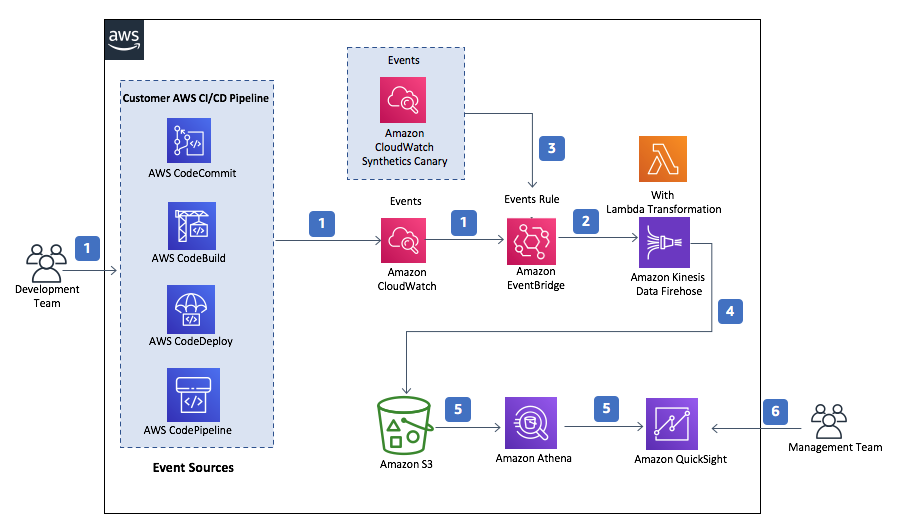
**Solution overview**

The following architectural diagram illustrates the workflow of the solution.



The workflow includes the following steps:

1. A developer initiates an activity in a CI/CD pipeline, such as pushing a code change to AWS CodeCommit or deploying an application using AWS CodeDeploy. These activities create events.
2. An [Amazon EventBridge](https://aws.amazon.com/eventbridge/) events rule detects the events based on predefined event patterns and then sends the event data to an [Amazon Kinesis Data Firehose](https://aws.amazon.com/kinesis/data-firehose/) delivery stream. One event rule is created per event source.
3. If a customer has set up an Amazon CloudWatch Synthetics canary and its Amazon CloudWatch alarm in their account, another events rule will capture events from the alarm that monitors the status of the canary. These resources are required to gather data for calculating MTTR metrics.
4. The Kinesis Data Firehose uses a Lambda function for data transformation. The Lambda function parses the raw event data to pass relevant data to the Firehose delivery stream, which in turn sends the data to an [Amazon Simple Storage Service](https://aws.amazon.com/s3/) (Amazon S3) bucket for downstream processing.
5. An [Amazon Athen](https://aws.amazon.com/athena/)a database points to the data in Amazon S3. It runs queries against the data and returns query results to [Amazon QuickSight](https://aws.amazon.com/quicksight/).
6. Amazon QuickSight obtains the query results and builds dashboard visualizations for the management team.

**Solution prerequisites**

1. You need to have a CI/CD pipeline that consists of AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy, and AWS CodePipeline in your account. For instructions, see  [Set Up a CI/CD Pipeline on AWS](https://aws.amazon.com/getting-started/projects/set-up-ci-cd-pipeline/) if you do not currently have a pipeline set up on AWS.

2. If you want to use the Amazon QuickSight visualization feature, you must subscribe to Amazon QuickSight Enterprise edition in the account where you deploy the solution. For instructions, see [Signing Up for an Amazon QuickSight Subscription](https://docs.aws.amazon.com/quicksight/latest/user/signing-up.html) in the Amazon QuickSight User Guide if you do not have a QuickSight Enterprise account set up.

Make a note of the QuickSight Principal [Amazon Resource Name](https://docs.aws.amazon.com/general/latest/gr/aws-arns-and-namespaces.html) (ARN). You will need it when you deploy the solution. To retrieve the Amazon QuickSight Principal ARN, you must have access to a shell or terminal with the AWS CLI installed. For installation instructions, see [What is the AWS Command Line Interface](https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html) in the AWS CLI User Guide. You can also use [AWS CloudShell](https://aws.amazon.com/cloudshell/) to run AWS CLI commands.

.

**Step 1: Launch the solution**

Launch the provided [AWS CloudFormation template](https://solutions-reference.s3.amazonaws.com/aws-devops-monitoring-dashboard/latest/aws-devops-monitoring-dashboard.template) to install the solution into your AWS account. The template has the following input parameters. You can modify them as needed.

|  |  |  |
| --- | --- | --- |
| Parameter | Default | Description |
| Athena Query Data Duration (Days) | 90 | Enter a duration (days) that Athena query uses to retrieve data. By default, Athena query retrieves data within the last 90 days. We recommend that you limit the duration to maximize performance and minimize cost. |
| AWS CodeCommit Repository List | ‘ALL’ | List of the names of AWS CodeCommit repositories that will be monitored. The names must be enclosed in single quotation marks and separated by commas (for example, *‘MyRepository1‘,’MyRepository2‘*). To monitor all the repositories, keep the default *‘ALL’* value. |
| S3 Transition Days | 365 | Enter the number of days after which you would like to transition Amazon S3 objects to Amazon S3 Glacier storage class. By default, objects are transitioned to Amazon S3 Glacier 365 days (one year) after creation. |
| Amazon QuickSight Principal ARN | <Optional Input> | Provide a QuickSight Admin user ARN (*arn:aws:quicksight:AWSRegion:AWSAccountId:user/default/QuickSightUserName*) to automatically create QuickSight dashboards. QuickSight Enterprise edition must be enabled for the account. To disable QuickSight dashboards creation, leave it blank. |
|

The stack takes approximately 10 minutes to deploy. After it’s successfully deployed, you should see that its status is CREATE\_COMPLETE in the AWS CloudFormation console.

*Note: If you provided an Amazon QuickSight Principal ARN, this solution launches a nested stack to create QuickSight resources into the account you provided.*

**Step 2: Configure Amazon QuickSight**

The solution uses Amazon QuickSight for data visualization. Follow these instructions to configure permissions and view datasets, analysis, and dashboards in Amazon QuickSight.

*Note: You can set up your own visualization tool if needed. For more information, see AWS DevOps Monitoring Dashboard Implementation Guide.*

1. After the stack is successfully deployed, go to the Outputs tab of the stack and make a note of the values for QSAnalysisURL, QSDashboardURL, and DevOpsMetricsS3Bucket.
2. Sign in to the [AWS Management Console](https://aws.amazon.com/console/) and navigate to Amazon QuickSight console.
3. Change the AWS Region in the URL to match the Region where you deployed the solution. For example, if you deployed the solution in the us-east-1 Region, the QuickSight URL will mirror the following path: *https://us-east-1.quicksight.aws.amazon.com/sn*.
4. In the upper right, choose your user name, and then choose Manage QuickSight.
5. From the left navigation pane, choose Security & permissions.
6. Under QuickSight access to AWS Services, choose Add or remove.
7. Select IAM, Amazon S3, and Amazon Athena. If these options are already selected, clear and then select the options again.
8. Choose Amazon S3, and then click the Details link.
9. Choose Select S3 buckets.
10. Select DevOpsMetricsS3Bucket, and then select the check box under Write permission for Athena Workgroup.
11. Choose Finish, and then choose Update.
12. On the Output tab of the stack, choose QSAnalysisURL and QSDashboardURL to open dashboard and analysis. You can also navigate to them in the QuickSight console. The solution creates one analysis, one dashboard, and a few datasets. All the QuickSight resources created by the solution are prefixed with the stack name (for example, *<stack-name>-dashboard*).

*Note: You might see a No Data message if the Amazon S3 metrics bucket is empty immediately after the solution is launched. Allow time for CI/CD activities to be sent to the solution. You can refresh the pages to view data and visuals after the solution finishes processing data and sends metrics to Amazon S3.*

**Step 3: Set up the canary and alarm**

The solution uses an Amazon CloudWatch Synthetics canary and Amazon CloudWatch alarm to collect data required for calculating MTTR metrics. Canaries are configurable scripts that run on a schedule to monitor your endpoints and APIs. An alarm is triggered when a canary job state changes (failure or success). The solution uses the alarm data to calculate the time it takes to restore a service, based on the interval between failure and success events.

Choose one of the following ways to set up the canary and its alarm:

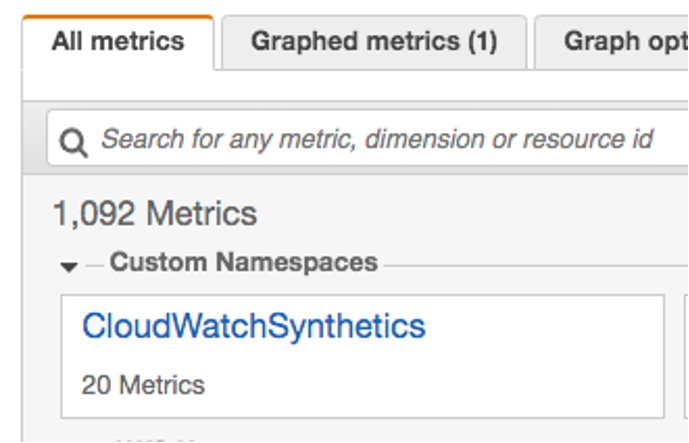
Automated setup (Recommended)

For your convenience, the solution provides a canary-alarm.template that you can deploy to create an alarm and/or canary in your account.

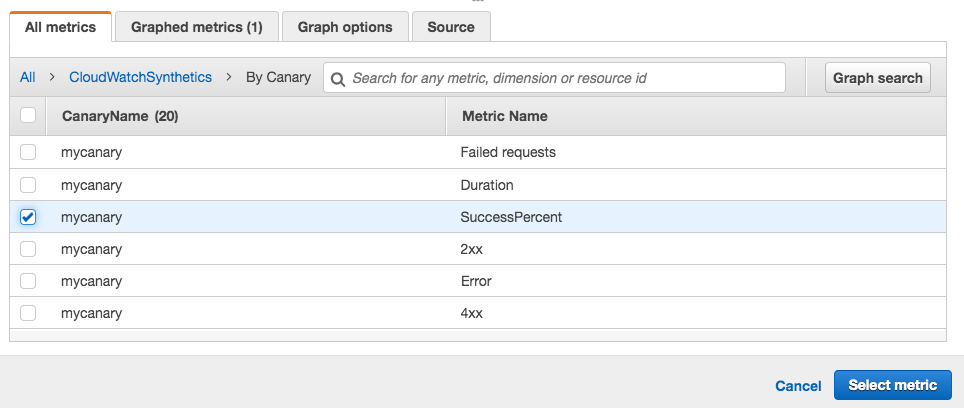
Manual setup

* If you don’t have a canary, follow [these steps](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Synthetics_Canaries_Create.html) to create one, otherwise go to next step.
* Follow [these steps](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/ConsoleAlarms.html) to create an alarm that monitors the state of the canary job. When you reach the step to select metrics, make sure you select CloudWatchSynthetics, your canary, and the SuccessPercent metric, as shown in the following two figures.

Select CloudWatchSynthetics metrics for the alarm.



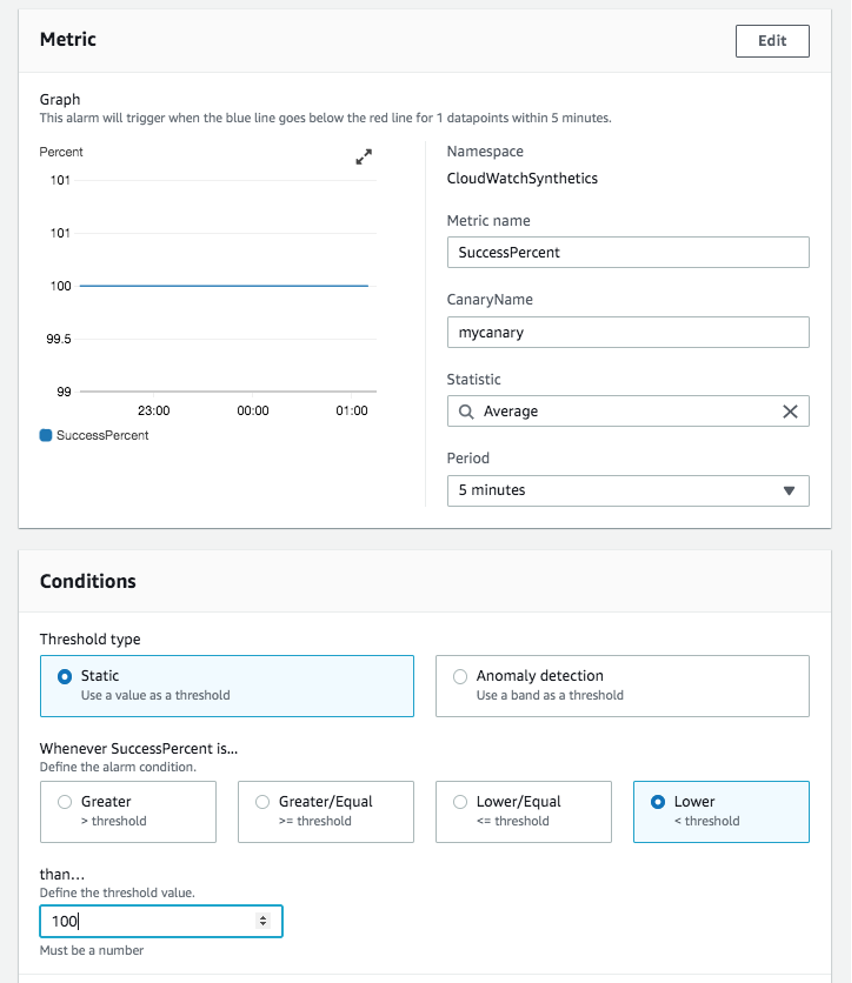
On the All metrics tab, search by canary, and then select your canary with the metric name of SuccessPercent.



Use this pattern for the alarm name: *SO0143-[my-application-name]-[my-repository-name]-MTTR* (for example, *SO0143-[MyDemoApplication]-[MyDemoRepo]-MTTR*). SO0143 is the solution ID. The application name is the name of the application that your canary monitors. The repository name is the name of the repository where the source code for your application resides. The solution uses the alarm name to determine if an alarm is used for MTTR metrics and which application and repository are associated with the metrics.

In the Conditions section, for Threshold type, choose Static. For Whenever SuccessPercent is, choose            Lower,  and enter a threshold value that fits your use case (for example, 100).

The following figure shows the alarm:



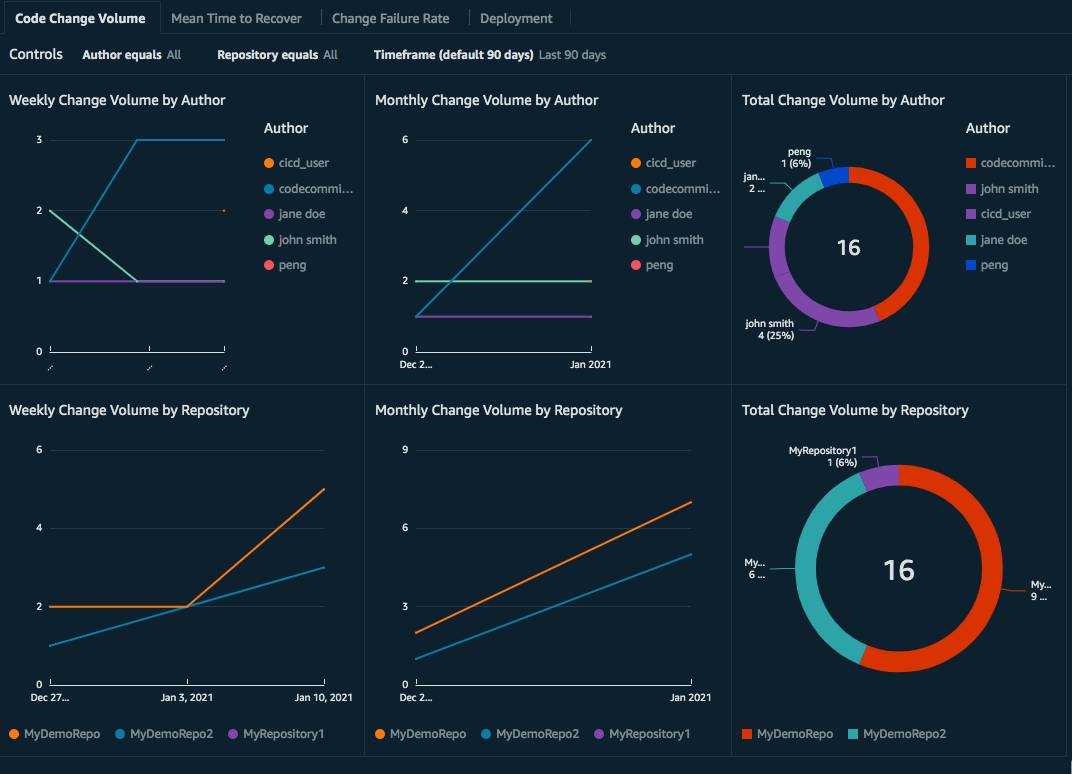
**Amazon QuickSight dashboard visualizations**

After the initial setup is done and the solution starts to process events data, you can view the metrics visualizations using Amazon QuickSight dashboards.

Let’s take a look at the dashboards available on Amazon QuickSight using data queried from Amazon Athena. By default, Amazon Athena queries retrieve data within the last 90 days to analyze and visualize DevOps metrics. This is an input parameter that can be configured by the user in the CloudFormation template. We recommend that you limit the data duration to maximize performance and minimize cost.

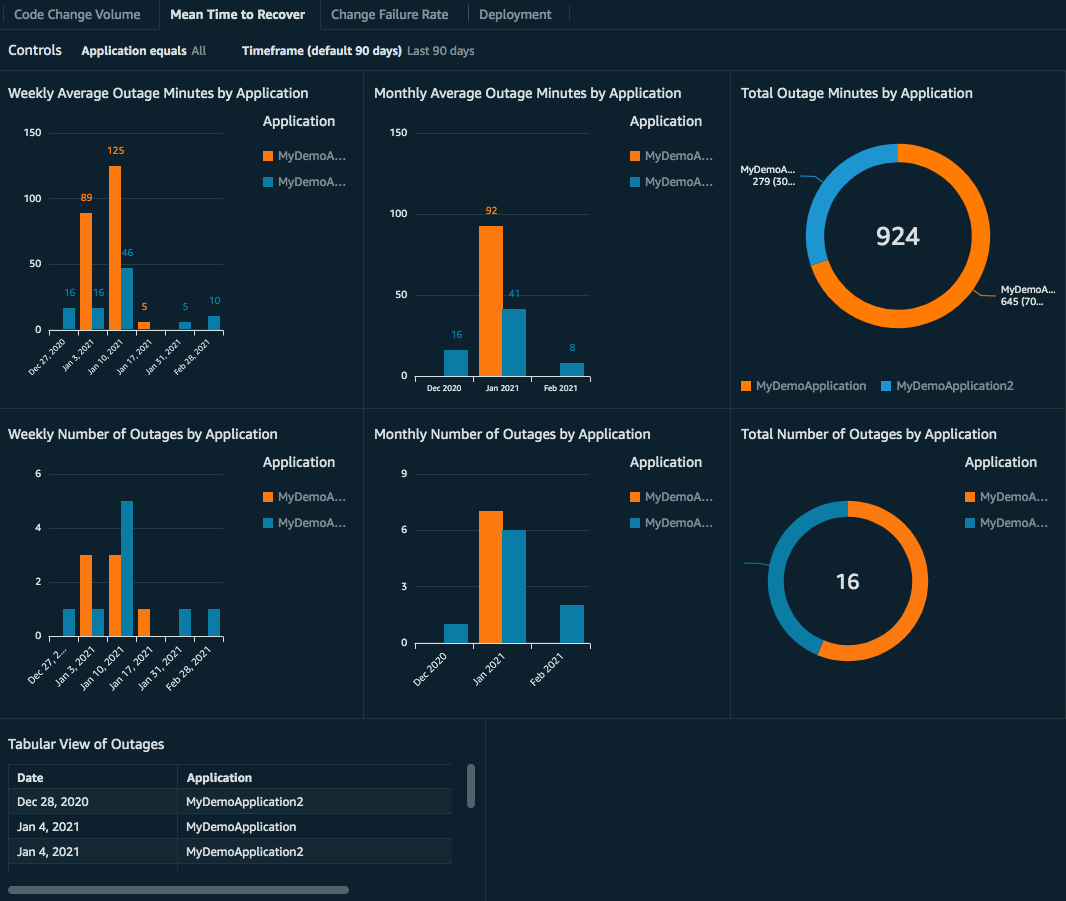
**Code change volume dashboards**

These dashboards display the number of code changes made by author and repository. They provide a weekly, monthly, and aggregated view of the metrics by author and repository. You can use the custom filter to filter data by author, repository, or time period. DevOps leaders can use this dashboard to improve visibility into the coding activities of their development teams. They can answer questions, such as who makes the most code changes and which repositories are the most active over time.



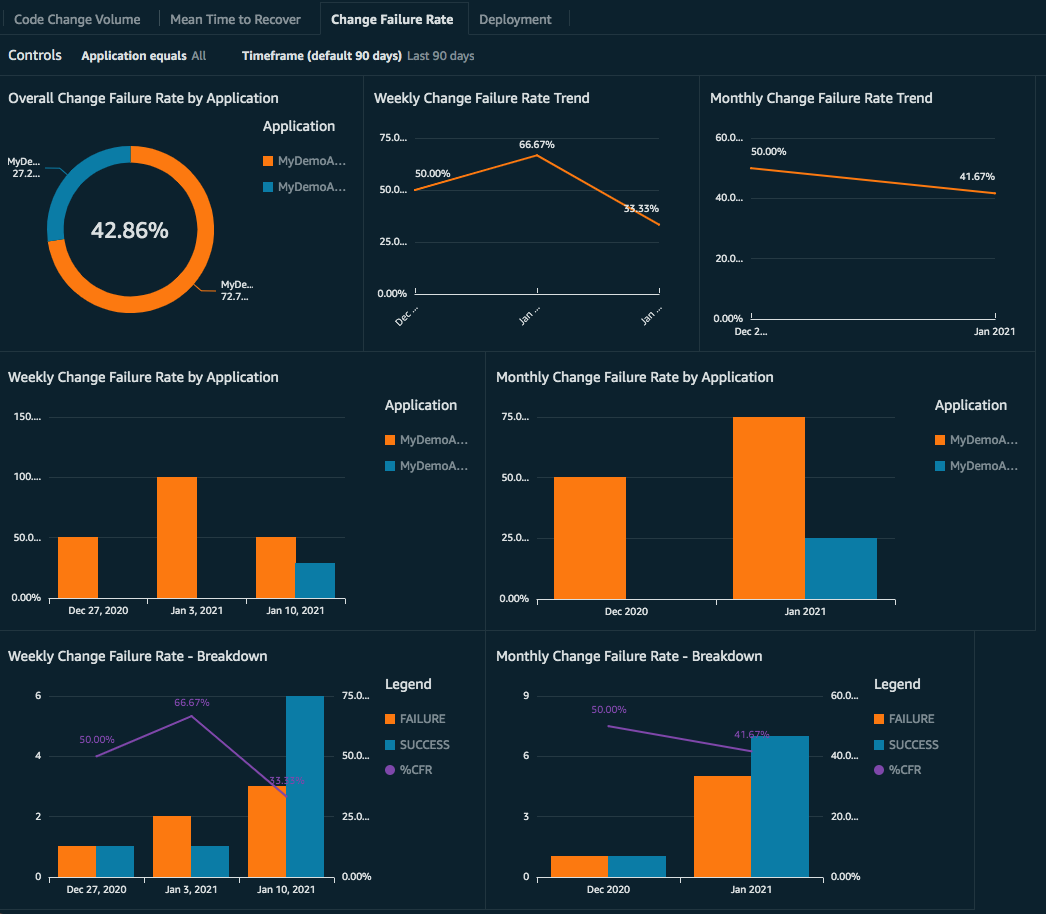
**MTTR dashboards**

These dashboards display outage minutes by application and the average time it takes to restore an application from a failure to success state. They provide a weekly, monthly, and aggregated view of the metrics by application. You can use the custom filter to filter data by application or time period. These dashboards help DevOps leaders correlate change activity to system stability, track and identify opportunities to improve the stability of applications.



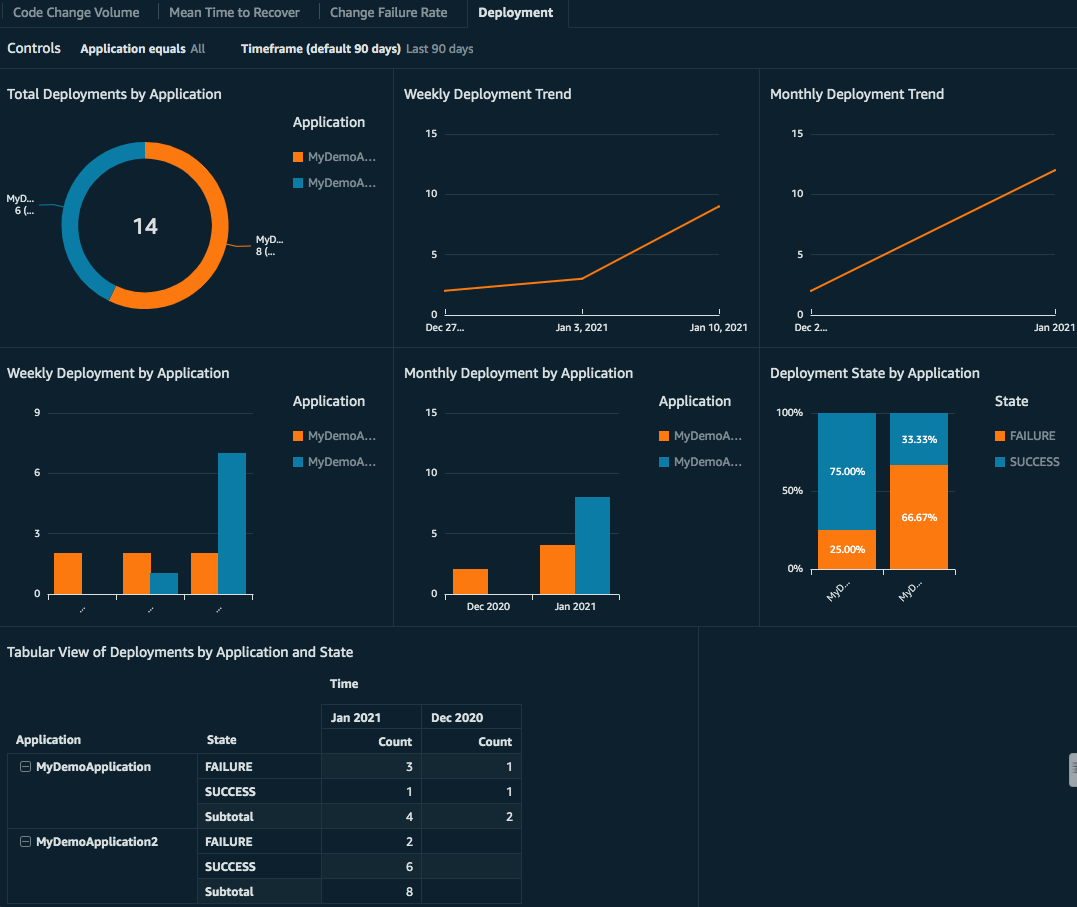
**Change failure rate dashboards**

These dashboards display the frequency of deployment failures per application by measuring the ratio of unsuccessful to total deployments. They provide a weekly, monthly, and aggregated view of the metrics by application. You can use the custom filter to filter metrics by application or time period. These dashboards help DevOps leaders track the code quality of their development teams and drive improvements to reduce the change failure rate over time.



**Deployment dashboards**

These dashboards display the deployment frequency and state (success/failure) by application. They provide a weekly, monthly, and aggregated view of the metrics by application. You can use the custom filter to filter metrics by application or time period. These dashboards enable DevOps leaders to track the frequency and quality of their continuous software release to end users.



**Cleanup**

To avoid charges in your account, after you test the solution, delete the stack and resources.

To use the console

In the AWS CloudFormation console, choose the solution’s root stack, and choose Delete.

To use the AWS CLI

Run the following command in your AWS CLI environment:

$ aws cloudformation delete-stack --stack-name <installation-stack-name