

Implementation Guide:

Dynatrace

November 2020



Table of Contents

Foreword	3
Solution overview and features	4
Architecture diagram.....	4
Pre-requisites	5
Deployment and configuration steps.....	5
Configuration: Generate Dynatrace API token.....	6
Configuration: Deploy Dynatrace Control Tower solution.....	9
What to expect	10
Solution estimated pricing.....	13
FAQs.....	13
Additional resources.....	13
Partner contact information.....	13

Foreword

Dynatrace for Control Tower is an operational intelligence solution that performs intelligent observability for application, services and compute resources at scale on the AWS cloud. By implementing this solution, you can enable Dynatrace's smart baselining capability dynamically and enable performance monitoring of your multi-account environments in real-time.

The purpose of this AWS Implementation Guide is to enable every AWS Marketplace customer to seamlessly activate, deploy and configure Dynatrace AWS monitoring in AWS Control Tower environments. Additionally, it allows them to take full advantage of the resources pre-configured by AWS Control Tower as part of the initialization.

Solution overview and features

Dynatrace AWS monitoring requires an AWS monitoring policy and a role configured for each AWS account within Dynatrace. Once the AWS account and role are configured within Dynatrace, Dynatrace makes calls to the Amazon API using this configuration to continuously ingest Amazon CloudWatch metrics into the Dynatrace platform.

The Dynatrace integrated solution for AWS Control Tower provides a simple way to automate Dynatrace monitoring for multi-account AWS environments by automating this configuration process when new AWS accounts are created. The result is a complete picture of customers' environment that combines workload insights with Amazon CloudWatch service metrics and AWS Control Tower governance and automation.

Dynatrace's automatic and intelligent observability platform includes:

- ✓ Application performance monitoring
- ✓ Infrastructure monitoring
- ✓ Artificial intelligence for IT operations (AIOps)
- ✓ Digital experience monitoring
- ✓ Digital business analytics

Architecture diagram

The Dynatrace solution for Control Tower automates the creation of AWS monitoring instance within Dynatrace for the new account.

The following resources make up the solution:

- **Control Tower Event Rule** - captures "**CreateManagedAccount**" AWS Control Tower lifecycle event
- **CloudFormation StackSet** - creates identity and access management (IAM) Dynatrace monitoring role in managed accounts
- **Lambda** - handles the Control Tower CreateManagedAccount event – creates StackSet instance and configure AWS monitoring settings in Dynatrace via the Dynatrace API
- **AWS Secrets Manager** - stores Dynatrace API URL and token
- **Dynatrace** – Customer software-as-a-service (SaaS) Dynatrace environment

Figure 1 below shows the relationship to these resources and the sequence of activity when AWS Control Tower triggers a "**CreateManagedAccount**" event.

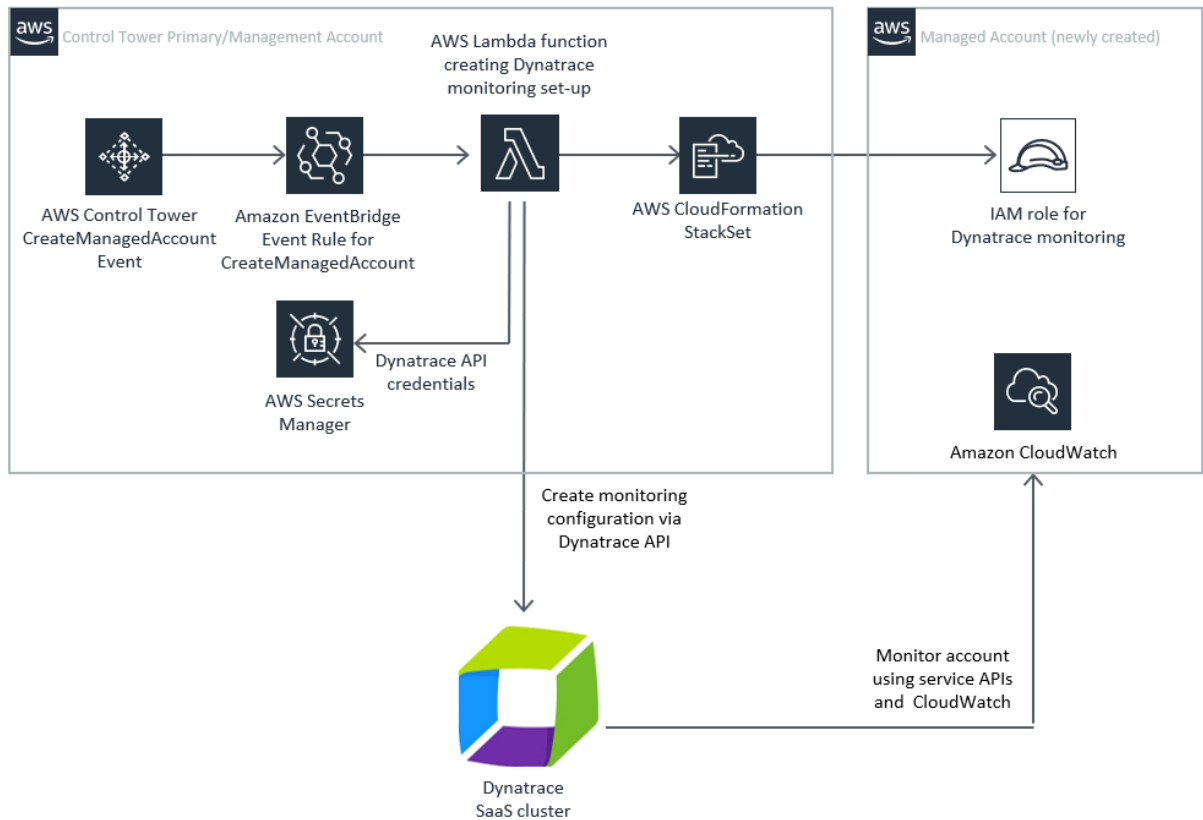


Figure 1 Dynatrace Architecture Diagram

Pre-requisites

To get started, you will need to provide a Dynatrace SaaS tenant. If you are new to Dynatrace and want to evaluate our platform for free, [sign up](#) for a 15 day trial

To get your own Dynatrace license now, go to the [AWS Marketplace](#) and request a Private Offer at sales@dynatrace.com or at +1 888 833-3652 for pricing and terms that fit your technical and business needs.

NOTE: The initial Control Tower solution works with Dynatrace SaaS only supporting metric collection for: Elastic Compute Cloud (EC2), Elastic Block Store (EBS), Elastic Load Balancer (ELB), Relational Database Service (RDS), DynamoDB, Lambda. Support for customer managed Dynatrace environments and extended AWS services is planned.

Deployment and Configuration Steps

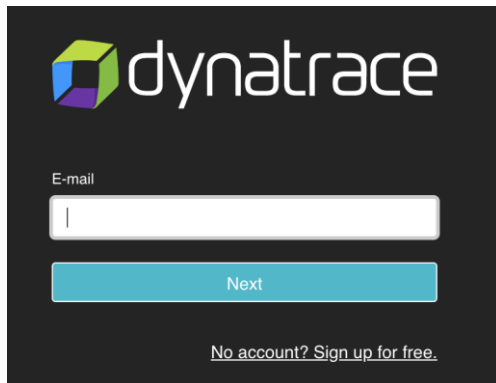
The deployment and configuration steps are done within both the Dynatrace and AWS web interfaces. The Dynatrace web interface is available as soon as your SaaS tenant is provisioned and is used to generate the API token used by the AWS Control Tower workflow and to view collected AWS metrics. The AWS web console is used to deploy the Dynatrace Control Tower solution and review the resulting Cloud Formation stackset creation status.

Configuration: Generate Dynatrace API Token

Step 1.1: Log into the Dynatrace web user interface (UI)

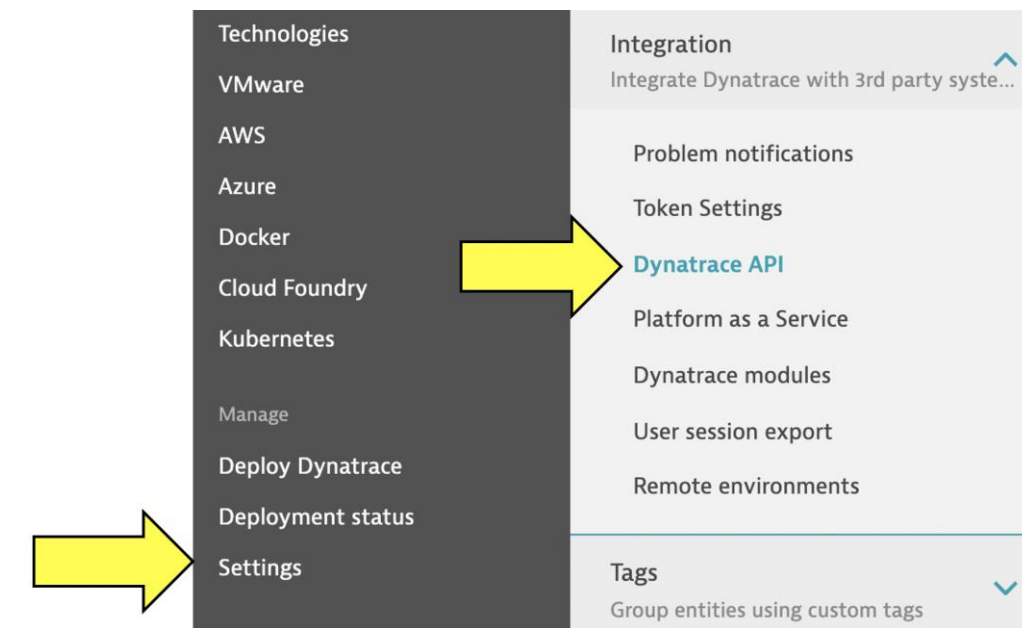
An automated email with the Dynatrace SaaS tenant URL will be sent to the email address of the person requesting its creation. Each environment that you monitor with Dynatrace is identified with a unique character string – the environment ID.

The Dynatrace SaaS URL will have a format of: <https://{your-environment-id}.live.dynatrace.com>. Once you access your URL, a login page such as this will be presented.



Step 1.2: Select **Settings** in the Dynatrace left side navigation menu.

Step 1.3: Go to **Integration** → **Dynatrace API**.



Step 1.4: Select **Generate token** button under “My Dynatrace API Tokens” section.

Dynatrace API

You can use our API to export Dynatrace monitoring data into your 3rd party reporting and analysis tools. Multiple API tokens can be created for different purposes.

Use the [Dynatrace API Explorer](#) or [read the API documentation](#) for use-cases and examples.

My Dynatrace API tokens

Generate a secure access API token that enables access to your Dynatrace monitoring data via our REST-based API.

 [Generate token](#)

Step 1.5: Enter a name for your token and select **API v1 “Read configuration” and “Write configuration” permissions.**

Generate a secure access API token that enables access to your Dynatrace monitoring data via our REST-based API.

Use the switches below to define the access scope of your Dynatrace API token.

API v1

Role/task oriented access scopes

- Access problem and event feed, metrics, and topology
- Read log content
- Create and read synthetic monitors, locations, and nodes
- Read synthetic monitors, locations, and nodes
- Read configuration
- Write configuration

API v2

Resource oriented access scopes

- Read metrics
- Ingest metrics
- Read entities
- Write entities
- Read network zones
- Write network zones

Step 1.6: Select **Generate** and save off your Token value for use in the next set of steps.

ControlTower token successfully generated

Configuration: Deploy Dynatrace Control Tower Solution

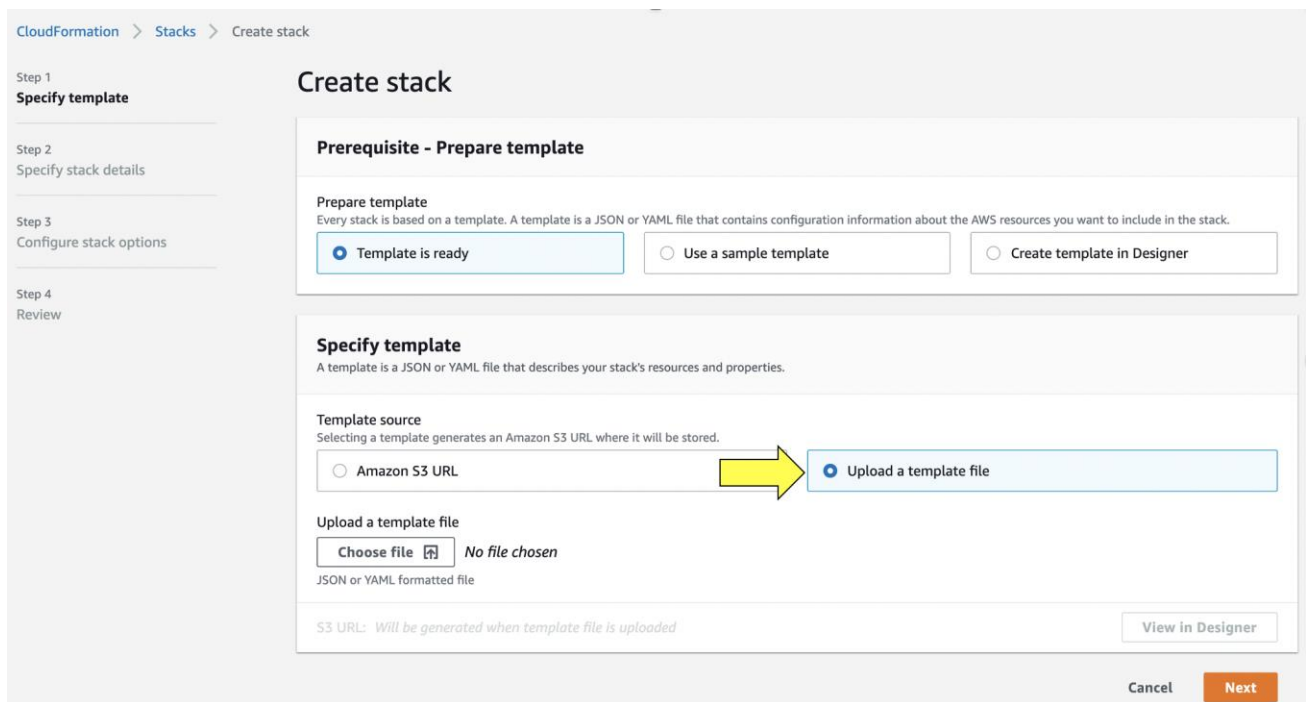
Step 2.1: Download the AWS CloudFormation template code from <https://github.com/Dynatrace/snippets/tree/master/technologies/aws/control-tower-templates>

Step 2.2: Login into AWS Control Tower primary account as user with AdministratorAccess

Step 2.3: Change to the region where AWS Control Tower is enabled

Step 2.4: From the AWS CloudFormation service, click the “Create Stack” button.

Step 2.5: On the “Specify Template” step, choose “Template is ready” and “Upload a template file” option



The screenshot shows the 'Create stack' wizard in the AWS CloudFormation console. The left sidebar indicates the current step is 'Step 1: Specify template'. The main content area is titled 'Create stack' and is divided into two sections: 'Prerequisite - Prepare template' and 'Specify template'.

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

Three radio button options are available:

- Template is ready
- Use a sample template
- Create template in Designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

Two radio button options are available:

- Amazon S3 URL
- Upload a template file

Upload a template file

A 'Choose file' button with a file icon is present, followed by the text 'No file chosen'. Below this, it says 'JSON or YAML formatted file'.

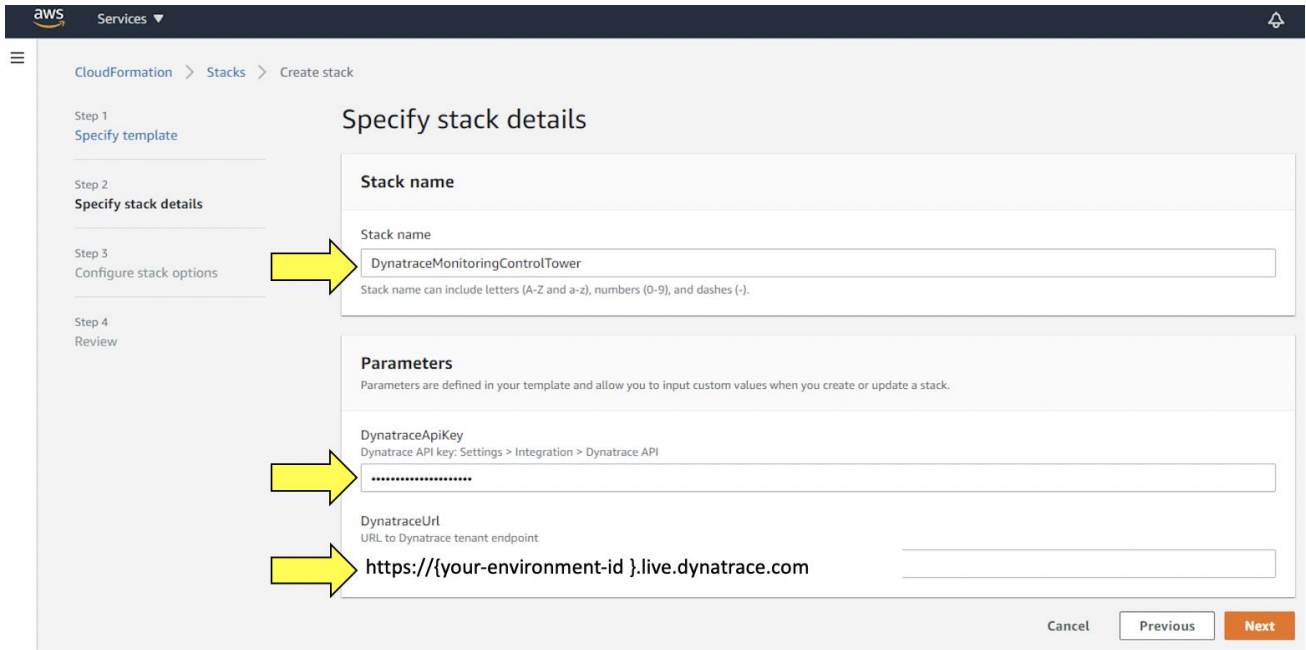
At the bottom of the 'Specify template' section, there is a text field for 'S3 URL: Will be generated when template file is uploaded' and a 'View in Designer' button.

At the bottom right of the entire wizard, there are 'Cancel' and 'Next' buttons.

Step 2.6: Upload the AWS CloudFormation template code downloaded in **step 2.1**. Click the “Next” button when complete.

Step 2.7: On the “Specify stack details” step, specify values for these parameters. Click the “Next” button when complete.

- Stack name – Any name that follows your organization’s naming convention.
- DynatraceUrl – Use the URL to Dynatrace tenant endpoint from **Step 1.1** above, for example [https://your-environment-id }.live.dynatrace.com](https://your-environment-id.live.dynatrace.com).
- DynatraceApiKey – Use the API token value that was created in **Step 1.6** above

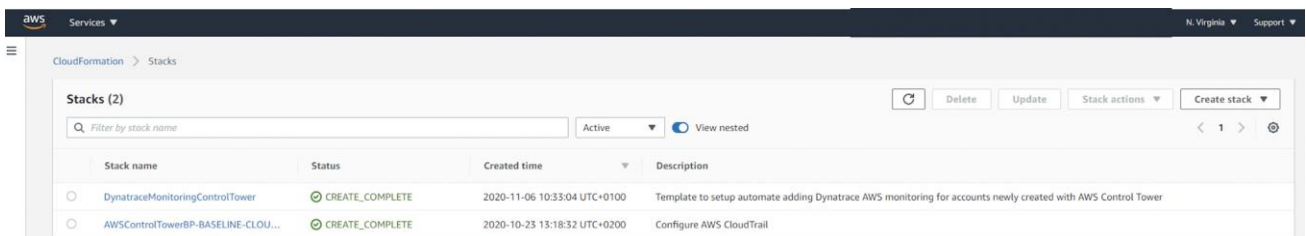


Step 2.8: On the “Configure stack options” step, leave defaults or optionally specify any option such as tags. Click the “next” button.

Step 2.9: On the “Review” step, review and click the “create stack” button when ready.

What to expect

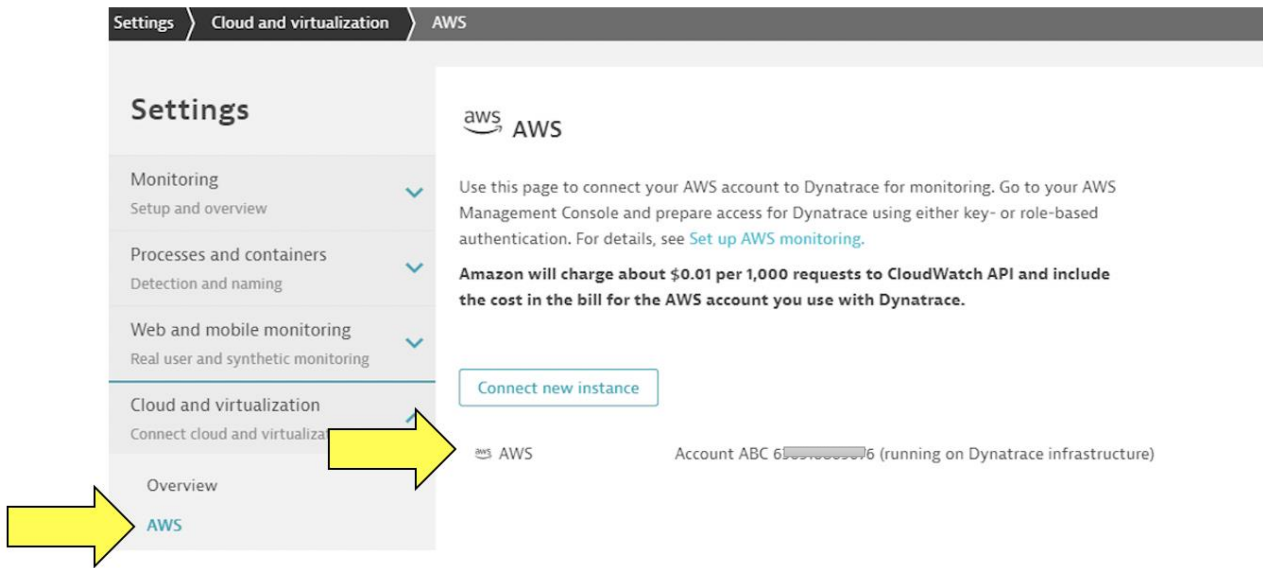
Step 3.1: On the CloudFormation Stack summary page, verify that stack was created successfully with a “CREATE_COMPLETE” status. In this example, the first row is for the Stack with a name of “DynatraceControl Tower”. The second row is for a stack that was also created by AWS Control Tower with Amazon CloudTrail logs.



Step 3.2: Log into the Dynatrace web UI

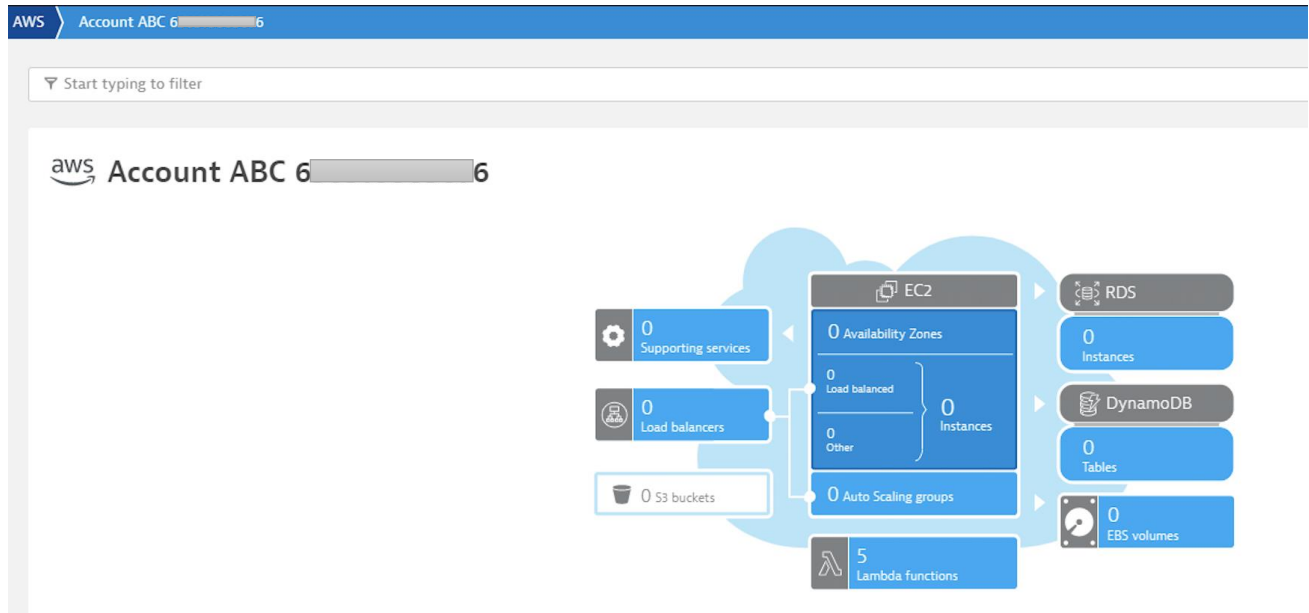
Step 3.3: Navigate to Settings → Cloud and virtualization → AWS in the Dynatrace left side navigation menu.

Step 3.4: Verify that a new AWS instance was added with a name that contains your Control Tower defined account name and AWS account number. Below is an example of a newly added AWS account instances.

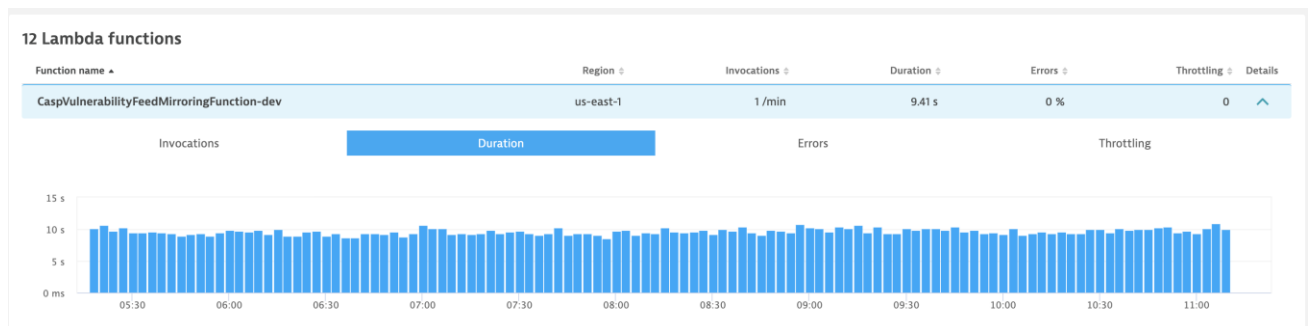


Step 3.5: To view collected metrics, navigate to the AWS menu option in the Dynatrace left side navigation menu. On this page, verify that the new monitored AWS account is listed.

Step 3.6: Click on the accounts to view the collected AWS service metrics. Below is an example for an individual AWS account at initial creation.



As data is collected, the info-graphic is updated with the counts for each service such as Amazon EC2 and AWS Lambda. By clicking on a given service, such as AWS Lambda, the metrics can be viewed as shown in this example below for a single AWS Lambda function.



NOTE: The initial AWS Control Tower solution works with Dynatrace SaaS only supporting metric collection for: Amazon Elastic Compute Cloud (EC2), Amazon Elastic Block Store (EBS), Amazon Elastic Load Balancer (ELB), Amazon Relational Database Service (RDS), Amazon DynamoDB, and AWS Lambda. Support for customer managed Dynatrace environments and extended AWS services is planned.

Solution Estimated Pricing

There is no cost from Dynatrace for this solution. There is a nominal AWS cost related to the AWS Lambda execution by AWS Control Tower for the AWS IAM setup and Dynatrace configuration API calls.

Visit us [here](#) for more pricing information for the collection of the metrics once the solution is in place.

Pricing details are available on [AWS Marketplace](#).

FAQs

Will the solution work if I am a Dynatrace customer running Dynatrace Managed on-premise or hosted on AWS?

No, the initial release of the Control Tower solution only supports Dynatrace SaaS infrastructure for monitoring. Support for Dynatrace managed clusters is planned.

Will the solution work if I am a Dynatrace customer using Dynatrace Environment ActiveGate(s)?

No, the initial release of the AWS Control Tower solution only supports Dynatrace SaaS infrastructure for monitoring. Support for customer managed Dynatrace Environment ActiveGates is planned.

Additional resources

- [Dynatrace Solution for AWS](#)
- [Set up Dynatrace SaaS for AWS monitoring documentation](#)
- [Dynatrace API Tokens](#)

Partner contact information

sales@dynatrace.com