Implementation Guide:

Integrating New Relic with AWS Control Tower

Quick Starts Reference Deployment

Table of Contents

Foreword 3
Solution Overview 4
Architecture Diagram 5
Prerequisites 6
Deploying the Solution 6
New Relic and AWS: Better Together 7
Pricing 8
Tearing it Down 8
Partner FAQs 8
Troubleshooting 10
Partner contact information 10

Foreword

New Relic is an AWS Partner Network (APN) Advanced Technology Partner focused on delivering observability as a platform, to help you create more perfect software. New Relic One is New Relic's observability platform that is open, connected, and programmable. For more information, see New Relic in AWS Marketplace.

AWS Control Tower leverages AWS best practices to easily set up a scalable, secure, well-architected, multi-account environment, referred to as a landing zone. The Account factory automates the provisioning of new accounts in your AWS environment. You can enable self-service for your teams to configure and provision new accounts using AWS Service Catalog. After you have set up your landing zone, you need operational insights into your multi-account environment.

The purpose of this AWS Implementation Guide is to enable you to seamlessly deploy, and as a result, automatically monitor your AWS Control Tower landing zone with New Relic's AWS integration.

Solution Overview

New Relic AWS Control Tower integration solution allows you to streamline the observability of your landing zone with New Relic. With this solution, enrolled accounts in your Control Tower managed organization are automatically monitored with your New Relic account, from the moment they are launched. It also lets you link existing accounts with New Relic, in case you've already set up your landing zone. You can then manage all your AWS operational data and insights from one place, with no need to hop back and forth between multiple AWS accounts or other set of observability tools.

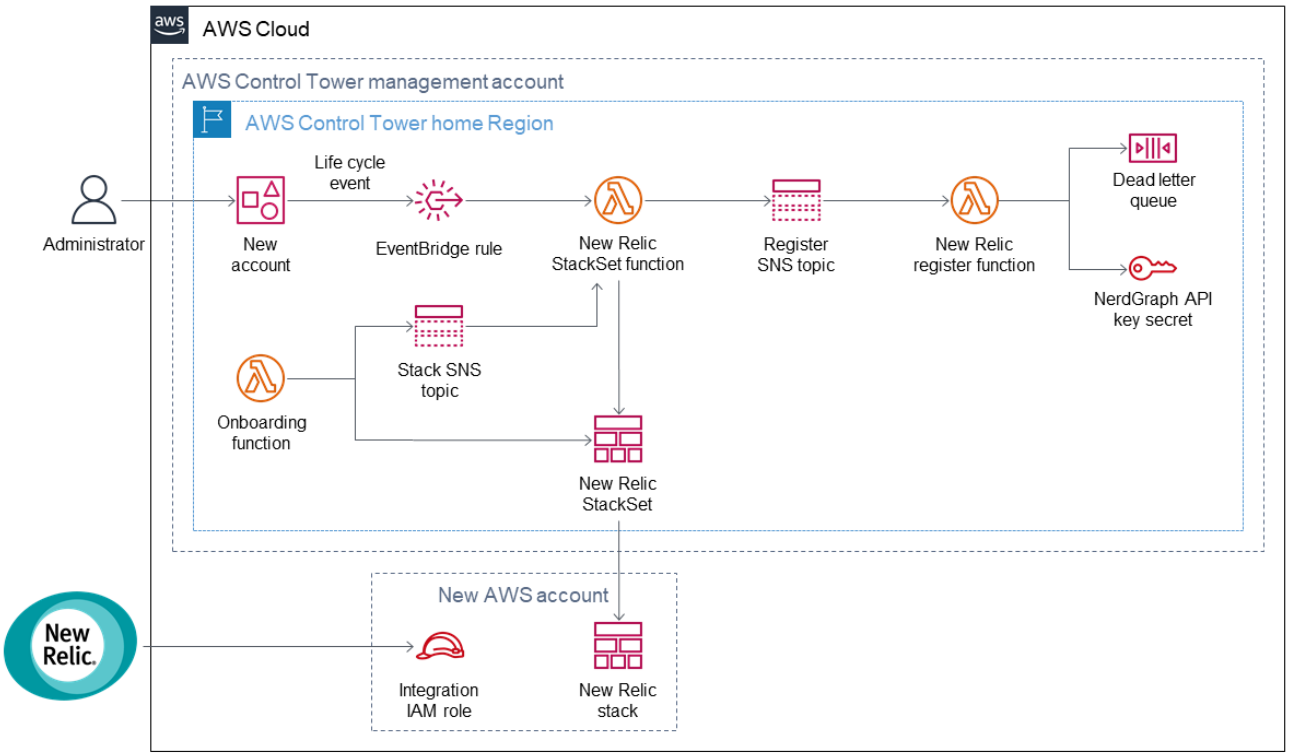
New Relic AWS integrations combines configuration monitoring and real-time health metrics with a dynamic, tag-driven approach to observability to give your DevOps teams full visibility of your diverse AWS infrastructure. It also supports seamless deployments of your workloads using AWS Outposts. For a list of the supported services and the data that can be collected, visit AWS integrations list.

New Relic AWS integrations require you to grant New Relic permission to read operational telemetry data from your AWS account. This is achieved by using an AWS IAM role, referred to as "New Relic Integration", that uses AWS Identity and Access Management (IAM) cross-account access. New Relic AWS integrations use the Amazon CloudWatch API to obtain telemetry data for the AWS services you monitor.

The solution is open source, and the code is available in AWS QuickStart GitHub repository. You must deploy the solution in your AWS Control Tower management account in the home Region. This is the Region where your AWS Control Tower landing zone was set up. This solution uses AWS CloudFormation for its deployment.

Architecture Diagram

The following architecture diagram illustrates the deployment view of the solution in an AWS Control Tower environment.



Let's walk through the resources deployed as part of the solution:

- An Amazon EventBridge rule that accepts a lifecycle event, delivered to it every time an administrator successfully enrolls a new or existing AWS account in AWS Control Tower.
- A Lambda function, named Onboarding that's launched as an AWS CloudFormation custom resource and creates an AWS CloudFormation StackSet, named New Relic StackSet. The StackSet includes the New Relic cross-account trust IAM role.
- An Amazon SNS topic named StackSet that the Onboarding function posts a message to, once the New Relic StackSet is successfully created.
- A Lambda function, named New Relic StackSet, that is triggered by
    - StackSet Amazon SNS topic (Onboarding function)
    - EventBridge rule (lifecycle event)

  The function launches the New Relic stack in
    - (Optional) all the existing accounts (enrolled before the Quick Start is deployed) that were passed when launching the Quick Start
    - all the newly enrolled accounts (enrolled after the Quick Start is deployed)

- An Amazon SNS topic named Register that the New Relic StackSet function posts a message to, once the New Relic stack is successfully created in the newly enrolled account or in each existing account.
- A secret, named New Relic NerdGraph API key retrieved from AWS Secrets Manager (not shown).
- A Lambda function, named New Relic Register, that is triggered by the StackSet Amazon SNS topic, and that invokes the New Relic NerdGraph mutation endpoint to link your AWS account with your New Relic account.
- An Amazon SQS dead letter queue that collects any messages that the New Relic Register function fails to process

Prerequisites

You need the following to implement New Relic's integration with AWS Control Tower:

- Fully deployed AWS Control Tower. For information about setting up an AWS Control Tower landing zone, see Getting Started with AWS Control Tower. You also need administrator privileges in the AWS Control Tower management account.
- An active New Relic account with Standard or higher pricing tier subscription, when using the New Relic One pricing plan. Don't have an account yet? Sign up for a perpetually free access to New Relic, which includes 100 GB of data ingest per month, one full access user and unlimited basic users. With your New Relic One pay-as-you-go plan, you only pay for what you use beyond the free tier each month.

Deploying the Solution

Now let's deploy the solution in your AWS Control Tower environment. At a high level, deployment involves following steps:

1. Make sure you have access to your New Relic account, or sign up for your free New Relic account. Take note of your New Relic Account ID and User key.
2. Using AWS CloudFormation, use the New Relic provided template to launch a stack in your AWS Control Tower management account in your "home" Region. To monitor any existing accounts enrolled in your Control Tower managed organization with New Relic, supply the list of those account IDs (as comma separated string for `LaunchAccountList` parameter) while launching the stack.
3. Use Account factory to vend and enroll one or more new AWS accounts. These new accounts will be automatically monitored with New Relic, from the moment they are launched.

Step 1.1: Make sure you have an active New Relic account

Make sure you have an active New Relic account with Standard or higher pricing tier, when using the New Relic One pricing plan, or signup for a perpetually free New Relic account.

Step 1.2: Take note of your New Relic account ID and User key

Log into your New Relic account. Take note of your New Relic account ID and NerdGraph User API key (User key). This solution uses New Relic NerdGraph API for linking your AWS accounts with New Relic.

Step 2: Launch AWS CloudFormation stack

1. Log in to your AWS Control Tower management account. This is the AWS account where AWS Control Tower is deployed.
2. Verify that you are in your "home" Region (where AWS Control Tower is deployed).
3. Launch the stack using the following NewRelic-ControlTowerCustomization QuickStart link. In the Parameters section:
    a. Enter your **New Relic Account ID** and **New Relic NerdGraph User Key**
    b. Optional: Enter **Existing AWS accounts list** (the comma separated list of existing AWS account IDs) that you wish to monitor with New Relic.
4. Select **Next** and create the stack.

Step 3: Verify New Relic Integration

Once a new account is enrolled into AWS Control Tower, it is automatically set up to allow your New Relic account to ingest operational telemetry data via Amazon CloudWatch and other AWS services supported by New Relic integration.

1. Log into your New Relic account, and then hover over the **Infrastructure** link on the top navigation bar and select the AWS menu item from the menu list.
2. You will be taken to the **AWS** page. If you happen to have access to multiple New Relic accounts, begin by choosing the New Relic account that you used for this implementation, from the account list **in the header panel next to New Relic ONE logo**. Otherwise, you should see your New Relic account show up in that place.
3. Make sure the account ID matches the one you used in this implementation. Your new AWS account will be listed in the screen.
4. Click on Account status dashboard link to view the account dashboard.

After waiting a few minutes, if you still do not see data for your AWS integrations in the account status dashboard, follow the suggestions in the Troubleshooting AWS integrations guide. Note that New Relic can obtain monitoring data from services and endpoints that are located in all AWS regions except from China regions.

New Relic and AWS: Better Together

Learn more about New Relic and AWS partnership at New Relic and AWS.

Pricing

There are two components to the overall price you should expect to pay. First is the cost of data ingested into your New Relic account. With New Relic, you get the first 100 GB of data for free, every month, and then pay $0.25 per GB of data ingested beyond the free limit. For more details on how New Relic is priced, see New Relic Pricing. The second component of the price is your AWS bill largely owing to the Amazon CloudWatch API calls. New Relic AWS integrations use the CloudWatch API to obtain telemetry data for the AWS services you monitor. The number of calls to the CloudWatch API increases as you enable more integrations, add AWS resources to those integrations, or scale those integrations across more Regions. For details on how CloudWatch API calls are charged, see Amazon CloudWatch pricing. There may be other components of your AWS bill including Network data transfer fee depending on your usage of New Relic infrastructure agents, running on your EC2 instances or your containers running on ECS or EKS.
Please refer to CloudWatch billing for information on how to manage the cost associated with New Relic AWS integrations.

Tearing it Down

If you intend to deploy the solution for testing and demonstration purposes and you don't intend to use New Relic AWS integrations any longer, you can Uninstall New Relic AWS integrations.

1. Remove the AWS CloudFormation stack
The time to complete this step depends on how many AWS accounts are included in your New Relic AWS Control Tower integration deployment. If deleting the AWS CloudFormation stack times out, it's safe to retry this step.

- Sign in to the AWS CloudFormation console in your Control Tower management account.
- Delete the New Relic AWS Control Tower integration stack to remove all AWS resources deployed by the stack. This also deletes all stack set instances, which include any IAM roles deployed for enrolled AWS accounts.
- When the stack is deleted, navigate to AWS CloudFormation StackSet, and search for the New Relic stack set to confirm it was removed.

2. Uninstall the New Relic integration
After you confirm that the AWS CloudFormation stack was removed, remove all linked accounts from New Relic. See Uninstall New Relic AWS integrations for details.

Partner FAQs

Can I purchase New Relic from the AWS Marketplace?

Yes! You can access and purchase New Relic One directly from the AWS Marketplace which offers pay-as-you-go pricing, including access to our perpetual free tier. For larger discounts, consider our Annual Pool of Funds offering.

What capabilities does New Relic provide?

New Relic is an observability platform that helps you build better software. You can bring in telemetry data from any source so that you can fully understand your system and how to improve it. To learn more, see Introduction to New Relic.

Can I ingest additional, external data into New Relic?

Yes. New Relic is best used as a single source of truth for operational data, regardless of the data's origins. In addition to New Relic's open-source instrumentation agents, New Relic provides out-of-the-box integrations open-source tools for ingesting data, such as Prometheus, Telegraf, FluentD, and Logstash. If these integrations don't work for you, New Relic's open-source Telemetry SDKs let you build your own integration.

New Relic offers several APIs for retrieving MELT (metrics, events logs, and traces) data types into without using an installed agent. New Relic also offers open-source telemetry integrations that report data from OpenCensus, OpenTelemetry, DropWizard, Prometheus, and more. New Relic's programmable platform lets you build New Relic One apps to connect system performance to business needs, such as business KPIs and customer engagements. For more information, see Get Data into New Relic.

What is the data retention period for my data in New Relic?

Data retention typically ranges from 8 to 395 days and the ability to edit data retention periods differs depending on your New Relic pricing plan. Reducing data retention below your contracted retention values will not reduce New Relic's data ingest charges. Conversely, increasing retention for targeted telemetry data types should trigger a conversation with New Relic about adjusting your data ingest charges. For more details, see Manage data retention.

Can I delete data from New Relic?

After telemetry data is reported to New Relic and available for querying, it cannot be edited or deleted. This is a purposeful design decision that optimizes New Relic's speed and performance, at scale. Data will expire (and will be purged) after its retention period ends.

How can I track my New Relic usage?

New Relic provides a UI for understanding your New Relic usage and managing your data. You can also query your usage data to get more detail than is available in the UI and set up alerts to get notifications about changes in your usage. To learn more, see Query and alert on billing/usage data.

How does New Relic ensure security and privacy of my data?

To learn about how New Relic ensures security, see New Relic Security. For further details, see Data privacy with New Relic and Security controls for privacy. For a list of compliance certifications, see Compliance certifications

How much does New Relic cost?

If you are an existing New Relic customer, see New Relic One billing. If you are new to New Relic, refer to New Relic pricing. For more details, contact New Relic Sales or see our Pricing and billing FAQs. You can also sign up for a perpetually free account that gives 100 GB of data ingest per month. You'll get access to all of New Relic's features, including a free license for Full-Stack Observability and Applied Intelligence.

Troubleshooting

I encountered a CREATE_FAILED error when I launched the Quick Start.

If AWS CloudFormation fails to create the stack, relaunch the template with **Rollback on failure** set to **Disabled**. This setting is in the AWS CloudFormation console under **Advanced** on the **Configure stack options** page. With this setting, the stack's state is retained, see Amazon CloudWatch for errors associated with the AWS Lambda function NewRelicOnboardingFunction.

I encountered a size-limitation error when I deployed the AWS CloudFormation templates.

Launch the Quick Start templates from the links in this guide or from another S3 bucket. If you deploy the templates from a local copy on your computer, or from a location other than an S3 bucket, you might encounter template-size limitations. For more information, see AWS CloudFormation quotas.

I included a list of AWS accounts during the deployment, but none of the accounts show up in New Relic's UI.

Ensure that your list includes only AWS account IDs that are managed by AWS Control Tower and that the account IDs are separated by commas. Also ensure that you deployed the stack in the "home" Region of your AWS Control Tower management account and that the New Relic account ID and NerdGraph User API key is correct. Lastly, inspect for any potential errors the Amazon CloudWatch logs for the AWS Lambda function NewRelicOnboardingFunction. If you can't troubleshoot using these techniques, refer to our Troubleshooting AWS integrations guide.

Partner contact information

AWS at New Relic, aws@newrelic.com