

**Lab Manual- Use Azure Monitor managed service for Prometheus as data source for Grafana using managed system identity**

**Prepared for**:

**Date:** 18th Dec 2023

**Prepared by:**

Document Name: Lab Manual **Document Number** AZLabn916

**Contributor:**

Contents

[1. Objective 3](#_Toc157340001)

[1. Azure Monitor managed service for Prometheus? 3](#_Toc157340002)

[2. Azure Managed Grafana 3](#_Toc157340003)

[2. Create 1 Node Azure Kubernetes Cluster 4](#_Toc157340004)

[3. Create a Custom Storage Class 6](#_Toc157340005)

[4. Configure system identity in graphana 11](#_Toc157340006)

[5. Configure from Azure Monitor workspace 12](#_Toc157340007)

[6. Create Prometheus data source 16](#_Toc157340008)

[7. Use Graphana 20](#_Toc157340009)

[8. Prometheus Explorer workbook 22](#_Toc157340010)

[9. PromQL 25](#_Toc157340011)

[1. Selecting a time series with PromQL 25](#_Toc157340012)

[2. Filtering by label 26](#_Toc157340013)

[3. Comparing current data with historical data 27](#_Toc157340014)

# Objective

## Azure Monitor managed service for Prometheus?

[Azure Monitor managed service for Prometheus](https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/prometheus-metrics-overview) is a fully managed, highly scalable, and reliable monitoring service available in Azure. It offers a turnkey solution for collecting, querying, and alerting on metrics from AKS clusters. With Azure Managed Prometheus, you no longer need to deploy and manage Prometheus and Grafana within your clusters using a Helm chart. Instead, you can focus on extracting meaningful insights from the collected metrics. You can use a single Azure Monitor workspace to collect Prometheus metrics from a group of AKS clusters and use a single Azure Managed Grafana as a single pan of glass to visualize and aggregate Prometheus metrics collected in the Azure Monitor workspace from one or multiple AKS clusters.

The following figure shows the Azure Monitor managed service for Prometheus overview diagram:

thumbnail image 2 of blog post titled 
 
 
  
 
 
 
    
  
   
    
      
       How to create an AKS cluster with Azure Managed Prometheus and Azure Managed Grafana via Bicep
       
      
     
   
  
 
   
 
 
 
 
 


## Azure Managed Grafana

[Azure Managed Grafana](https://learn.microsoft.com/en-us/azure/managed-grafana/overview) is a managed service that provides a comprehensive data visualization platform built on top of the Grafana software by Grafana Labs. It's made as a fully managed Azure service operated and supported by Microsoft. Grafana helps you combine metrics, logs and traces into a single user interface. With its extensive support for data sources and graphing capabilities, you can view and analyze your application and infrastructure telemetry data in real time.

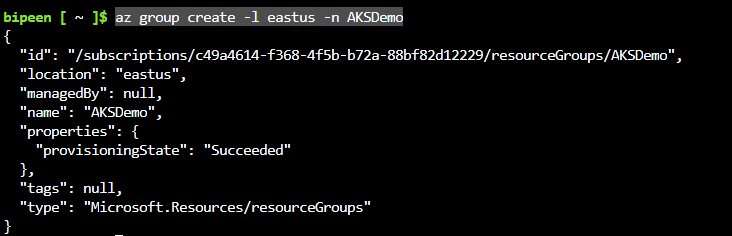
Azure Managed Grafana is optimized for the Azure environment. It works seamlessly with many Azure services and provides the following integration features:

* Built-in support for [Azure Managed Prometheus](https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/prometheus-grafana) and [Azure Data Explorer](https://learn.microsoft.com/en-us/azure/data-explorer/).
* User authentication and access control using Azure Active Directory identities.
* Direct import of existing charts from the Azure portal.

In particular, by integrating with [Azure Monitor managed service for Prometheus](https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/prometheus-metrics-overview), [Azure Managed Grafana](https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/prometheus-grafana) allows you to create rich and customizable dashboards to visualize the Prometheus metrics collected in an Azure Monitor workspace from one or more AKS clusters. Azure Managed Grafana enables you to gain deep visibility into your AKS clusters, troubleshoot issues, and make informed decisions based on real-time data. You can also set up [Azure Monitor alerts](https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-overview) and use them with [Azure Managed Grafana](https://learn.microsoft.com/en-us/azure/managed-grafana/how-to-use-azure-monitor-alerts).

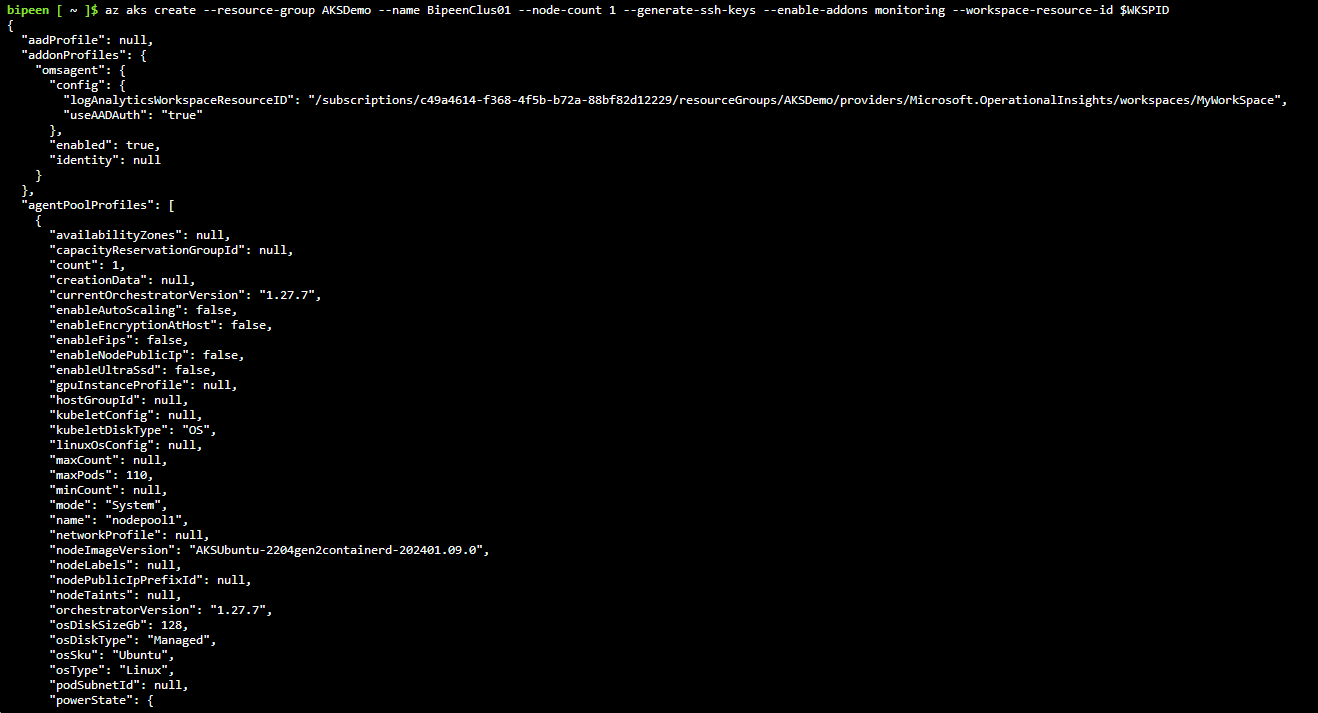
# Create 1 Node Azure Kubernetes Cluster

az group create -l eastus -n AKSDemo



To create an AKS cluster, use the [az aks create](https://learn.microsoft.com/en-us/cli/azure/aks" \l "az-aks-create) command. The following example creates a cluster named BipeenClus01 with one node and generate SSH-key. It will automatically use 3 Nodes when you don’t specify node count

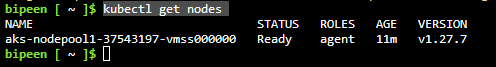
az aks create --resource-group AKSDemo --name BipeenClus01 --node-count 1 --generate-ssh-keys



az aks get-credentials --resource-group AKSDemo --name BipeenClus01 --overwrite-existing



kubectl get nodes



We will first create the deployment using the following command.

kubectl create deployment nginx-project --image=nginx

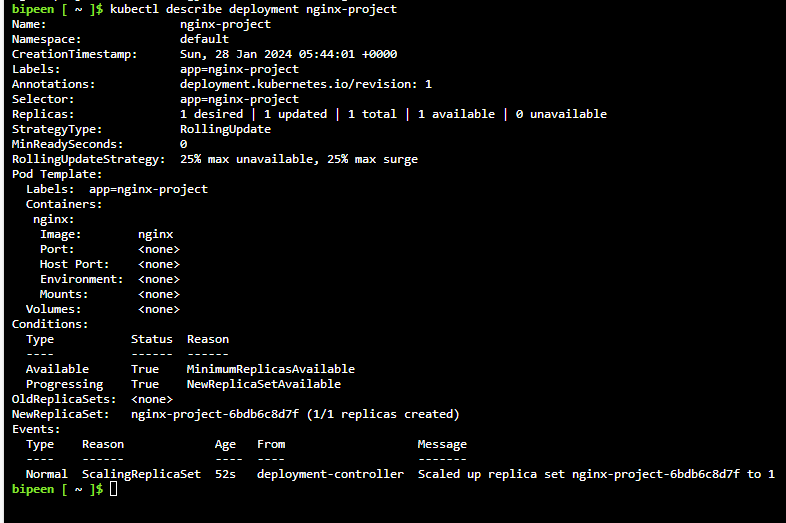


kubectl get po



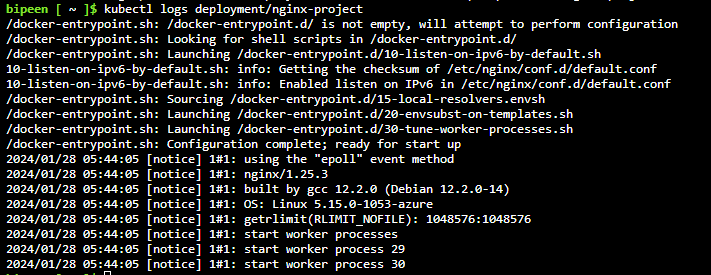
Use the following command to get the details of the deployment.

kubectl describe deployment nginx-project

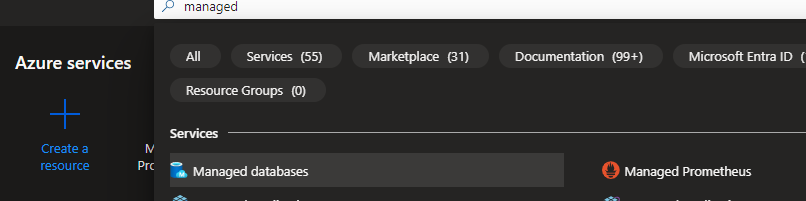


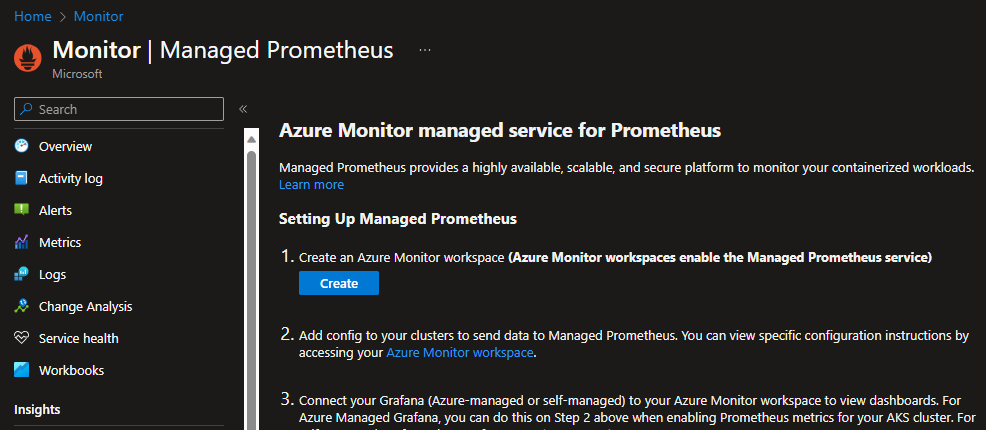
To get the logs, we can run the following command.

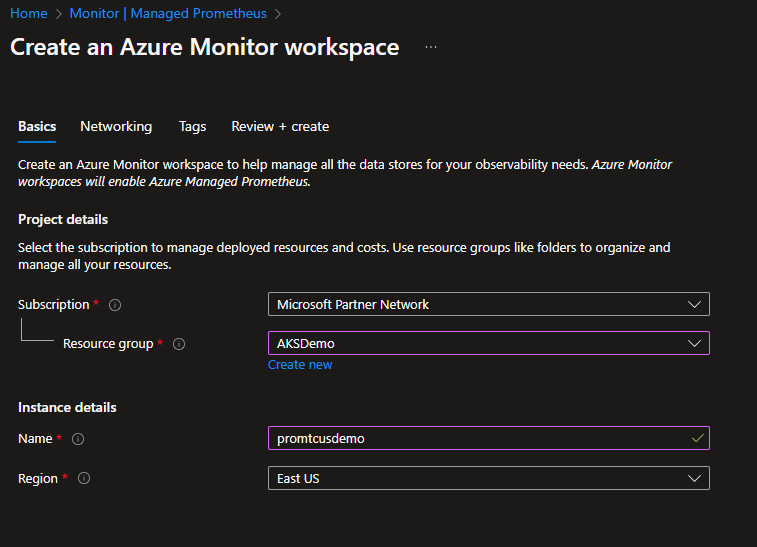
kubectl logs deployment/nginx-project



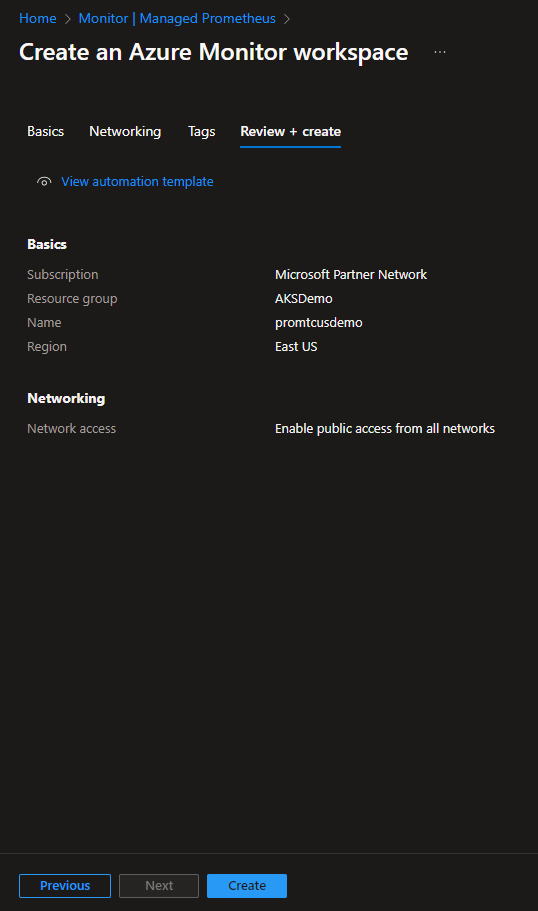
# Create a Custom Storage Class



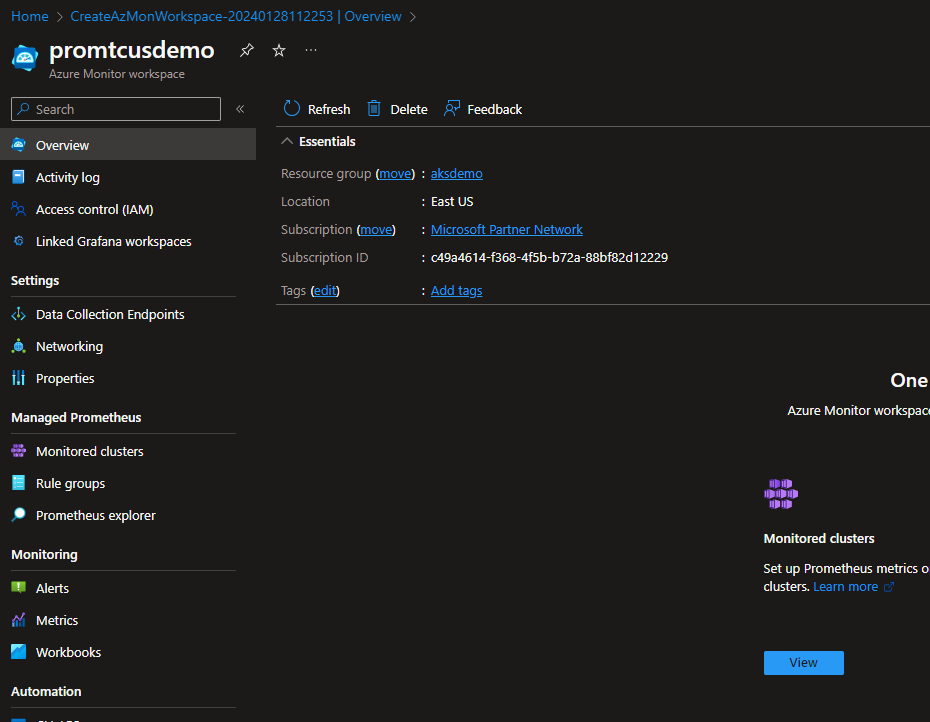


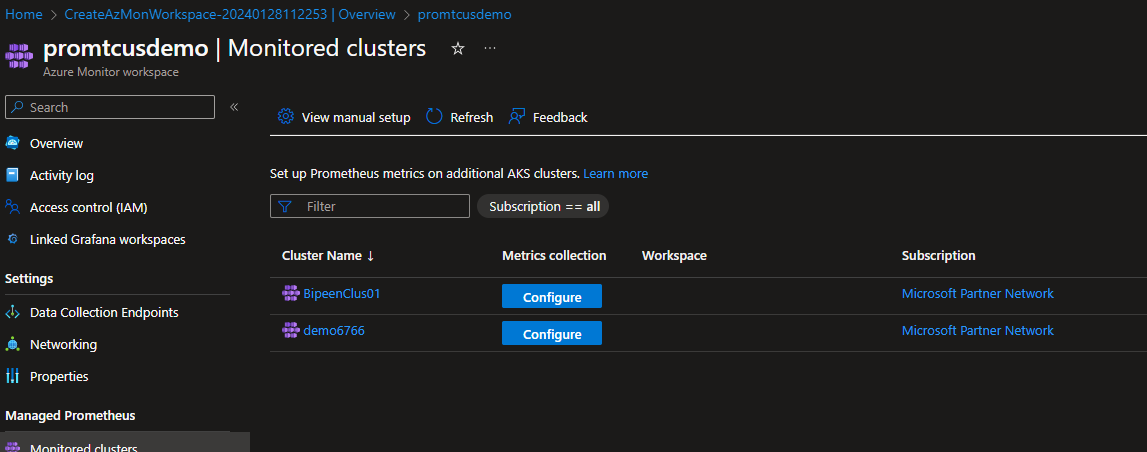


Review and Create

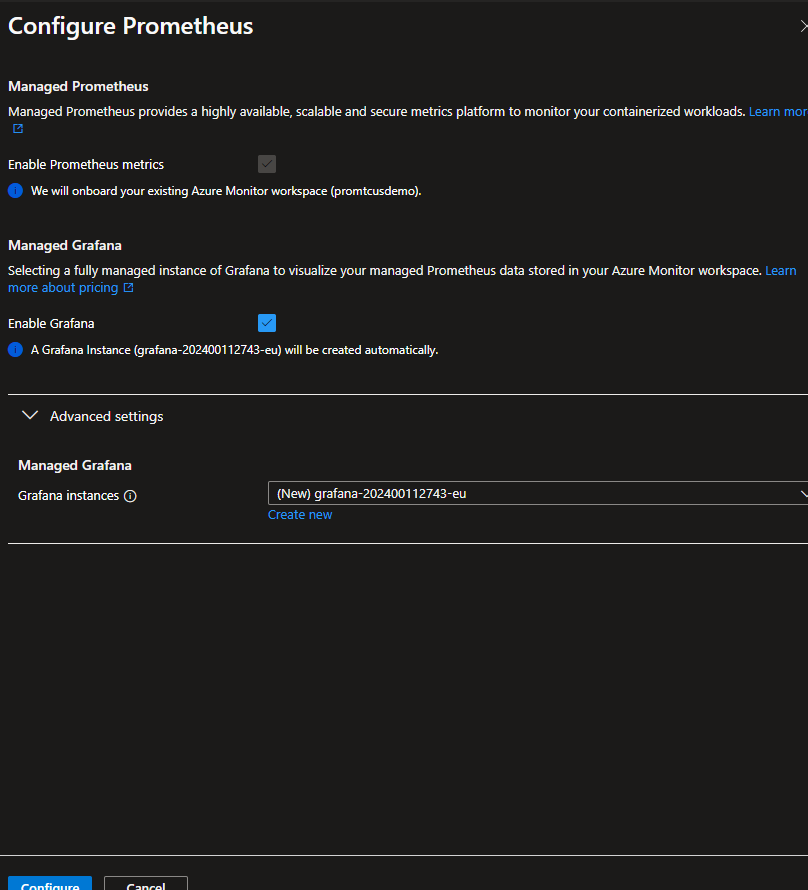


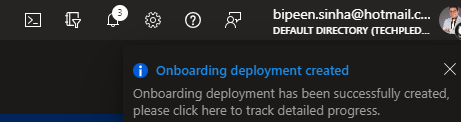
Once Created go inside and click managed clusters

****

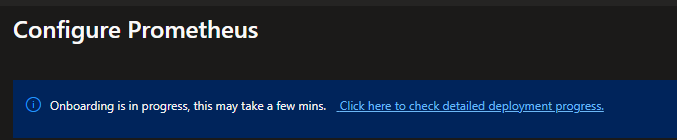
****

**Clicl configure and enable graphana**

****

****

**It take 10-15 min**

****

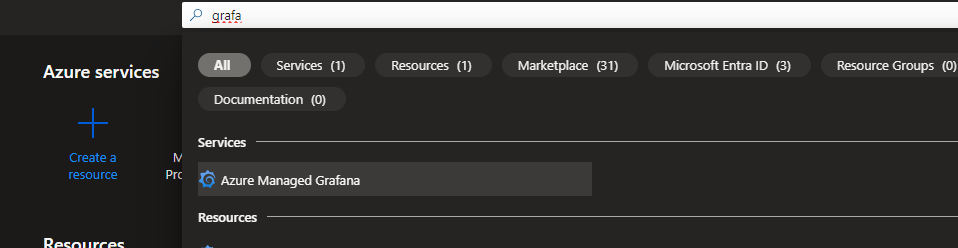
# Configure system identity in graphana

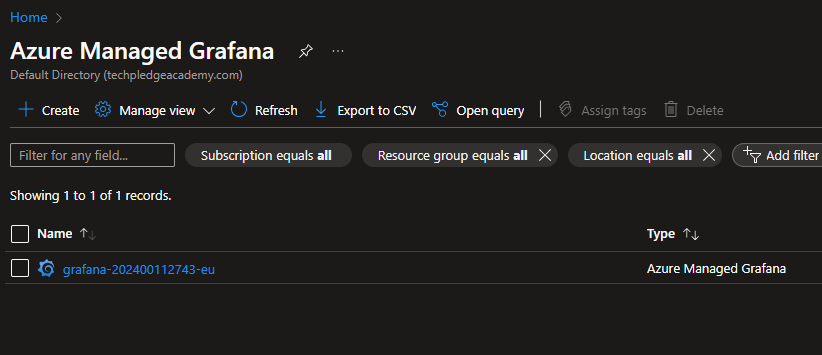
Your Grafana workspace requires the following settings:

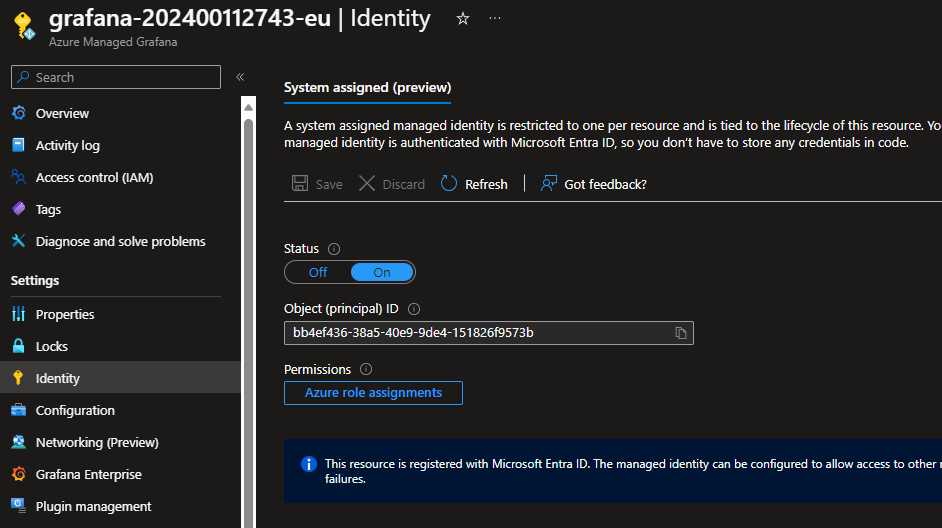
* System managed identity enabled
* **Monitoring Data Reader** role for the Azure Monitor workspace

Both of these settings are configured by default when you created your Grafana workspace and linked it to an Azure Monitor workspace. Verify these settings on the **Identity** page for your Grafana workspace.

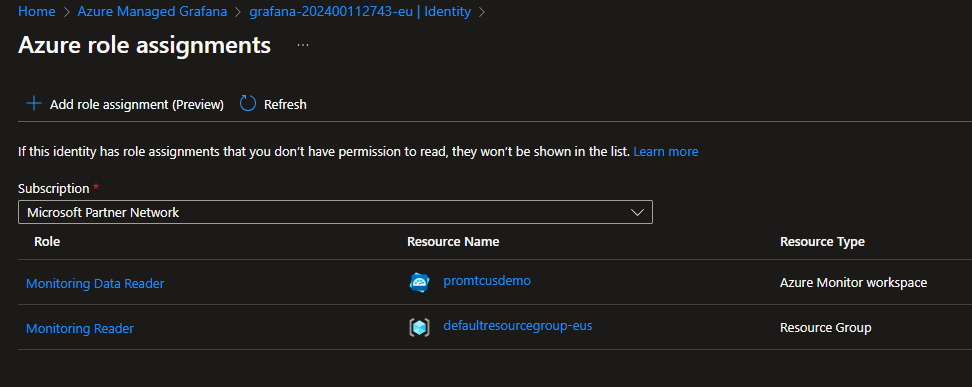
**once created search and open Managed Graphana**

****

****

****

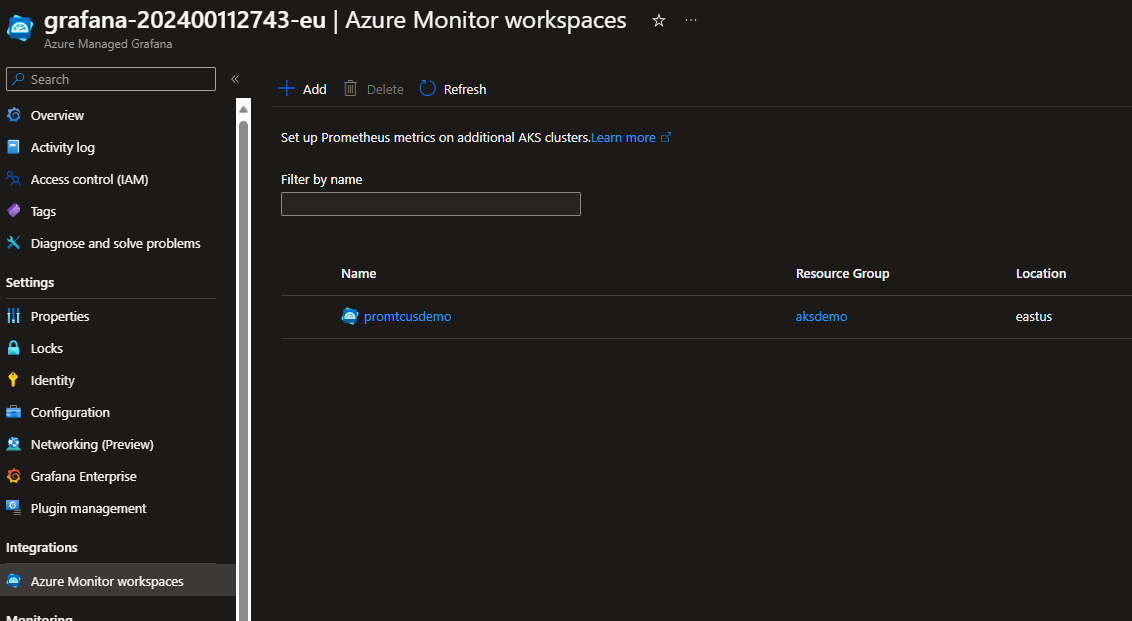
**Azure role assignments** to review the existing access in your subscription.

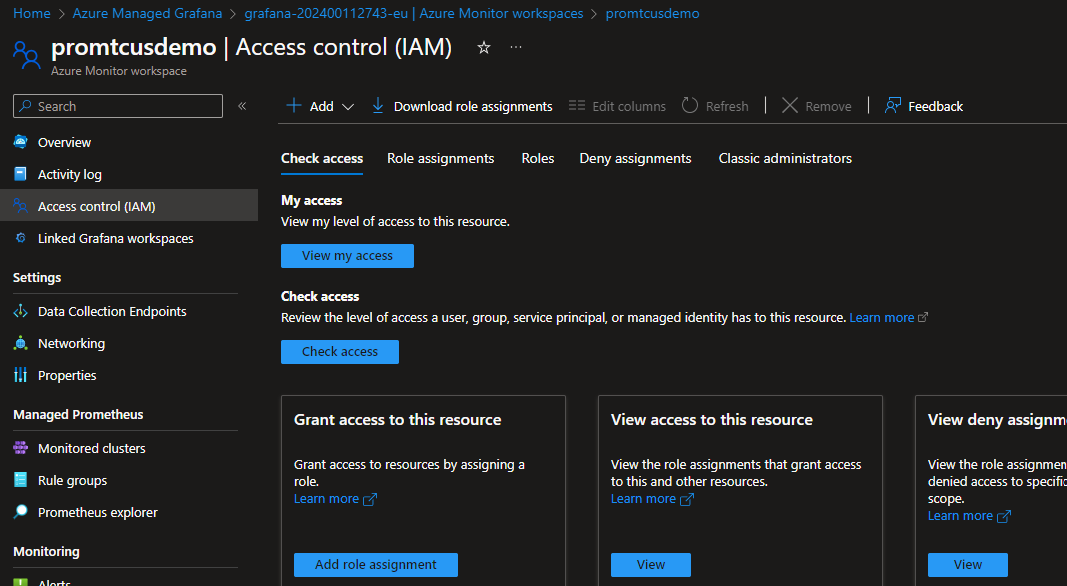
****

# Configure from Azure Monitor workspace

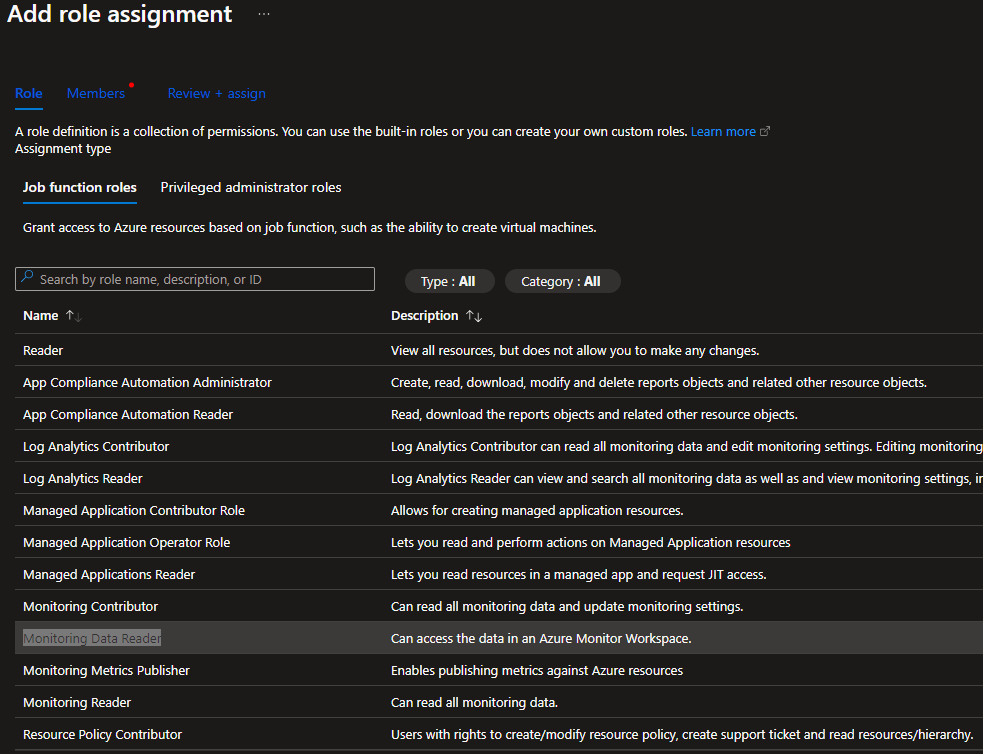
Use the following steps to allow access to only a specific Azure Monitor workspace:

1. Open the **Access Control (IAM)** page for your Azure Monitor workspace in the Azure portal.
2. Select **Add role assignment**.

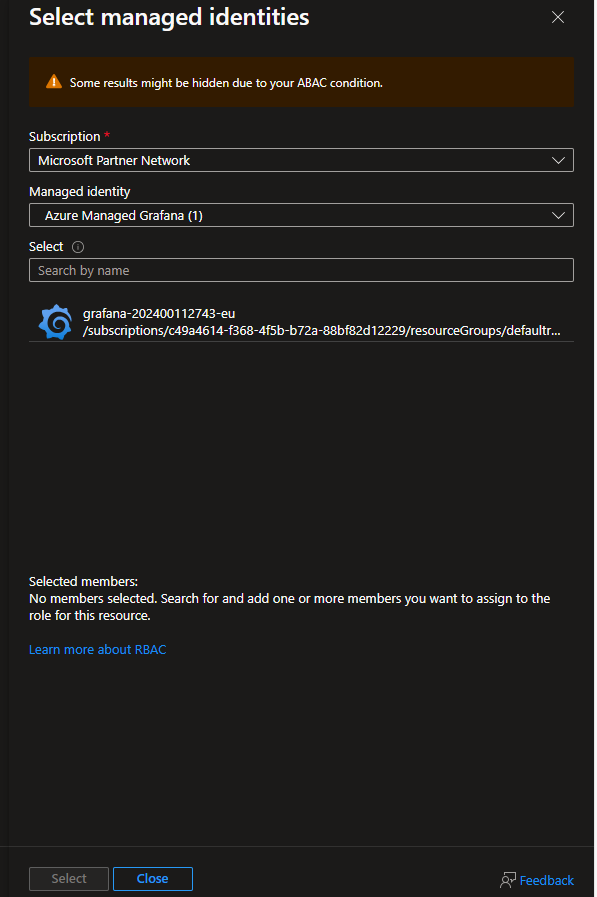
****

****

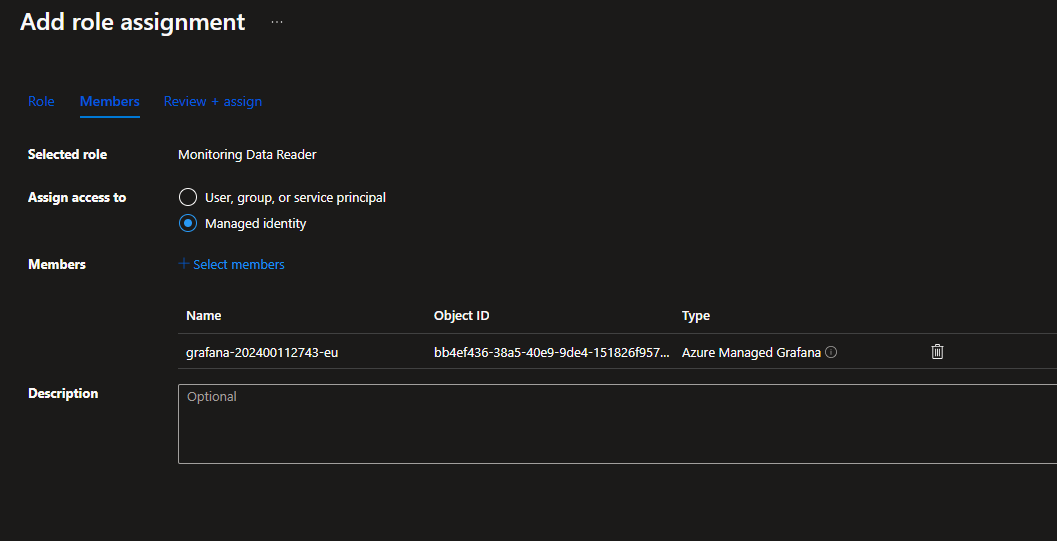
Select **Monitoring Data Reader** and select **Next**.

****

1. For **Assign access to**, select **Managed identity**.
2. Select **+ Select members**.
3. For **Managed identity**, select **Azure Managed Grafana**.
4. Select your Grafana workspace and then select **Select**.

****

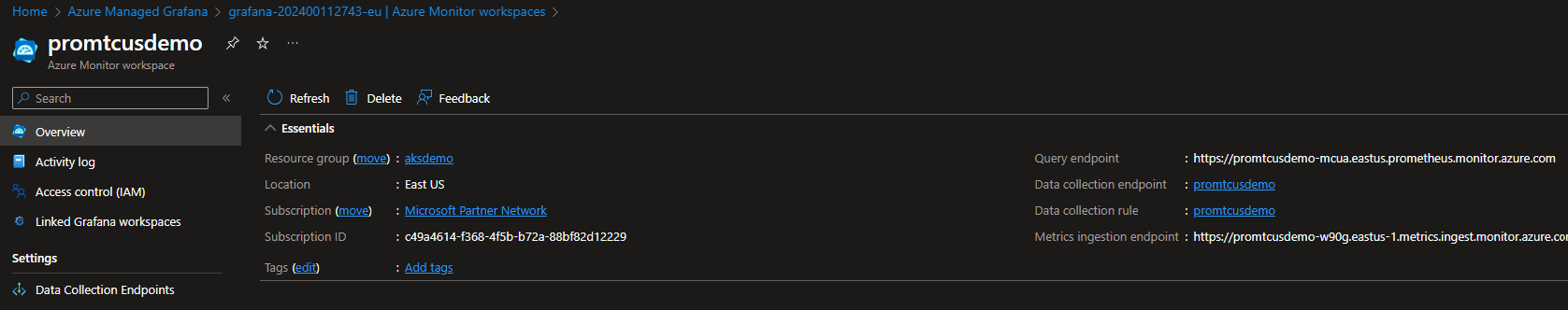
1. Select **Review + assign** to save the configuration.

****

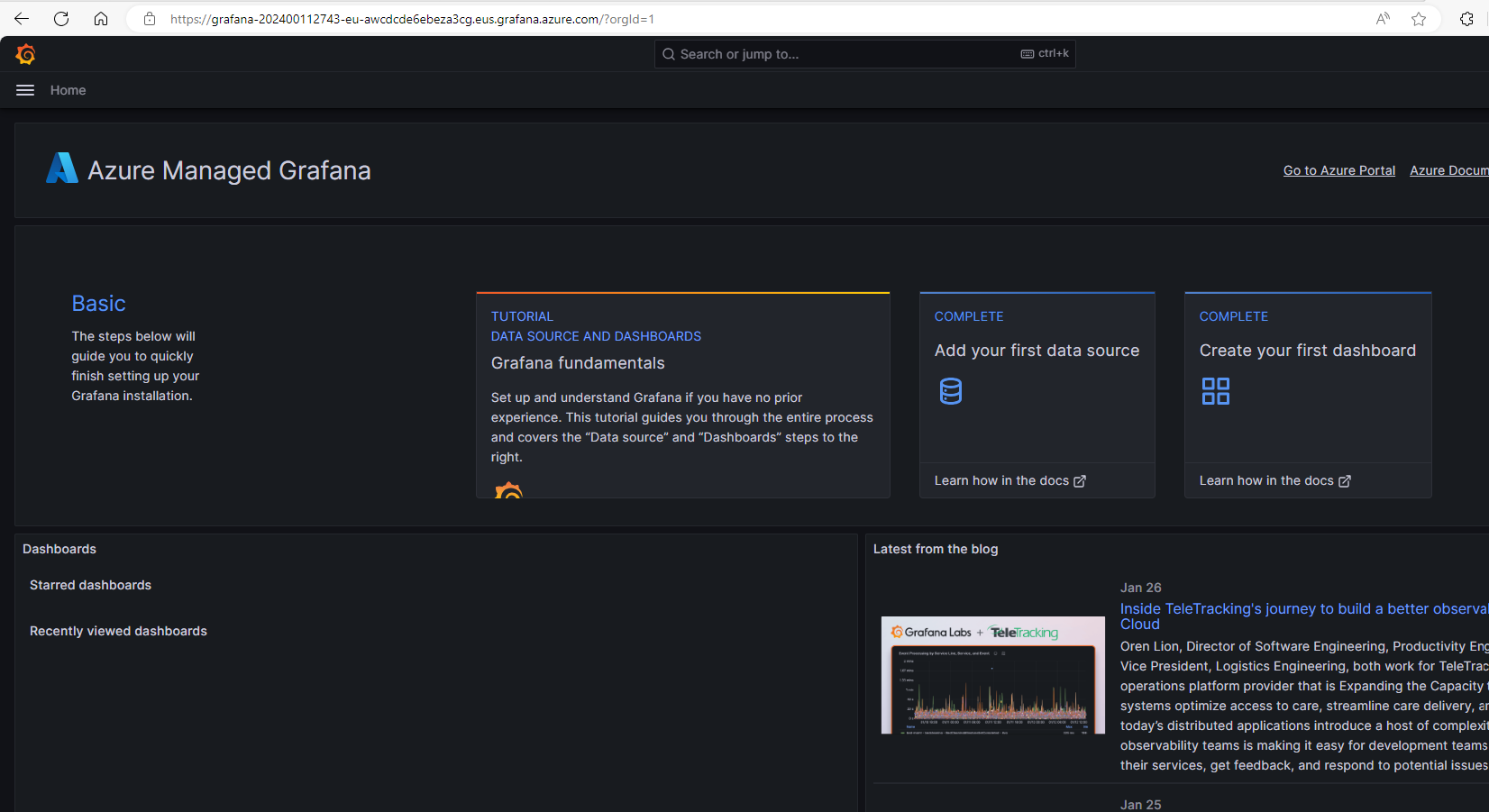
# Create Prometheus data source

1. Open the **Overview** page for your Azure Monitor workspace in the Azure portal.
2. Copy the **Query endpoint**, which you'll need in a step below.

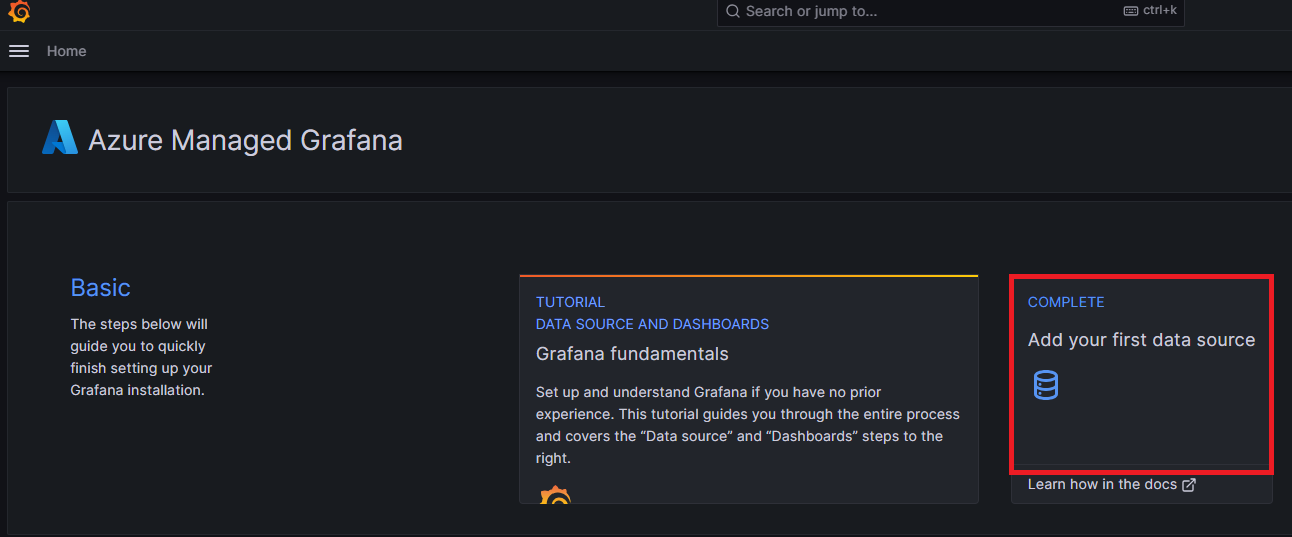
<https://promtcusdemo-mcua.eastus.prometheus.monitor.azure.com>



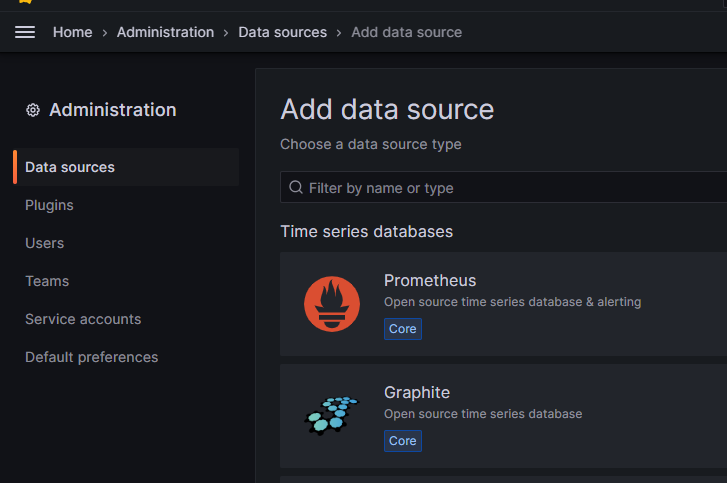
1. Open your Azure Managed Grafana workspace in the Azure portal.
2. Select on the **Endpoint** to view the Grafana workspace



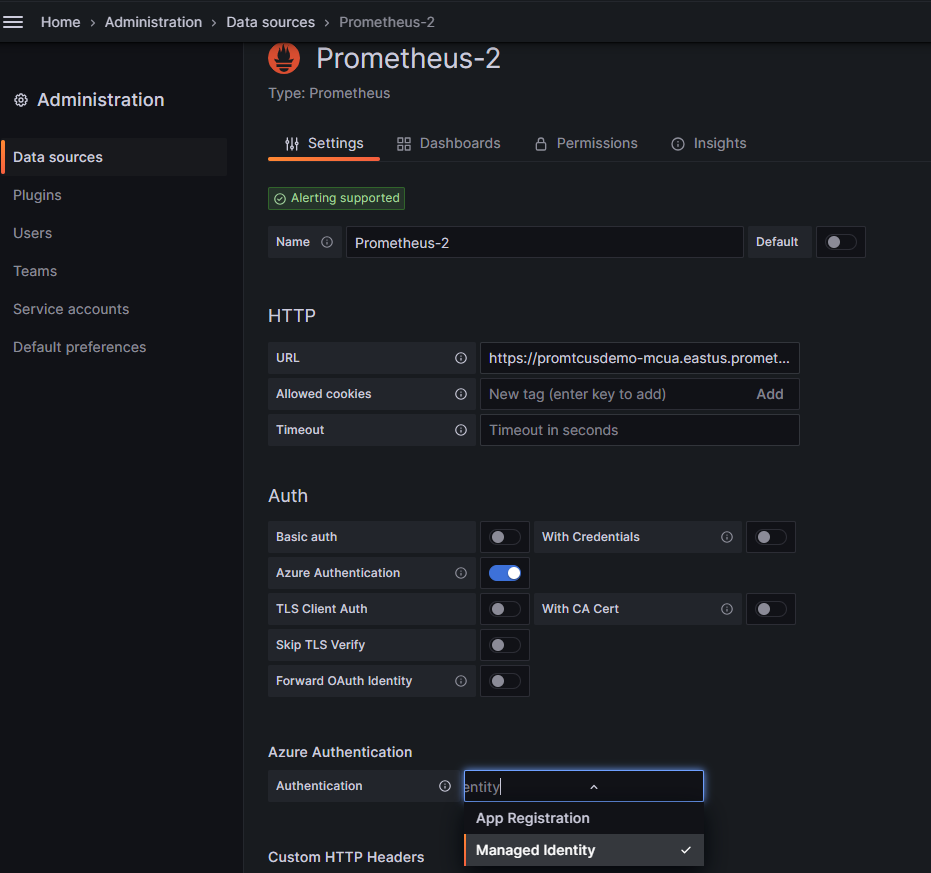
1. Select **Configuration** and then **Data source**.



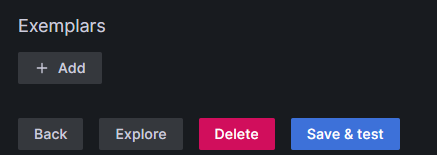
1. Select **Add data source** and then **Prometheus**.

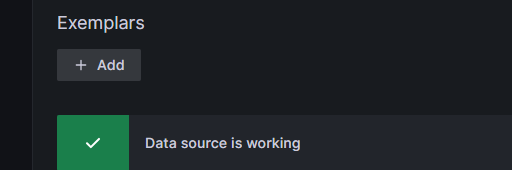


1. For **URL**, paste in the query endpoint for your Azure Monitor workspace.
2. Select **Azure Authentication** to turn it on.
3. For **Authentication** under **Azure Authentication**, select **Managed Identity**.

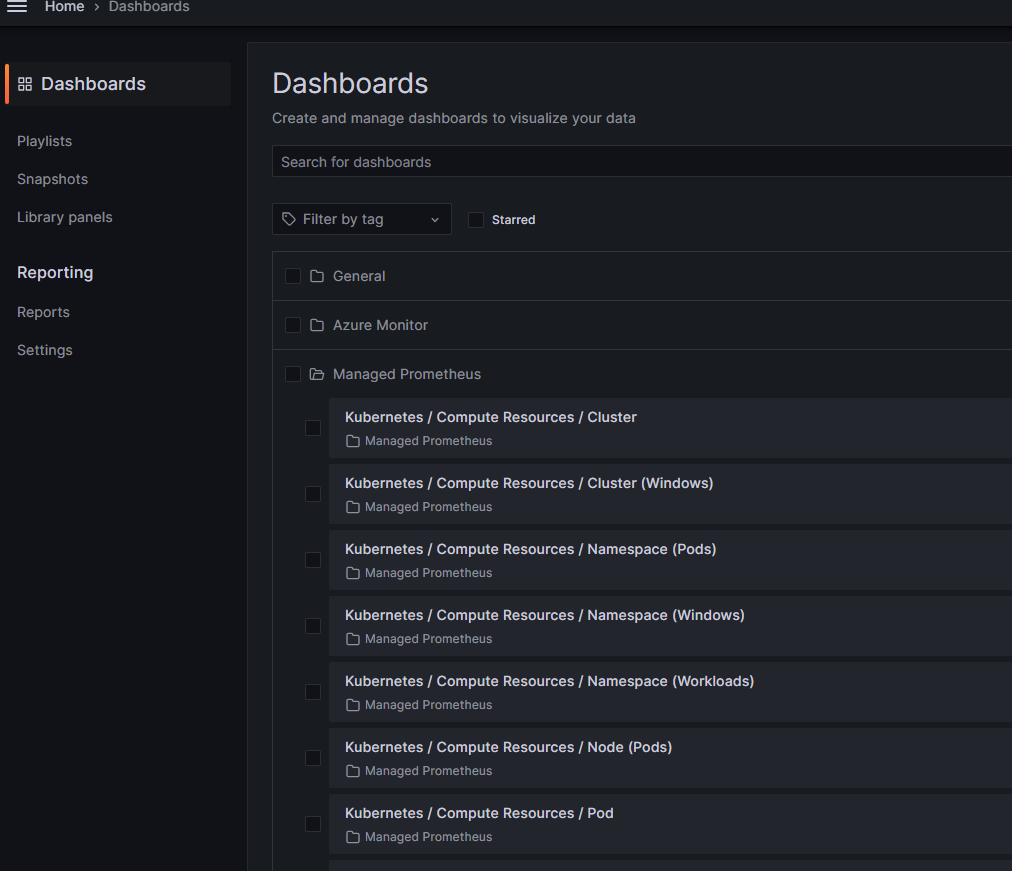


1. Scroll to the bottom of the page and select **Save & test**.

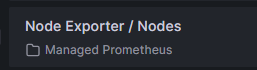


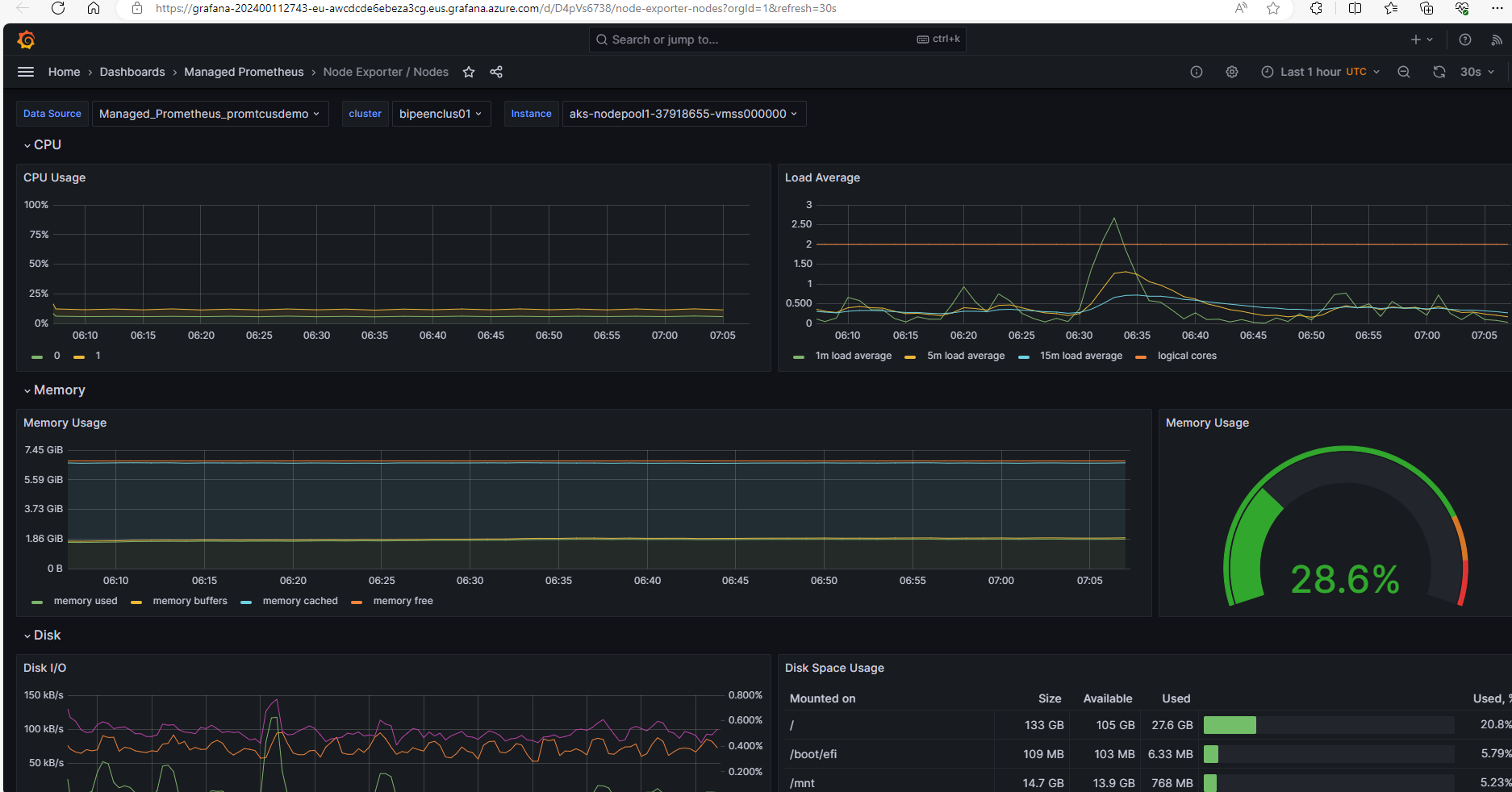


# Use Graphana

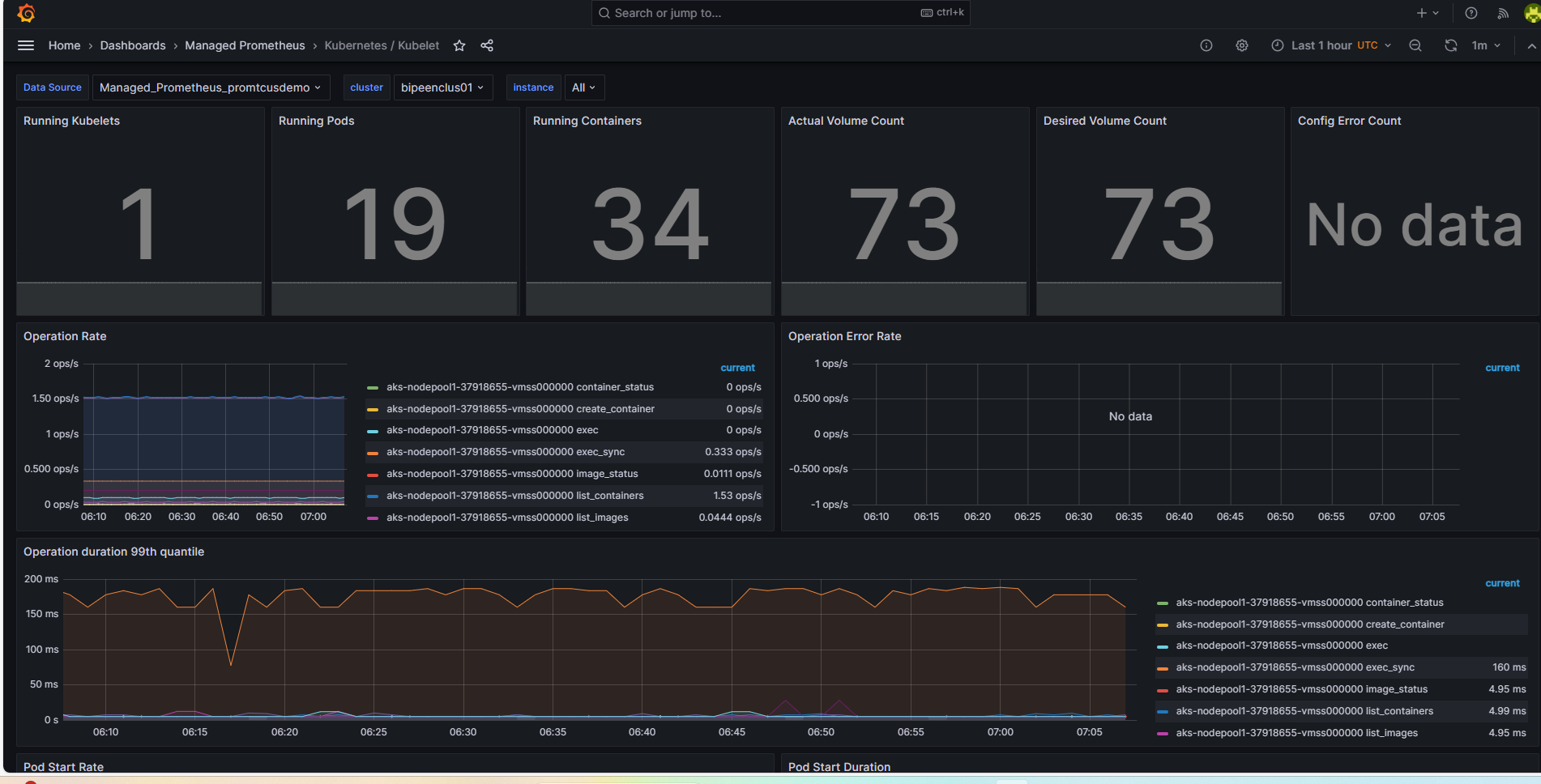


Open Node Explorere

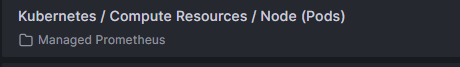








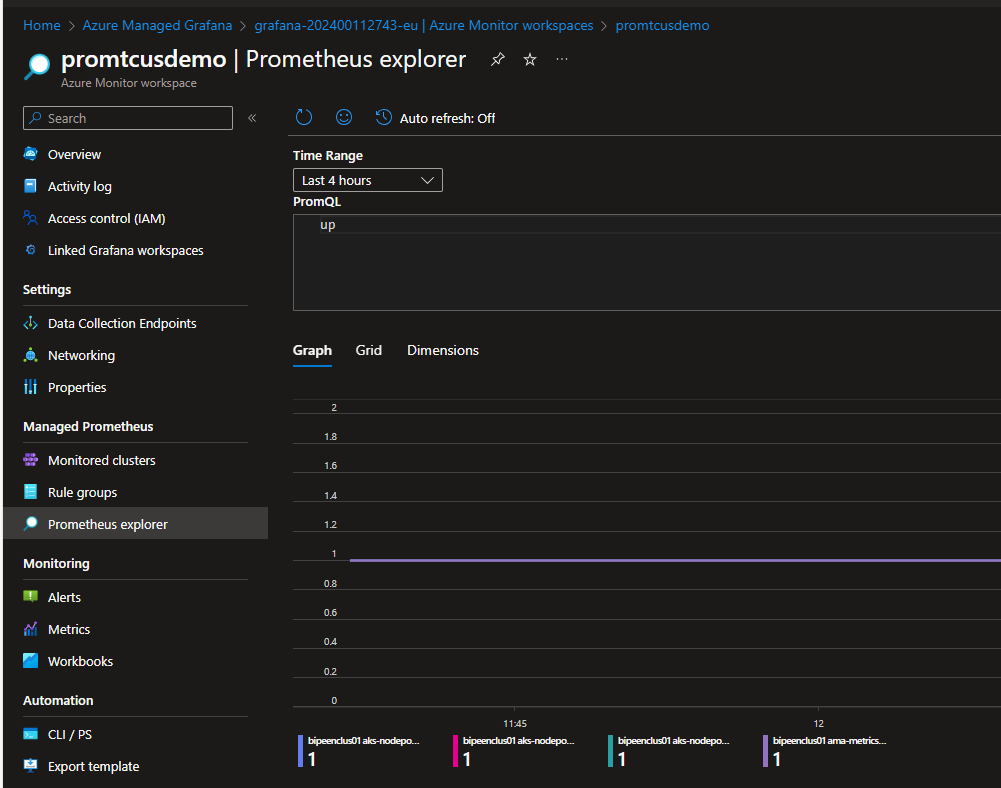




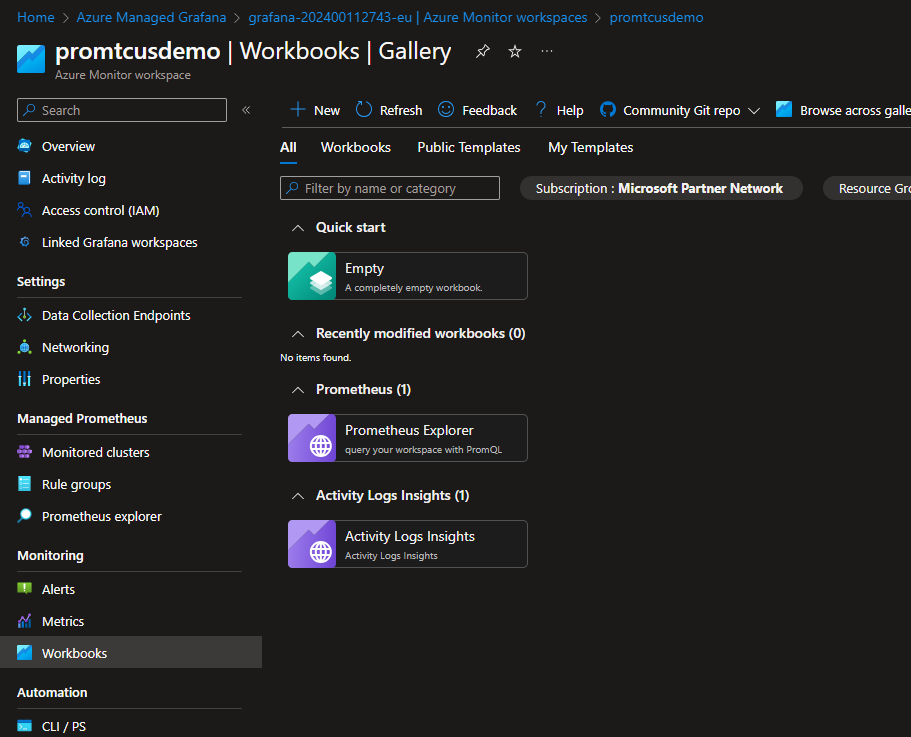
# Prometheus Explorer workbook

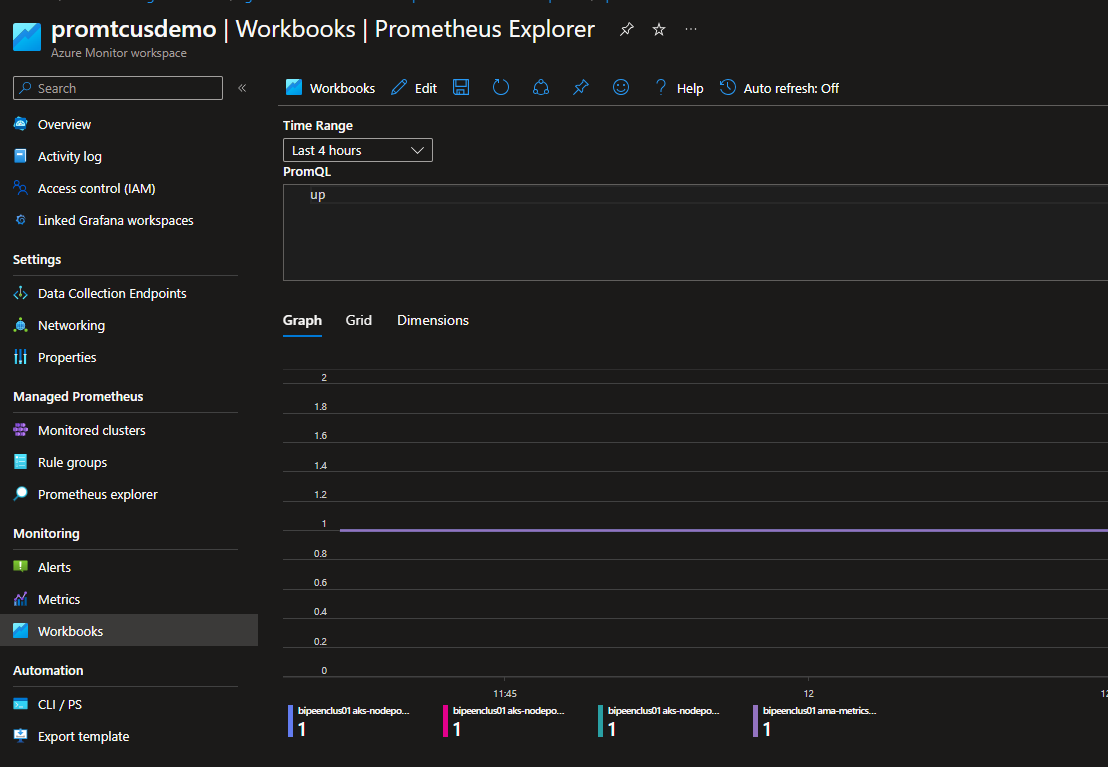
Azure Monitor workspaces include an exploration workbook to query your Prometheus metrics.

1. From the Azure Monitor workspace overview page, select **Prometheus explorer**



1. Or the **Workbooks** menu item, and in the Azure Monitor workspace gallery, select the **Prometheus Explorer** workbook tile.





\

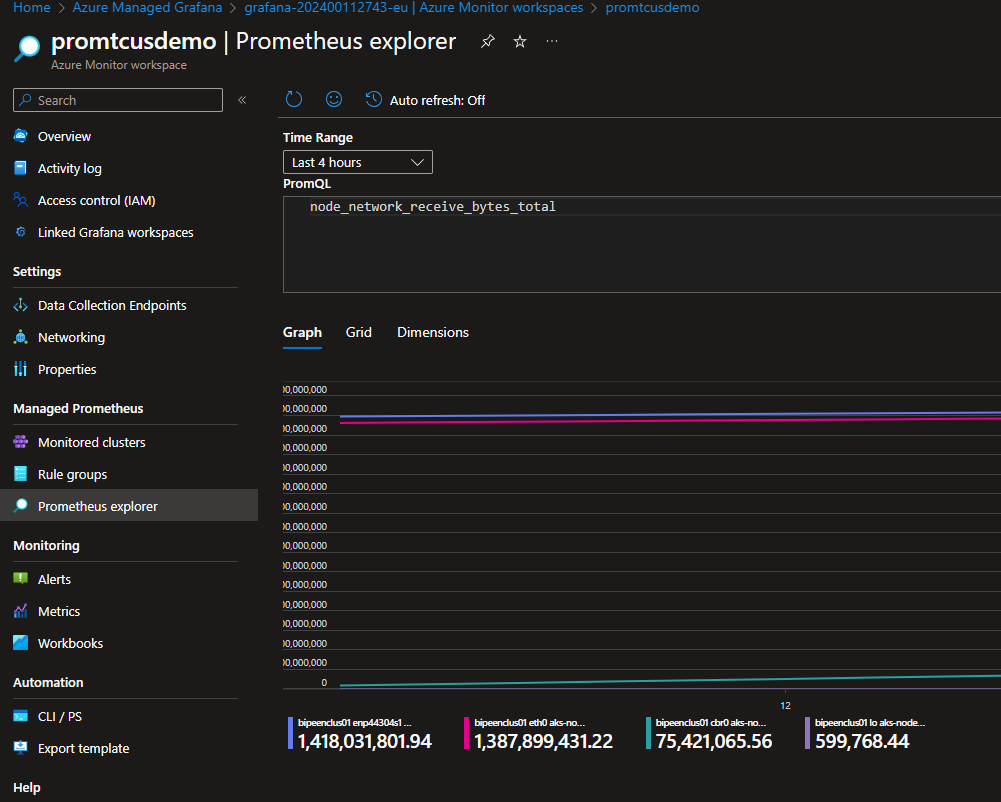
# [PromQL](https://prometheus.io/docs/prometheus/latest/querying/basics/)

[PromQL](https://prometheus.io/docs/prometheus/latest/querying/basics/) is a query language for [Prometheus monitoring system](https://prometheus.io/). It is designed for building powerful yet simple queries for graphs, alerts or derived time series (aka [recording rules](https://prometheus.io/docs/prometheus/latest/configuration/recording_rules/)). PromQL is designed from scratch and has zero common grounds with other query languages used in time series databases such as [SQL in TimescaleDB](https://www.timescale.com/), [InfluxQL](https://docs.influxdata.com/influxdb/v1.7/query_language/" \t "_blank) or [Flux](https://github.com/influxdata/flux).

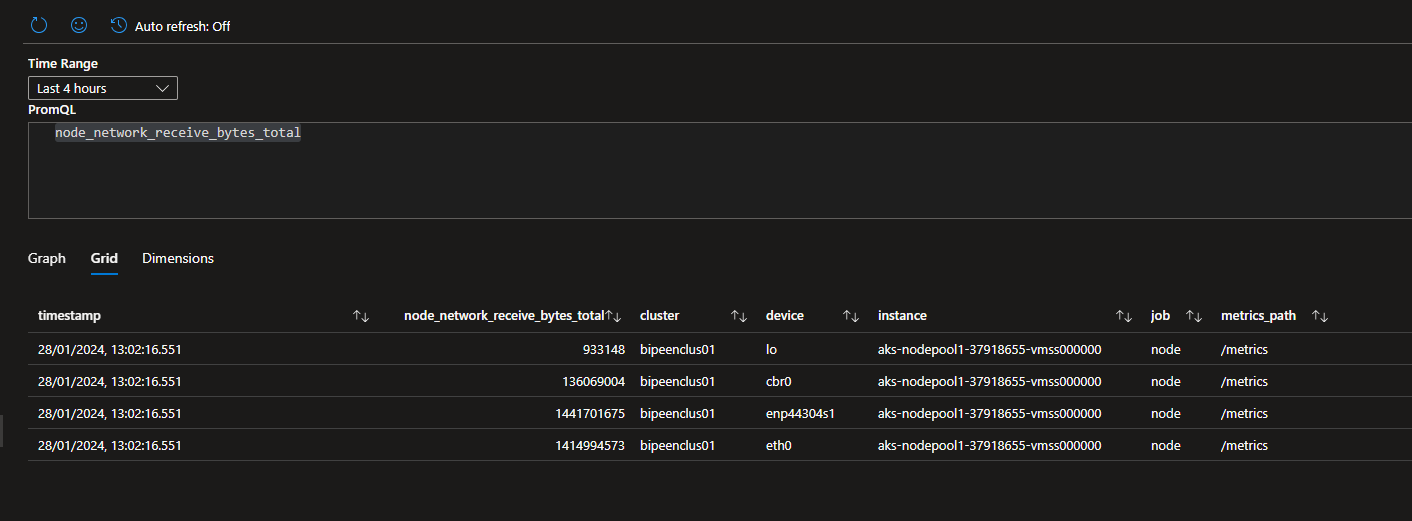
## Selecting a time series with PromQL

Selecting a time series with PromQL is as simple as writing a time series name in the query. For instance, the following query would return all the time series with name node\_network\_receive\_bytes\_total:

node\_network\_receive\_bytes\_total



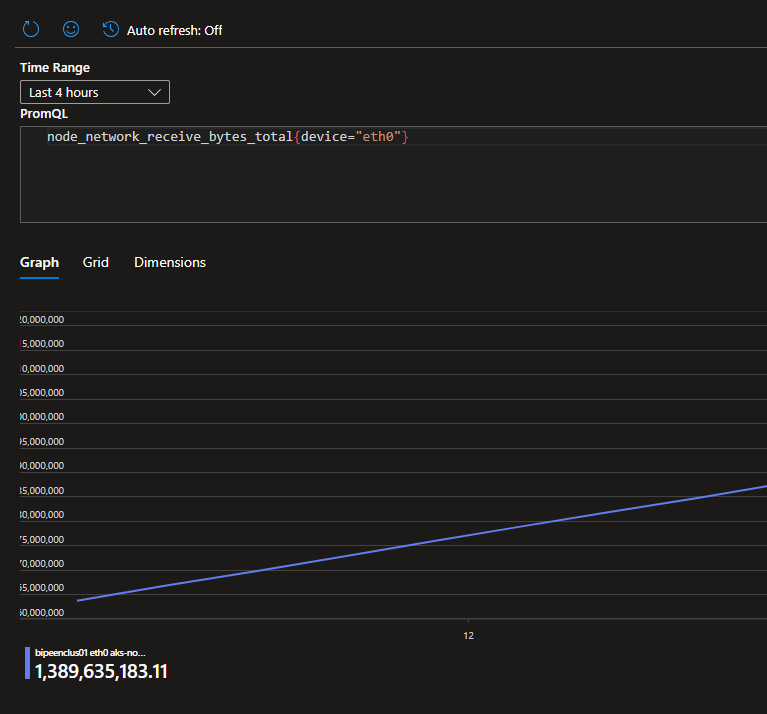
See the grid view also



## Filtering by label

A single metric name may correspond to multiple time series with distinct label sets as in the example above. How to select time series matching only {device="eth0"}? Just mention the required label in the query

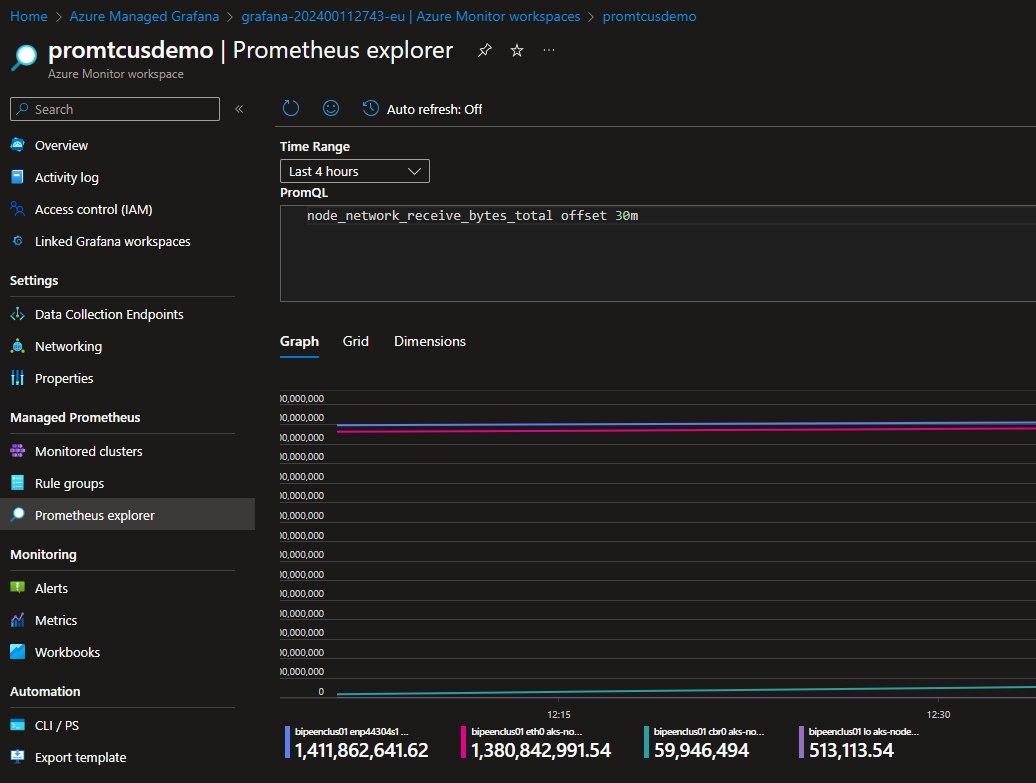
node\_network\_receive\_bytes\_total{device="eth0"}



## Comparing current data with historical data

PromQL allows querying historical data and combining / comparing it to the current data. Just add [offset](https://prometheus.io/docs/prometheus/latest/querying/basics/#offset-modifier) to the query. For instance, the following query would return 30 min old for all the time series with node\_network\_receive\_bytes\_total name:

node\_network\_receive\_bytes\_total offset 30m



az group delete --name AKSDemo --yes --no-wait