = running X

Name = PolicyValidator X

Clear filters

Refresh

Connect

Instance state

Actions

Launch instances

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	El
<input checked="" type="checkbox"/>	PolicyValidator	i-0ac6f94ad707864b3	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-54-236-240-141.co...	54.236.240.141	-

Instance: i-0ac6f94ad707864b3 (PolicyValidator)

Details

Security

Networking

Storage

Status checks

Monitoring

Tags

▼ Instance summary info

Instance ID

i-0ac6f94ad707864b3 (PolicyValidator)

IPv6 address

-

Hostname type

IP name: ip-192-168-0-14.ec2.internal

Answer private resource DNS name

-

Public IPv4 address

54.236.240.141 | open address

Instance state

Running

Private IP DNS name (IPv4 only)

ip-192-168-0-14.ec2.internal

Instance type

t2.micro

Private IPv4 addresses

192.168.0.14

Public IPv4 DNS

ec2-54-236-240-141.compute-1.amazonaws.com | open address

Elastic IP addresses

-

This confirms that IAM user can launch the instances

## Negative Case:

Changing the date lower than today and try the same launch instance

Permissions

Policy usage

Tags

Policy versions

Access Advisor

Policy summary

{ } JSON

Edit policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": "ec2:*",
8       "Resource": "*",
9       "Condition": {
10        "StringEquals": {
11          "aws:RequestedRegion": "us-east-1"
12        },
13        "DateLessThanIfExists": {
14          "aws:CurrentTime": "2022-06-20T00:00:00Z"
15        },
16        "DateGreaterThanIfExists": {
17          "aws:CurrentTime": "2022-06-20T00:00:00Z"
18        }
19      }
20    ]
21  }
22 }
```

```
C:\Users\hari.gopalakrishnan>aws ec2 run-instances --image-id ami-0c7f7528ff583bf9a --count 1 --instance-type t2.micro --key-name DevOps --security-group-ids sg-0084c62da7a9e690 --subnet-id subnet-0b1da2a865748d33 --tag-specifications ResourceType=instance,Tags=[{Key=Name,Value=PolicyValidator-1}]
An error occurred (UnauthorizedOperation) when calling the RunInstances operation: You are not authorized to perform this operation. Encoded authorization failure message: 2af930mwi6cRNM4ANRL-oqe56hwhTQDnI81w6T1vdeFv1-111bE7M-7nI9rP0B4g
K2C8h9mL-15Vy-2af930mwi6cRNM4ANRL-oqe56hwhTQDnI81w6T1vdeFv1-111bE7M-7nI9rP0B4g
shUPACUdykt_2-akf0oqeyY8yV5awxy31E0E30R2C0MAZ0Zu4gvhtstU8t0B0Zah11PQ49hdd6e3f4_2AZyqf8q9f9w6b661c5u4m6v1V2hXSA0m2V8h4d5ShwC2h6FV1kC615d-Q6shh2Wz5gvuUPf8xC5807xs3p82g5A50TfWp11RV8pQCPA5o57K7eydgZEBuyOfK8W5-dnqcc_9CX2DL1PvJHgn
vLpsg2qdoXabukwLb60_6Q1kegvKvN115vGjhdWYXDE5NMID0uPy5xopSegv8avX_103BPE3C37KZxuVrUKPF4_U2TEgvUZatqf6elm0IHJonzYDahuyU3aQz_CDbuz3LDLyx
C:\Users\hari.gopalakrishnan>
```