

Infrastructure Monitoring By Using New Relic

- Go to New Relic and login there one of option called
- Infrastructure click on it
- And go to AWS
- Create new role for new relic and give read only access permission.

Select trusted entity

Trusted entity type

<input type="radio"/> AWS service Allow AWS services like EC2, Lambda, or others to perform actions in this account.	<input checked="" type="radio"/> AWS account Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.	<input type="radio"/> Web identity Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
<input type="radio"/> SAML 2.0 federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.	<input type="radio"/> 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 (512771275801)

☒ Another AWS account

Account ID

Identifier of the account that can use this role

3619358

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

3619358

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.

Permissions policies (Selected 1/777)

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

Filter policies by property or policy name and press enter

150 matches

< 1 2 3 4 5 6 7 8 >

ReadOnlyAccess X

Clear filters

	Policy name	Type	Description
<input type="checkbox"/>	AmazonVPCReadOnlyAccess	AWS m...	Provides read only access to Amazon VPC via the AWS Management Console.
<input type="checkbox"/>	CloudWatchEventsReadOnlyAcc...	AWS m...	Provides read only access to Amazon CloudWatch Events.
<input type="checkbox"/>	AmazonMQApiReadOnlyAccess	AWS m...	Provides read only access to AmazonMQ via our API/SDK.
<input type="checkbox"/>	AWSCodePipelineReadOnlyAccess	AWS m...	Provides read only access to AWS CodePipeline via the AWS Management Console.
<input checked="" type="checkbox"/>	ReadOnlyAccess	AWS m...	Provides read-only access to AWS services and resources.
<input type="checkbox"/>	AmazonRekognitionReadOnlyAcc...	AWS m...	Access to all Read rekognition APIs
<input type="checkbox"/>	AWSCodeDeployReadOnlyAccess	AWS m...	Provides read only access to CodeDeploy resources.
<input type="checkbox"/>	AmazonSESReadOnlyAccess	AWS m...	Provides read only access to Amazon SES via the AWS Management Console.
<input type="checkbox"/>	AWSWAFReadOnlyAccess	AWS m...	Provides read only access to AWS WAF actions.
<input type="checkbox"/>	AmazonKinesisReadOnlyAccess	AWS m...	Provides read only access to all streams via the AWS Management Console.
<input type="checkbox"/>	AWSCloudMapReadOnlyAccess	AWS m...	Provides read-only access to all AWS Cloud Map actions.
<input type="checkbox"/>	AmazonElasticCacheReadOnlyAccess	AWS m...	Provides read-only access to Amazon ElasticCache via the AWS Management Console.

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

newrelic-iam-role

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

Description

Add a short explanation for this role.

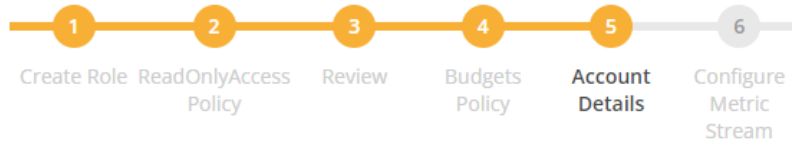
newrelic-iam-role

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": "754728514883"
9       },
10      "Condition": {
11        "StringEquals": {
12          "sts:ExternalId": "3619358 "
```



[< Back to Step 4](#)

Step 5: Add Account Details

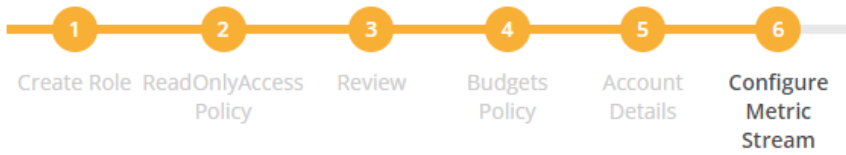
Add your AWS account name as it will show in the New Relic UI.

Changing the AWS account name is not recommended. Doing so may break New Relic Insights widgets, dashboards, and data apps created by your New Relic users.

Paste the ARN created in the previous step

Cancel Setup

Next



[< Back to Step 5](#)

Step 6: Configure AWS Metric Stream

Almost there!

To start receiving data, configure AWS metric streams to send your CloudWatch metrics to New Relic via AWS Kinesis Data Firehose.

Use the automated process via CloudFormation: [Use the CloudFormation Template](#)

Or complete the setup via AWS Console / API: [Manual setup documentation](#).

Done

Managed Kafka

Neptune

RDS

Route 53

S3

SNS

Step Functions

Trusted Advisor

WAF

X-Ray

MediaPackage VOD

QLDB

Redshift

Route53 Resolver

SES

SQS

Transit Gateway

VPC

WAFV2

☒

EC2 ?

Cancel Setup

Next

ams

age VOD

:solver

eway

We're setting up your integration

New Relic is retrieving monitoring data from AWS account Ronak Prajapati and configuring AWS dashboards in New Relic Insights. This may take up to 5 minutes.

OK

- New Relic Dashboard for AWS View Services EC2,S3

AWS services
[Learn how](#) to monitor your AWS services with New Relic Infrastructure

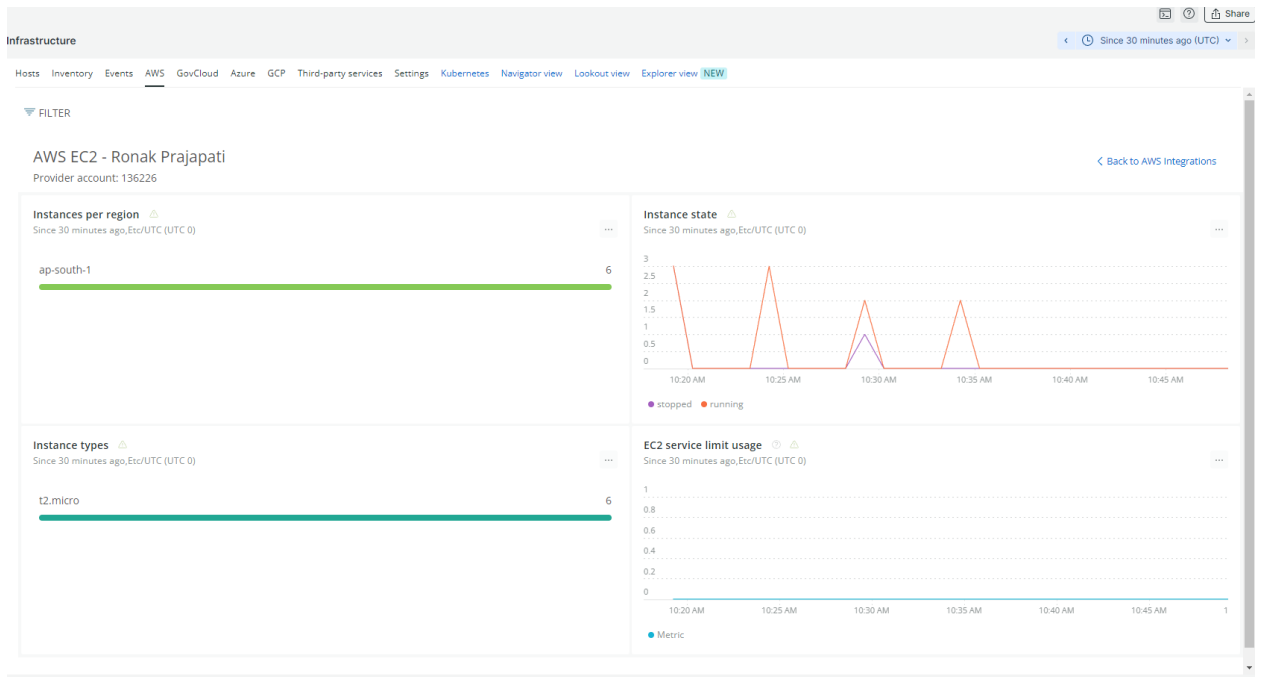
+ Add an AWS account

API Ronak Prajapati

Provider account: 136226

INTEGRATION NAME ^ DASHBOARDS CONFIGURE CREATE ALERT EXPLORE DATA DOCUMENTATION

EC2 EC2 dashboard Configure Set Alert | Alert API Info EC2 data EC2 Documentation



AWS services
[Learn how](#) to monitor your AWS services with New Relic Infrastructure

+ Add an AWS account

API Ronak Prajapati

Provider account: 136226

INTEGRATION NAME ^ DASHBOARDS CONFIGURE CREATE ALERT EXPLORE DATA DOCUMENTATION

EC2 EC2 dashboard Configure Set Alert | Alert API Info EC2 data EC2 Documentation

S3 S3 dashboard Configure Set Alert | Alert API Info S3 data S3 Documentation