

Federator.ai - AWS IAM Role and IAM Policy Setup Guide

- [Get an external ID](#)
- [Setup AWS IAM policy for Federator.ai](#)
- [AWS permissions](#)
 - [Required AWS IAM Policy](#)
- [AWS IAM role for Federator.ai](#)
- [Add AWS VM/ASG Clusters to Federator.ai](#)

For allowing [ProphetStor Federator.ai](#) AWS account to query AWS EC2/ASG/CloudWatch APIs, you need to create an IAM role and IAM policy in your AWS account for Federator.ai pulling metadata/metrics from EC2/ASG/CloudWatch. This document will provide you with details steps for setting up an AWS IAM role and IAM policy and then completing the configuration process of adding AWS VM/ASG clusters to Federator.ai.

Get an external ID

1. Get the external ID from Federator.ai “Add Cluster” page (choose Configuration → Clusters → Add Cluster). For more information about AWS external ID, please refer to the [IAM User Guide](#) AWS document.

The screenshot shows the 'Add Cluster' configuration interface. It features several input fields and options: a text field for 'Cluster' name, radio buttons for 'Cluster Type' (Kubernetes Cluster and VM Cluster), radio buttons for 'Metrics Data Source' (vCenter and AWS CloudWatch), radio buttons for 'AWS IAM Role' and 'AWS Access Keys', a dropdown for 'Region' (US East (N. Virginia)), a text field for 'AWS External ID' (highlighted with a red box), and a text field for 'AWS IAM Role ARN'. There is a 'Generate New ID' button next to the AWS External ID field. At the bottom, there is a checkbox for 'Collect Historical Data' and three buttons: 'Cancel', 'Test Connection', and 'Save'.

Setup AWS IAM policy for Federator.ai

2. create a new IAM policy in the [AWS IAM Console](#).

3. select **JSON** tab, and paste the Required **AWS permissions** in the textbox. Name policy `federatorai-integration-policy` or one of your own choosing.

Step 1
[Specify user details](#)

Step 2
Set permissions

Step 3
Review and create

Set permissions


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](#)

Permissions options

- Add user to group**
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions**
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly**
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1141)

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

< 1 2 3 4 5 6 7 ... 58 >  [Create policy](#)

<input type="checkbox"/>	Policy name	▲	Type	▼	Attached entities	▼
--------------------------	-----------------------------	---	------	---	-----------------------------------	---

Create policy

1 2 3

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor

JSON

[Import managed policy](#)

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Action": [  
6         "autoscaling:Describe*",  
7         "cloudwatch:Describe*",  
8         "cloudwatch:Get*",  
9         "cloudwatch:List*",  
10        "ec2:Describe*",  
11      ]  
12    }  
13  ]  
14 }
```

🛡️ Security: 0 🚫 Errors: 0 ⚠️ Warnings: 0 💡 Suggestions: 0

Policies > federatorai-integration-policy

Summary

[Delete policy](#)

Policy ARN arn:aws:iam:: :policy/federatorai-integration-policy [🔗](#)

Description federatorai-integration-policy

[Permissions](#)
[Policy usage](#)
[Tags](#)
[Policy versions](#)
[Access Advisor](#)

[Policy summary](#)
[{} JSON](#)
[Edit policy](#)
[?](#)

Q Filter

Service ▾	Access level	Resource	Request condition
Allow (5 of 369 services) Show remaining 364			
CloudWatch	Full: List, Read	All resources	None
EC2	Limited: List	All resources	None
EC2 Auto Scaling	Full: Read Limited: List	All resources	None
Resource Group Tagging	Limited: Read	All resources	None
Support	Full access	All resources	None

AWS permissions

AWS IAM policy defines the AWS permissions that you assign to Federator.ai and enables Federator.ai to pull metadata/metrics from AWS EC2/ASG/CloudWatch.

Required AWS IAM Policy

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": [
6         "autoscaling:Describe*",
7         "cloudwatch:Describe*",
8         "cloudwatch:Get*",
9         "cloudwatch:List*",
10        "ec2:Describe*",
11        "support:*",
12        "tag:GetResources",
13        "tag:GetTagKeys",
14        "tag:GetTagValues"
15      ],
16      "Effect": "Allow",
17      "Resource": "*"
18    }
19  ]
20 }
21

```

Policy	DESCRIPTION
cloudwatch:ListMetrics	List the available CloudWatch metrics.
cloudwatch:GetMetricData	Get data points for a described metric.
cloudwatch:Describe*	DescribeAlarmHistory DescribeAlarms DescribeAlarmsForMetric

	DescribeAnomalyDetectors DescribeInsightRules
tag:getResources	Get custom tags by resource type.
tag:getTagKeys	Get tag keys by region.
tag:getTagValues	Get tag values by region.
autoscaling:DescribeAutoScalingGroups	List all Auto Scaling groups.
autoscaling:DescribeAutoScalingInstances	Gets information about the Auto Scaling instances in the account and Region.
autoscaling:DescribePolicies	List available policies (for autocompletion in events and monitors).
autoscaling:DescribeTags	List tags for an Auto Scaling group. This will add ASG custom tags on ASG CloudWatch metrics.
autoscaling:DescribeScalingActivities	Generate events when an ASG scales up or down.
ec2:DescribeInstanceStatus	Describes the status of the specified instances or all of your instances.
ec2:DescribeInstanceTypes	Describes the details of the instance types that are offered in a location.
ec2:DescribeVolumes	Describes the specified EBS volumes or all of your EBS volumes.
ec2:DescribeSecurityGroups	Adds SecurityGroup names and custom tags to ec2 instances.
ec2:DescribeTags	Describes the specified tags for your EC2 resources.
ec2:DescribeInstances	Adds tags to ec2 instances and ec2 cloudwatch metrics.
support:*	Add metrics about service limits. <small>It requires full access because of AWS limitations</small>

For the details of actions of AWS IAM policy, please refer to [AWS EC2 API Actions](#), [EC2 Auto Scaling API Actions](#), and [CloudWatch API Actions](#).

AWS IAM role for Federator.ai

Create an IAM role for Federator.ai to use AWS permissions defined in `federatorai-integration-policy` IAM policy.

4. Create a new role in the AWS [IAM Console](#).
5. Select **AWS account** for the trusted entity type and **Another AWS account**.

Select trusted entity [Info](#)

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
- 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)**
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**
Requires that the assuming entity use multi-factor authentication.

6. Enter ProphetStor Federator.ai AWS account ID `635005593121` as **Another AWS account ID**. This grants Federator.ai access AWS EC2/ASG/CloudWatch APIs to pull your AWS EC2/ASG/CloudWatch metadata/metrics.

7. Select **Require external ID** and leave **Require MFA** disabled, then enter the external ID copied in the **Get an external ID** section. For more information, please refer to the [IAM User Guide AWS](#) document.

8. Search `federatorai-integration-policy` and attach `federatorai-integration-policy` policy to the IAM role and click **Next**.

Add permissions [Info](#)

Permissions policies (Selected 1/920) [Info](#)

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

1 match < 1 > [Settings](#)

"federatorai-integration-policy" [X](#) [Clear filters](#)

<input checked="" type="checkbox"/>	Policy name ↗	Type	Description
<input checked="" type="checkbox"/>	+ federatorai-integration-...	Custom...	federatorai-integration-policy

▶ Set permissions boundary - optional [Info](#)

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

9. Enter an IAM role name, such as `FederatorAIIntegrationRole` and Description for the IAM role.

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

`FederatorAIIntegrationRole`

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

Description

Add a short explanation for this role.

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

Step 1: Select trusted entities

Edit

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Action": "sts:AssumeRole",
7-       "Principal": {
8-         "AWS": "arn:aws:iam::[redacted]:role/[redacted]"
9-       },
10-      "Condition": {
11-        "StringEquals": {
12-          "sts:ExternalId": "[redacted]"
13-        }
14-      }
15-    }
16-  ]
17- }
```

Step 2: Add permissions

Edit

Policy name	Type	Attached as
federatorai-integration-policy	Customer managed	Permissions policy

10. Create `FederatoraiIntegrationRole` IAM role.

11. Copy your AWS `FederatoraiIntegrationRole` ARN, such as `arn:aws:iam::[AccountID]:role/FederatoraiIntegrationRole` for Federator.ai used later.

IAM > Roles > `FederatoraiIntegrationRole`

FederatoraiIntegrationRole

Delete

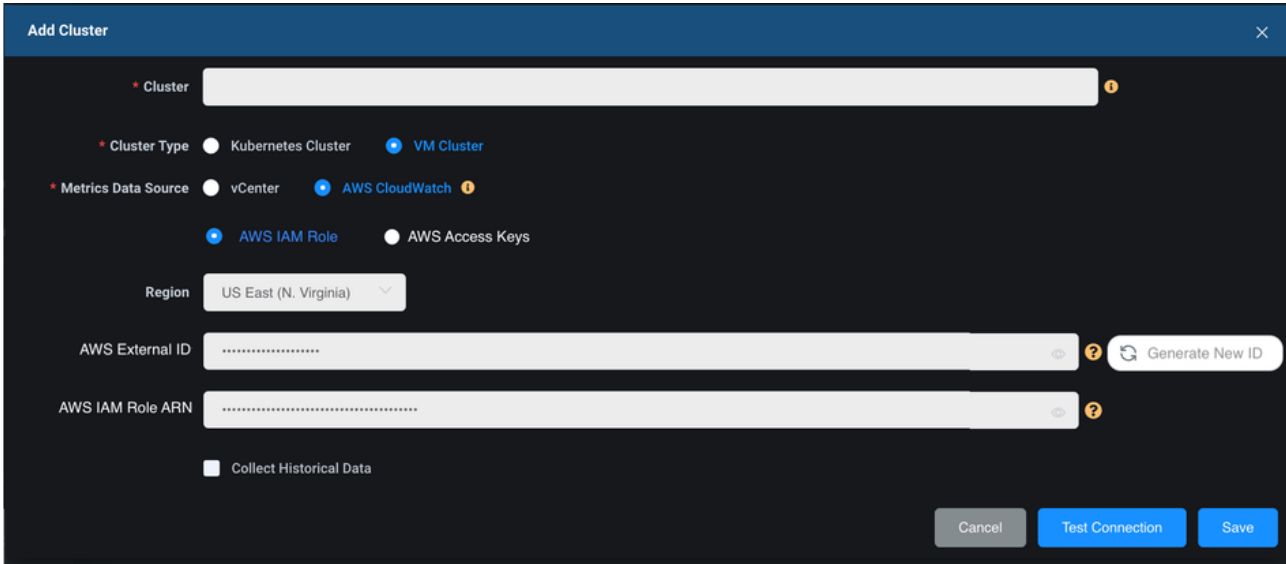
Summary

Edit

Creation date April 12, 2023, 16:07 (UTC+08:00)	ARN <code>arn:aws:iam::[redacted]:role/FederatoraiIntegrationRole</code>	Link to switch roles in console <code>https://signin.aws.amazon.com/switchrole?roleName=FederatoraiIntegrationRole&account=[redacted]</code>
Last activity None	Maximum session duration 1 hour	

Add AWS VM/ASG Clusters to Federator.ai

- In Federator.ai UI, choose Configuration → Clusters → Add Cluster
- Enter a cluster name
- Select **VM Cluster** as Cluster Type
- Select **AWS CloudWatch** for Metrics Data Source
- Select **AWS IAM Role**
- Select the **Region** of your AWS VM/ASG cluster
- Paste your AWS IAM role `FederatoraiIntegrationRole` ARN, such as `arn:aws:iam::{AccountID}:role/FederatoraiIntegrationRole` to **AWS IAM Role ARN** field.



The screenshot shows the 'Add Cluster' form in the Federator.ai UI. The form is titled 'Add Cluster' and has a close button (X) in the top right corner. The form contains the following fields and options:

- Cluster**: A text input field with a red asterisk and a help icon (i).
- Cluster Type**: Radio buttons for 'Kubernetes Cluster' and 'VM Cluster'. 'VM Cluster' is selected.
- Metrics Data Source**: Radio buttons for 'vCenter' and 'AWS CloudWatch'. 'AWS CloudWatch' is selected.
- AWS IAM Role**: Radio buttons for 'AWS IAM Role' and 'AWS Access Keys'. 'AWS IAM Role' is selected.
- Region**: A dropdown menu showing 'US East (N. Virginia)'.
- AWS External ID**: A text input field with a red asterisk, a help icon (i), and a 'Generate New ID' button.
- AWS IAM Role ARN**: A text input field with a red asterisk and a help icon (i).
- Collect Historical Data**: A checkbox that is currently unchecked.

At the bottom of the form, there are three buttons: 'Cancel', 'Test Connection', and 'Save'.

- Click `Save` to add an AWS VM/ASG cluster.
- Select AWS VMs/ASG for the cluster.

* Cluster ⓘ

* Cluster Type Kubernetes Cluster VM Cluster

* Metrics Data Source vCenter AWS CloudWatch ⓘ

Region ▾

AWS External ID ⓘ

AWS IAM Role ARN ⓘ

Collect Historical Data: from 2023/01/10 to 2023/04/10

Status: Completed

Scaling Group Individual VMs Auto Scaling Group

Non-Members 0/3

- k8s-1-1 - stopped
- i-0674fd7edc0fda307 - stopped
- k8s-1 - stopped

Add >

< Remove

Members 0/2

- Demo_Spot - running
- Demo_Ondemand - running

Cancel

Test Connection

Save