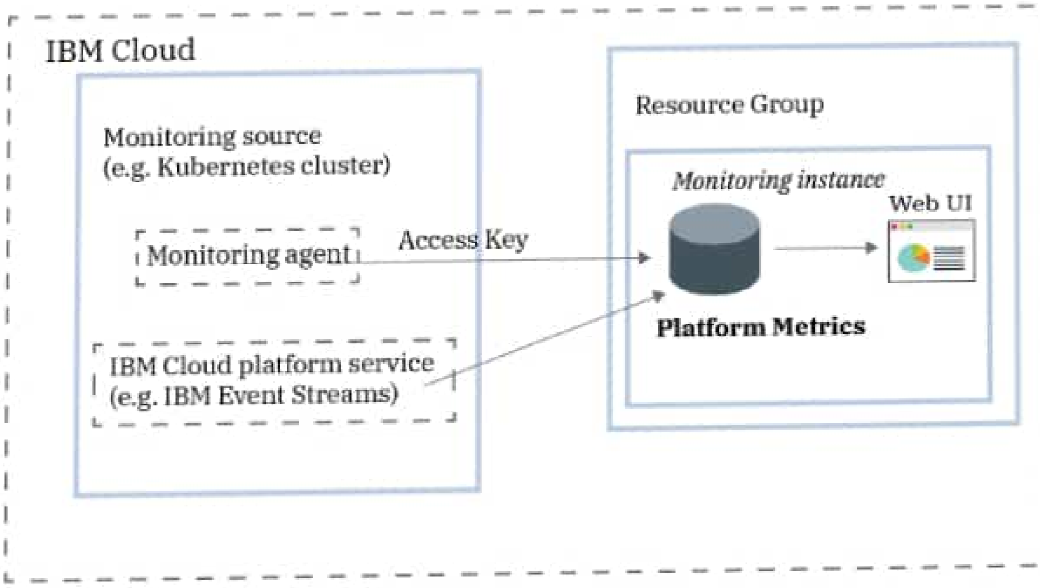
# Getting started tutorial

IBM Cloud® Monitoring is a cloud-native, and container-intelligence management system that you can include as part of your IBM Cloud architecture. Use it to gain operational visibility into the performance and health of your applications, services, and platforms. It offers administrators, DevOps teams and developers full stack telemetry with advanced features to monitor and troubleshoot, define alerts, and design custom dashboards. In architectures that are focused on container and microservices, you can use Secure to protect, monitor, and enhance forensic analysis of your pipeline and runtime components.

The following figure shows the components overview for the IBM Cloud Monitoring service that is running on IBM Cloud:



To add monitoring features with IBM Cloud Monitoring in the IBM Cloud, you must provision an instance of the IBM Cloud Monitoring service.

Before you provision an instance, consider the following information:

- The account owner can create, view, and delete an instance of a service in the IBM Cloud. This user can also grant permissions to other users to work with the IBM Cloud Monitoring service.
- Other IBM Cloud users with `administrator` or `editor` permissions can manage the IBM Cloud Monitoring service in the IBM Cloud. These users must also have platform permissions to create resources within the context of the resource group where they plan to provision the instance.

You provision an instance within the context of a resource group. You use a resource group to organize your services for access control and billing purposes. You can provision the IBM Cloud Monitoring instance in the *default* resource group or in a custom resource group.

After you provision an instance, you must configure metric sources, enable platform metrics, or both.

- A metric source is any resource that you want to monitor and control its performance and health.

- You can configure a monitoring agent to collect metrics from a source. For example, you can configure a monitoring agent for a Kubernetes cluster. You use the access key to configure the monitoring agent that is responsible for collecting and forwarding metric data to your instance.

  The monitoring agent can be configured to push metrics via the public or private endpoints by using the appropriate ingestion URL. Details can found in the endpoints section.

  After the IBM Cloud Monitoring agent is deployed in a metric source, collection and forwarding of metrics to the instance is automatic. The IBM Cloud Monitoring agent automatically collects and reports on pre-defined metrics. You can configure which metrics to monitor in an environment.

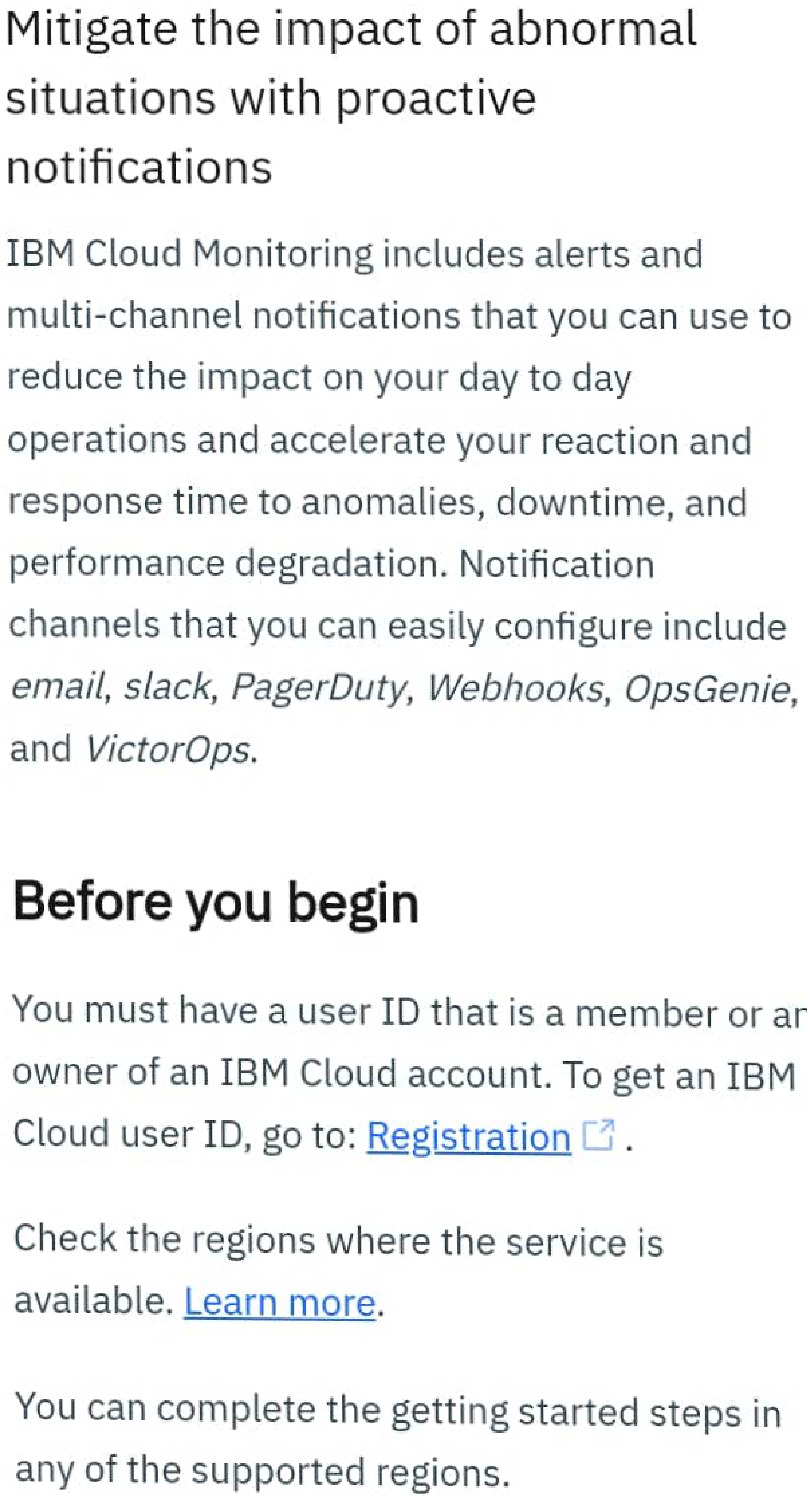
## Features

### Accelerate the diagnosis and resolution of performance incidents

IBM Cloud Monitoring offers deep visibility into your infrastructure and applications with the ability to troubleshoot from service level all the way down to the system level. Pre-defined dashboards and alerts simplify identification of potential threats or problems. By using IBM Cloud Monitoring, developers and DevOps teams monitor and troubleshoot performance issues in real-time, identify the source of errors, and eliminate problems.

### Control the cost of your monitoring infrastructure

IBM Cloud Monitoring includes functionality that help you control the cost of your monitoring infrastructure in the IBM Cloud. You can configure the metric sources for which you want to monitor their performance. You can enable a pre-defined alert to warn you of usage changes that will impact your billing.



### Mitigate the impact of abnormal situations with proactive notifications

IBM Cloud Monitoring includes alerts and multi-channel notifications that you can use to reduce the impact on your day to day operations and accelerate your reaction and response time to anomalies, downtime, and performance degradation. Notification channels that you can easily configure include *email*, *slack*, *PagerDuty*, *Webhooks*, *OpsGenie*, and *VictorOps*.

## Before you begin

You must have a user ID that is a member or ar owner of an IBM Cloud account. To get an IBM Cloud user ID, go to: Registration .

Check the regions where the service is available. Learn more.

You can complete the getting started steps in any of the supported regions.

- The account owner can create, view, and delete an instance of a service in the IBM Cloud, and can grant permissions to othe users to work with the IBM Cloud Monitoring service.
- You must have permissions to create resources in the *Default* resource group.
- Other IBM Cloud users with `administrator` or `editor` permissions can manage the IBM Cloud Monitoring service in the IBM Cloud. These users must also have platform permissions to create resources within the context of the resource group where they plan to provision the instance.

To grant a user administrator role for the service and to manage instances within a resource group in the account, the user must have an IAM policy for the IBM Cloud Monitoring service with the platform role **Administrator** within the context of the resource group.

Complete the following steps to assign a user administrator role to the IBM Cloud Monitoring service within the context of a resource group:

1. From the menu bar, click **Manage** > **Access (IAM)**, and then select **Users**.
2. From the row for the user that you want to assign access, select the **Actions** menu, and then click **Assign access**.
3. Select **Assign access within a resource group**.
4. Select a resource group.
5. If the user does not have a role already granted for the selected resource group, choose a role for the **Assign access to a resource group** field.

   Depending on the role that you select, the user can view the resource group on their dashboard, edit the resource group name, or manage user access to the group.

   You can select **No access**, if you want the user to only have access to the IBM Cloud Monitoring service in the resource group.

6. Select **IBM Cloud Monitoring**.
7. Select the platform role **Administrator**.
8. Click **Assign**.

## Step 2. Provision an instance of the IBM Cloud Monitoring service

To add monitoring features with IBM Cloud Monitoring in the IBM Cloud, you must provision an instance of the IBM Cloud Monitoring service.

You provision an instance within the context of a resource group. A resource group lets you organize your services for access control and billing purposes. You can provision the IBM Cloud Monitoring instance in the *default* resource group or in a custom resource group.

To provision an instance through the IBM Cloud UI, complete the following steps:

1. Log in to your IBM Cloud account.

   Click IBM Cloud dashboard ↗ to launch the IBM Cloud dashboard.

   After you log in with your user ID and password, the IBM Cloud UI opens.

2. Click **Catalog**. The list of the services that are available in IBM Cloud opens.

3. To filter the list of services that is displayed, select the **Logging and**

4. Click the **IBM Cloud Monitoring** tile.
5. Select the location.
6. Select a service plan.

   To provision an instance that only includes the *Monitor* component, select the plan **Graduated Tier**.

   To provision an instance that include the *Monitor* and the *Secure* components, select the plan **Graduated Tier - Sysdig Secure + Monitor**.

   For more information about the service plans, see Service plans.

7. Enter a service name.
8. Select a resource group. By default, the **Default** resource group is set.
9. Set on automatic collection of platform metrics by clicking **Enable**.
10. Click **Create** to provision an instance.

The service UI opens.

## Step 3. Configure platform metrics

Platform metrics are metrics that are exposed by enabled-monitoring services and the platform in IBM Cloud. You must configure a monitoring in a region to monitor these metrics. Learn more.

To see the list of enabled-monitoring services, see Cloud services.

For example, to configure platform metrics in a region, complete the following steps:

1. From theIBM Cloud dashboard, go to the menu icon ☰ > **Observability** to access the *Observability* dashboard.
2. Select **Monitoring** > **Configure platform metrics**.
3. Select a region.
4. Choose the monitoring that will collect metrics from enabled services on that location.
5. Click **Save**.

The main *Observability* page opens.

The instance that you choose to receive metrics shows the flag **Platform metrics**.

# Step 4. Configure a monitoring agent

After you provision an instance, you must configure a monitoring agent for each host that you want to monitor. For example, a host can be a cloud resource that you want to monitor and control its performance and health such as a Kubernetes cluster. You may also monitor hosts outside the IBM Cloud.

The monitoring agent automatically collects and reports on pre-defined metrics. You use the *access key* to configure the monitoring agent that is responsible for collecting and forwarding metric data to your instance. For more information, see Working with access keys.

# Step 5. Launch the web UI

After you provision an instance of the IBM Cloud Monitoring service in the IBM Cloud, and configure a monitoring agent for your node, you can view, monitor, and manage data through the service's web UI.

You launch the web UI within the context of the monitoring, from the IBM Cloud UI.

Complete the following steps to launch the monitoring UI:

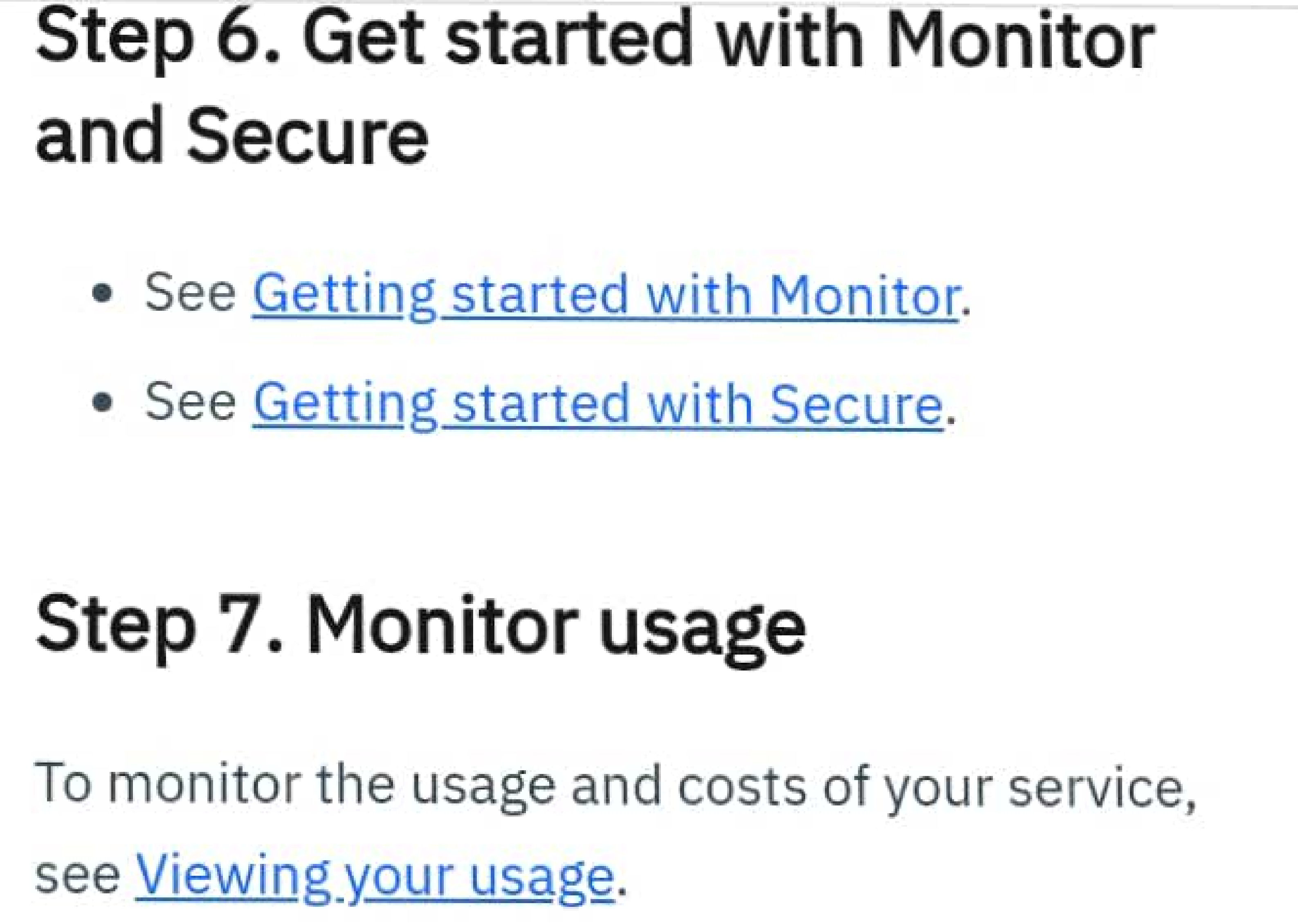
1. Log in to your IBM Cloud account.

   Click IBM Cloud dashboard to launch the IBM Cloud dashboard.

   After you log in with your user ID and password, the IBM Cloud Dashboard opens.

2. In the navigation menu, select **Observability**.
3. Select **Monitoring**.

   The list of monitoring instances that are available on IBM Cloud is displayed.



## Step 6. Get started with Monitor and Secure

- See Getting started with Monitor.
- See Getting started with Secure.

## Step 7. Monitor usage

To monitor the usage and costs of your service, see Viewing your usage.