

# Azure Monitoring

Azure Monitor maximizes the availability and performance of your applications and services by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.

Just a few examples of what you can do with Azure Monitor include:

- Detect and diagnose issues across applications and dependencies with [Application Insights](#).
- Correlate infrastructure issues with [Azure Monitor for VMs](#) and [Azure Monitor for Containers](#).
- Drill into your monitoring data with [Log Analytics](#) for troubleshooting and deep diagnostics.
- Support operations at scale with [smart alerts](#) and [automated actions](#).
- Create visualizations with Azure [dashboards](#) and [workbooks](#).

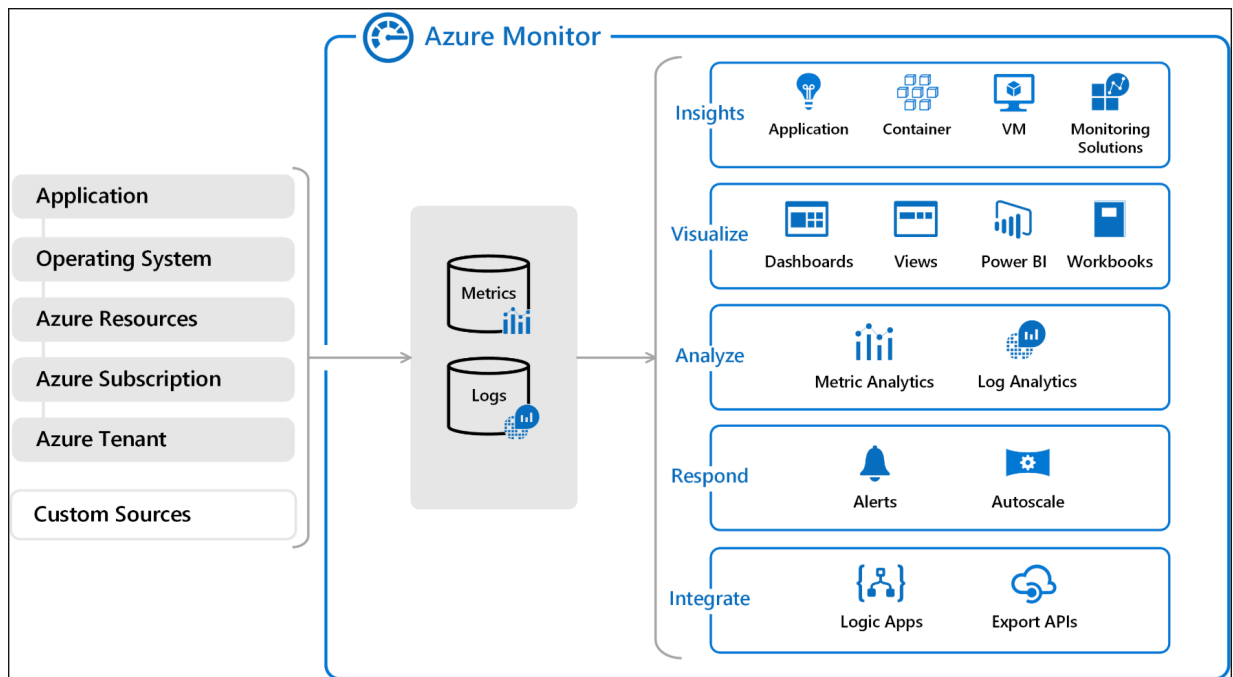
<https://docs.microsoft.com/en-us/azure/azure-monitor/overview>

Diagnostic logs provide rich, frequent data about the operation of an Azure resource. Azure Monitor makes the following two types of diagnostic logs available.

- **Tenant logs:** These logs come from tenant-level services that exist outside of an Azure subscription, such as Azure Active Directory logs.
- **Resource logs:** These logs come from Azure services that deploy resources within an Azure subscription, such as network security groups or Storage accounts.

## Overview

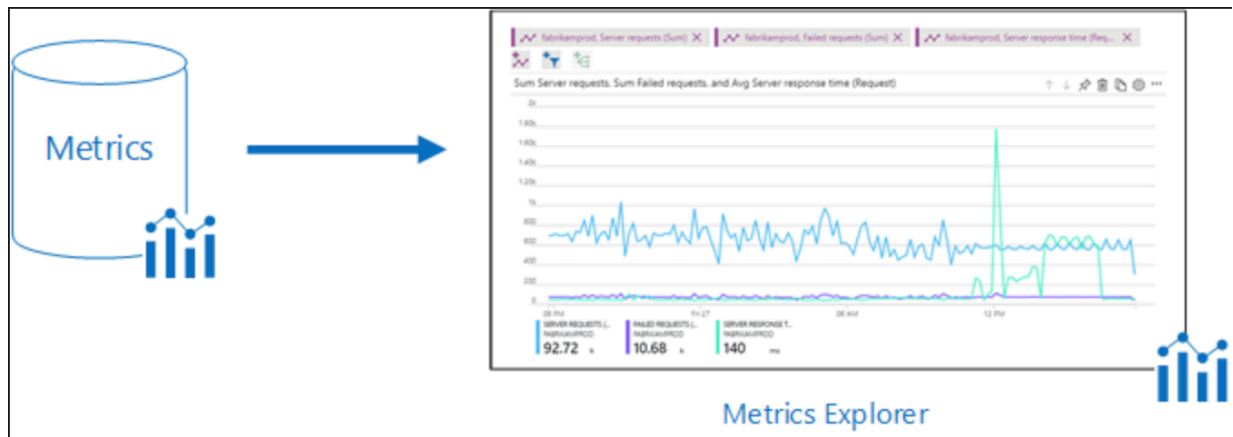
The following diagram gives a high-level view of Azure Monitor. At the center of the diagram are the data stores for metrics and logs, which are the two fundamental types of data use by Azure Monitor. On the left are the [sources of monitoring data](#) that populate these [data stores](#). On the right are the different functions that Azure Monitor performs with this collected data such as analysis, alerting, and streaming to external systems.



## Monitoring data platform

All data collected by Azure Monitor fits into one of two fundamental types, [metrics and logs](#). [Metrics](#) are numerical values that describe some aspect of a system at a particular point in time. They are lightweight and capable of supporting near real-time scenarios. [Logs](#) contain different kinds of data organized into records with different sets of properties for each type. Telemetry such as events and traces are stored as logs in addition to performance data so that it can all be combined for analysis.

For many Azure resources, you'll see data collected by Azure Monitor right in their Overview page in the Azure portal. Have a look at any virtual machine for example, and you'll see several charts displaying performance metrics. Click on any of the graphs to open the data in [metrics explorer](#) in the Azure portal, which allows you to chart the values of multiple metrics over time. You can view the charts interactively or pin them to a dashboard to view them with other visualizations.



Log data collected by Azure Monitor can be analyzed with [queries](#) to quickly retrieve, consolidate, and analyze collected data. You can create and test queries using [Log Analytics](#) in the Azure portal and then either directly analyze the data using these tools or save queries for use with [visualizations](#) or [alert rules](#). Azure Monitor uses a version of the [Kusto query language](#) used by Azure Data Explorer that is suitable for simple log queries but also includes advanced functionality such as aggregations, joins, and smart analytics.



## What data does Azure Monitor collect?

Azure Monitor can collect data from a variety of sources. You can think of monitoring data for your applications in tiers ranging from your application, any operating system and services it relies on, down to the platform itself. Azure Monitor collects data from each of the following tiers:

- **Application monitoring data:** Data about the performance and functionality of the code you have written, regardless of its platform.
- **Guest OS monitoring data:** Data about the operating system on which your application is running. This could be running in Azure, another cloud, or on-premises.

- **Azure resource monitoring data:** Data about the operation of an Azure resource.
- **Azure subscription monitoring data:** Data about the operation and management of an Azure subscription, as well as data about the health and operation of Azure itself.
- **Azure tenant monitoring data:** Data about the operation of tenant-level Azure services, such as Azure Active Directory.

As soon as you create an Azure subscription and start adding resources such as virtual machines and web apps, Azure Monitor starts collecting data.

[Activity logs](#) record when resources are created or modified.

[Metrics](#) tell you how the resource is performing and the resources that it's consuming.

Extend the data you're collecting into the actual operation of the resources by [enabling diagnostics](#) and [adding an agent](#) to compute resources. This will collect telemetry for the internal operation of the resource and allow you to configure different [data sources](#) to collect logs and metrics from Windows and Linux guest operating system.

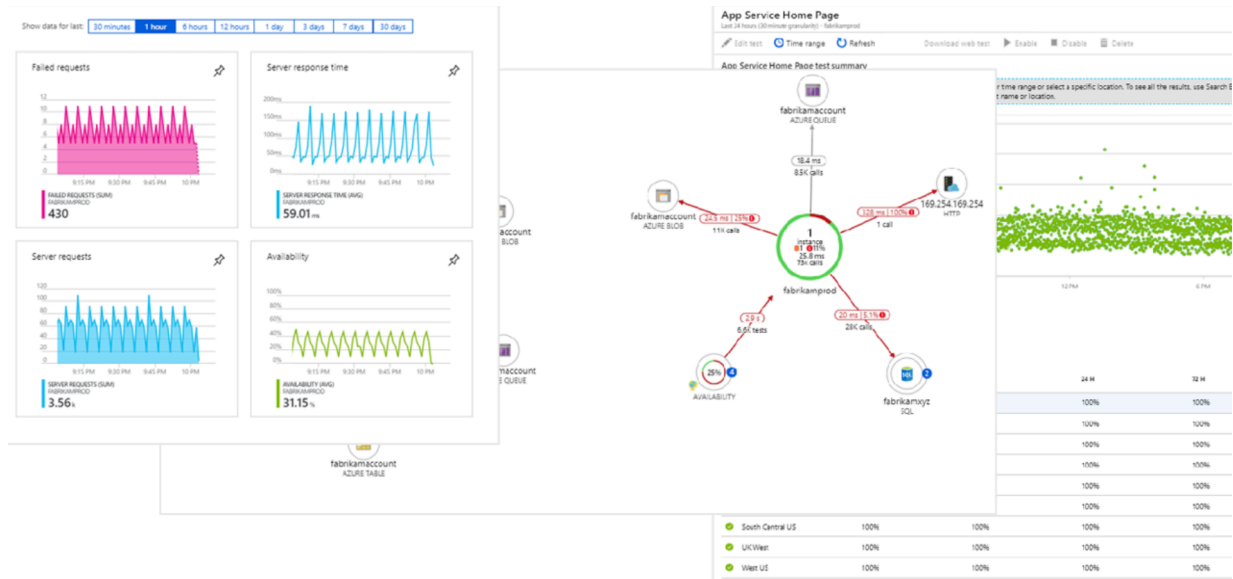
Enable monitoring for your [App Services application](#) or [VM and virtual machine scale set application](#), to enable Application Insights to collect detailed information about your application including page views, application requests, and exceptions. Further verify the availability of your application by configuring an [availability test](#) to simulate user traffic.

## Insights

Monitoring data is only useful if it can increase your visibility into the operation of your computing environment. Azure Monitor includes several features and tools that provide valuable insights into your applications and other resources that they depend on. [Monitoring solutions](#) and features such as [Application Insights](#) and [Azure Monitor for containers](#) provide deep insights into different aspects of your application and specific Azure services.

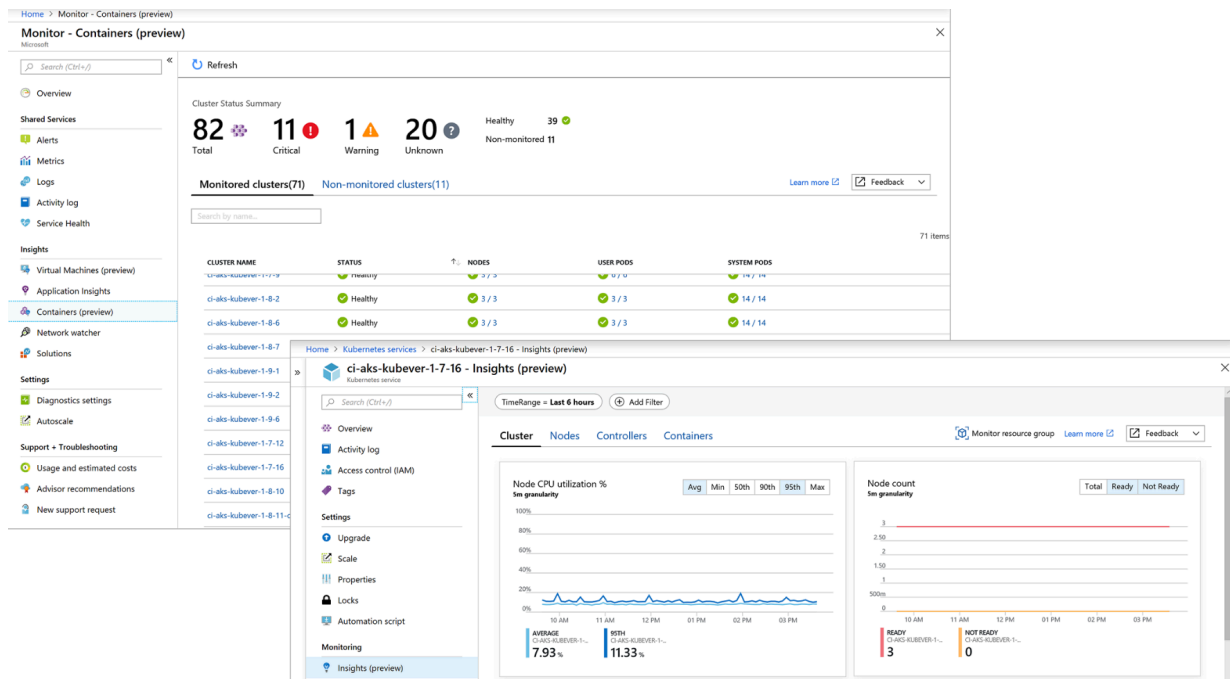
### Application Insights

[Application Insights](#) monitors the availability, performance, and usage of your web applications whether they're hosted in the cloud or on-premises. It leverages the powerful data analysis platform in Azure Monitor to provide you with deep insights into your application's operations and diagnose errors without waiting for a user to report them. Application Insights includes connection points to a variety of development tools and integrates with Visual Studio to support your DevOps processes.



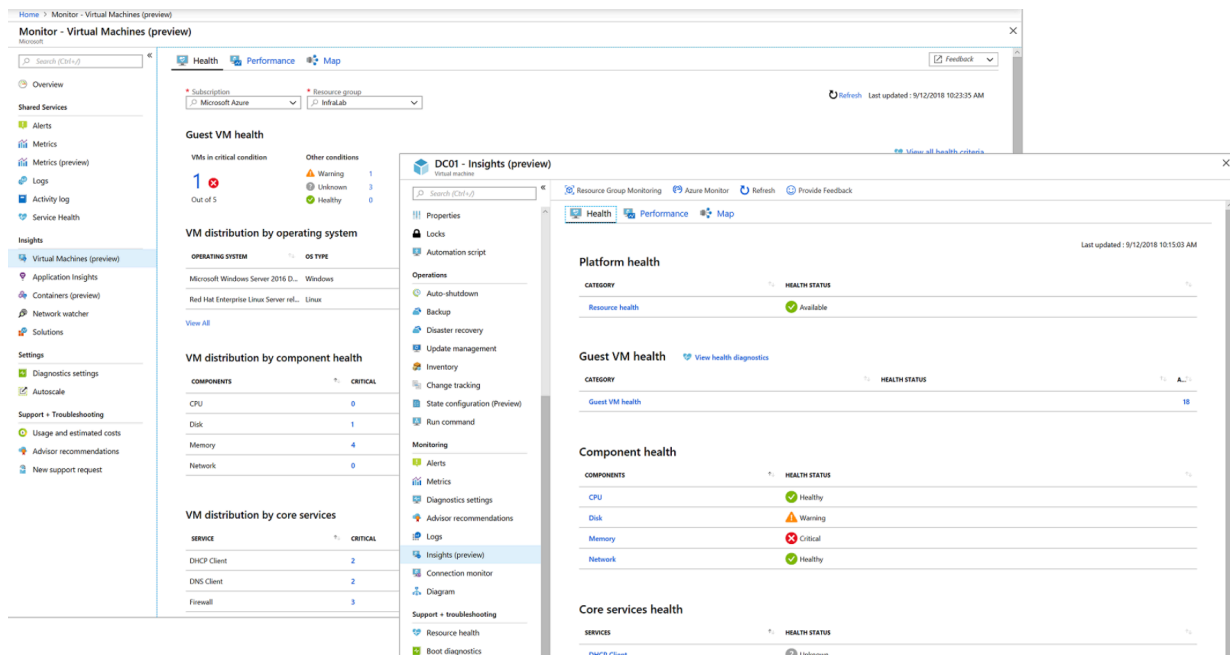
## Azure Monitor for containers

[Azure Monitor for containers](#) is a feature designed to monitor the performance of container workloads deployed to managed Kubernetes clusters hosted on Azure Kubernetes Service (AKS). It gives you performance visibility by collecting memory and processor metrics from controllers, nodes, and containers that are available in Kubernetes through the Metrics API. Container logs are also collected. After you enable monitoring from Kubernetes clusters, these metrics and logs are automatically collected for you through a containerized version of the Log Analytics agent for Linux.



## Azure Monitor for VMs

Azure Monitor for VMs monitors your Azure virtual machines (VM) at scale by analyzing the performance and health of your Windows and Linux VMs, including their different processes and interconnected dependencies on other resources and external processes. The solution includes support for monitoring performance and application dependencies for VMs hosted on-premises or another cloud provider.

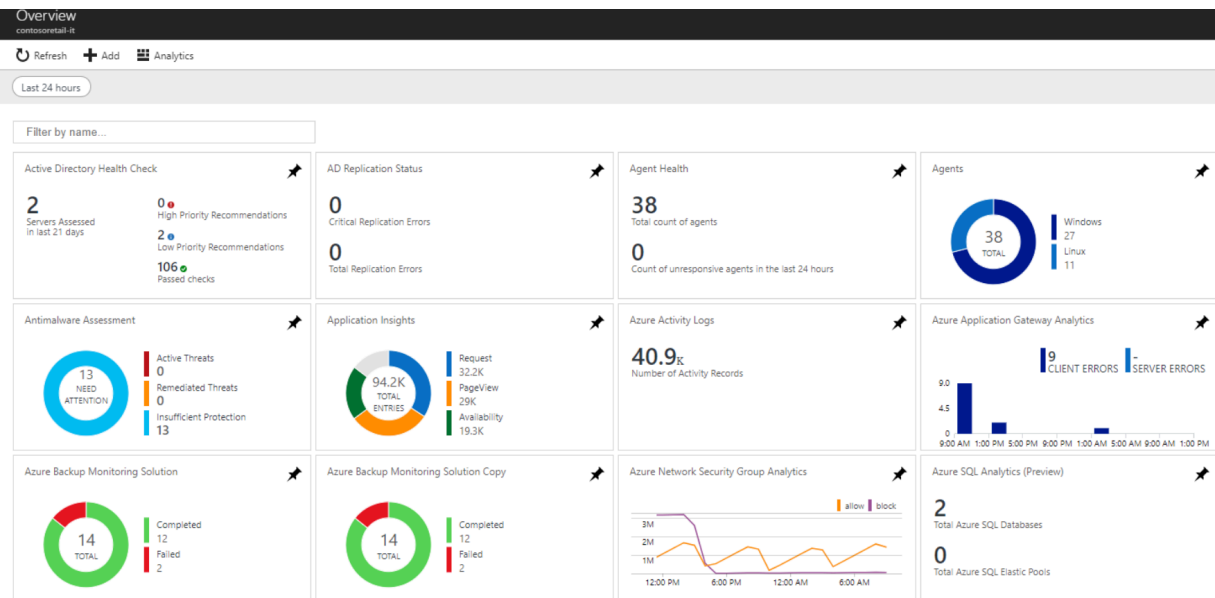


## Monitoring solutions

[Monitoring solutions](#) in Azure Monitor are packaged sets of logic that provide insights for a particular application or service.

Monitoring solutions leverage services in Azure to provide additional insight into the operation of a particular application or service.

They include logic for collecting monitoring data for the application or service, [queries](#) to analyze that data, and [views](#) for visualization. Monitoring solutions are [available from Microsoft](#) and partners to provide monitoring for various Azure services and other applications.

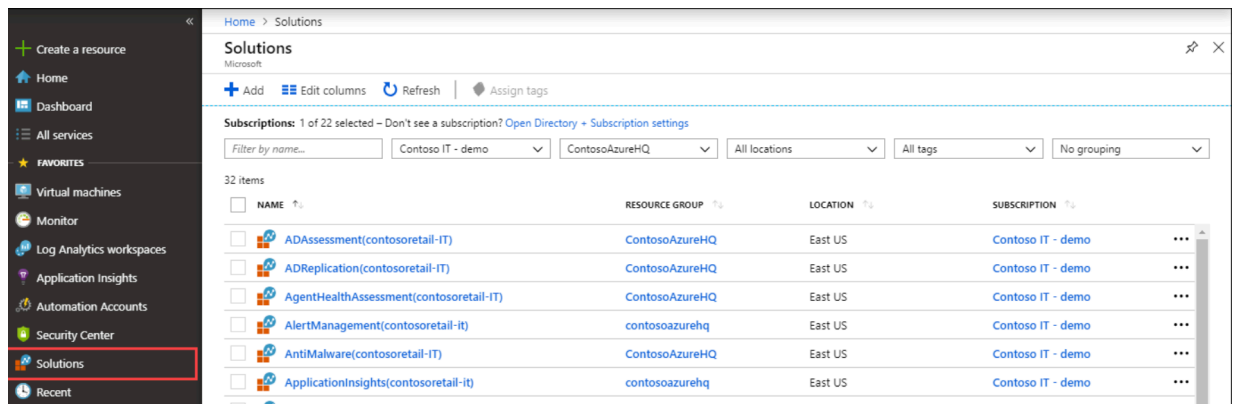


Monitoring solutions can contain multiple types of Azure resources, and you can view any resources included with a solution just like any other resource. For example, any log queries included in the solution are listed under **Solution Queries** in [Query explorer](#). You can use those queries when performing ad hoc analysis with [log queries](#).

### List installed monitoring solutions

Use the following procedure to list the monitoring solutions installed in your subscription.

1. Log in to the Azure portal.
2. Open **All services** and locate **Solutions**.
3. Solutions installed in all your workspaces are listed. The name of the solution is followed by the name of the workspace it's installed in.
4. Use the dropdown boxes at the top of the screen to filter by subscription or resource group.

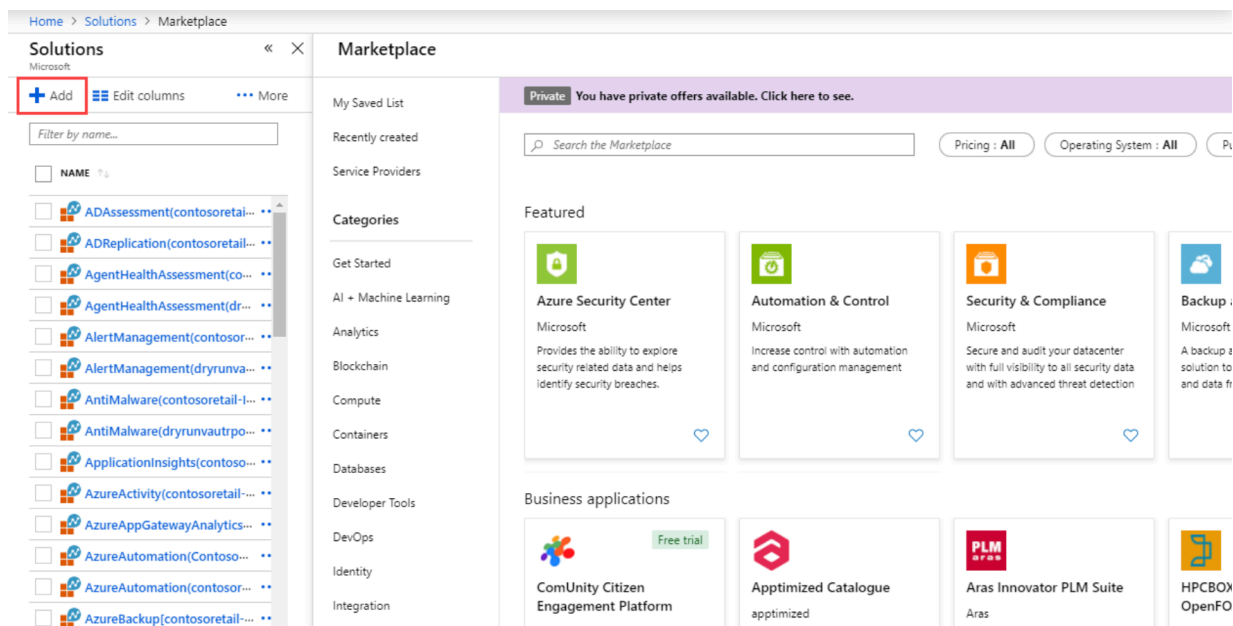


NAME	RESOURCE GROUP	LOCATION	SUBSCRIPTION
ADAssessment(contosoetail-IT)	ContosoAzureHQ	East US	Contoso IT - demo
ADReplication(contosoetail-IT)	ContosoAzureHQ	East US	Contoso IT - demo
AgentHealthAssessment(contosoetail-IT)	ContosoAzureHQ	East US	Contoso IT - demo
AlertManagement(contosoetail-IT)	contosoazurehq	East US	Contoso IT - demo
AntiMalware(contosoetail-IT)	ContosoAzureHQ	East US	Contoso IT - demo
ApplicationInsights(contosoetail-IT)	contosoazurehq	East US	Contoso IT - demo

## Install a monitoring solution

Monitoring solutions from Microsoft and partners are available from the [Azure Marketplace](#). You can search available solutions and install them using the following procedure. When you install a solution, you must select a [Log Analytics workspace](#) where the solution will be installed and where its data will be collected.

1. From the [list of solutions for your subscription](#), click **Add**.
2. Browse or search for a solution. You can also browse solutions from [this search link](#).
3. Locate the monitoring solution you want and read through its description.
4. Click **Create** to start the installation process.
5. When the installation process starts, you're prompted to specify the Log Analytics workspace and provide any required configuration for the solution.



**Solutions**

**Marketplace**

Private You have private offers available. Click here to see.

Search the Marketplace

Pricing: All Operating System: All

**Featured**

- Azure Security Center** (Microsoft): Provides the ability to explore security related data and helps identify security breaches.
- Automation & Control** (Microsoft): Increase control with automation and configuration management.
- Security & Compliance** (Microsoft): Secure and audit your datacenter with full visibility to all security data and with advanced threat detection.
- Backup** (Microsoft): A backup solution to and data fr...

**Business applications**

- ComUnity Citizen Engagement Platform** (Green trial)
- Apptimized Catalogue** (apptimized)
- Aras Innovator PLM Suite** (Aras)
- HPCBOX OpenFO** (HPCBOX)

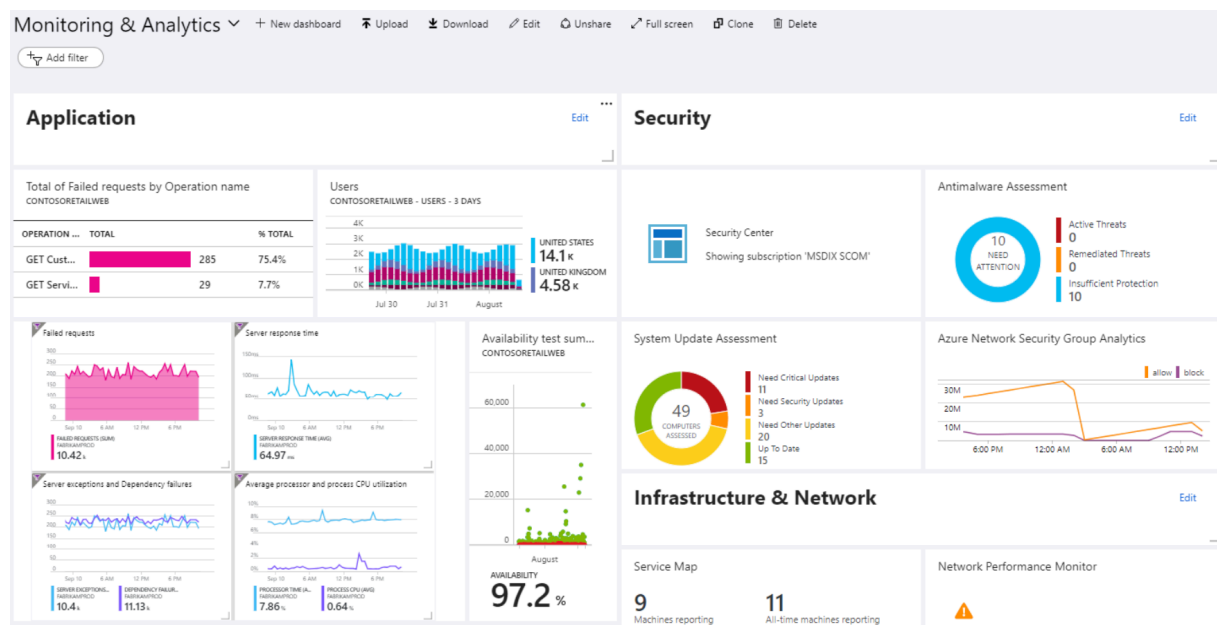
## Visualizing monitoring data



[Visualizations](#) such as charts and tables are effective tools for summarizing monitoring data and presenting it to different audiences. Azure Monitor has its own features for visualizing monitoring data and leverages other Azure services for publishing it to different audiences.

## Dashboards

[Azure dashboards](#) allow you to combine different kinds of data, including both metrics and logs, into a single pane in the [Azure portal](#). You can optionally share the dashboard with other Azure users. Elements throughout Azure Monitor can be added to an Azure dashboard in addition to the output of any log query or metrics chart. For example, you could create a dashboard that combines tiles that show a graph of metrics, a table of activity logs, a usage chart from Application Insights, and the output of a log query.



## Power BI

[Power BI](#) is a business analytics service that provides interactive visualizations across a variety of data sources and is an effective means of making data available to others within and outside your organization. You can configure Power BI to [automatically import log data from Azure Monitor](#) to take advantage of these additional visualizations.

## Integrate and export data

You'll often have the requirement to integrate Azure Monitor with other systems and to build custom solutions that use your monitoring data. Other Azure services

work with Azure Monitor to provide this integration.

### Event Hub

[Azure Event Hubs](#) is a streaming platform and event ingestion service that can transform and store data using any real-time analytics provider or batching/storage adapters. Use Event Hubs to [stream Azure Monitor data](#) to partner SIEM and monitoring tools.

### Logic Apps

[Logic Apps](#) is a service that allows you to automate tasks and business processes using workflows that integrate with different systems and services. Activities are available that read and write metrics and logs in Azure Monitor, which allows you to build workflows integrating with a variety of other systems.

### API

Multiple APIs are available to read and write metrics and logs to and from Azure Monitor in addition to accessing generated alerts. You can also configure and retrieve alerts. This provides you with essentially unlimited possibilities to build custom solutions that integrate with Azure Monitor.

## Monitor virtual machines in Azure

To detect and help diagnose performance and health issues with the guest operating system, .NET based or Java web application components running inside the VM, Azure Monitor delivers centralized monitoring with comprehensive features such as Azure Monitor for VMs and Application Insights.

### Diagnostics and metrics

You can set up and monitor the collection of [diagnostics data](#) using [metrics](#) in the Azure portal, the Azure CLI, Azure PowerShell, and programming Applications Programming Interfaces (APIs). For example, you can:

- **Observe basic metrics for the VM.** On the Overview screen of the Azure portal, the basic metrics shown include CPU usage, network usage, total of disk bytes, and disk operations per second.
- **Enable the collection of boot diagnostics and view it using the Azure portal.** When bringing your own image to Azure or even booting one of the platform images, there can be many reasons why a VM gets into a non-bootable state. You can easily enable boot diagnostics when you create a VM by clicking **Enabled** for Boot Diagnostics under the Monitoring section of the Settings screen.

As VMs boot, the boot diagnostic agent captures boot output and stores it in Azure storage. This data can be used to troubleshoot VM boot issues. Boot diagnostics are not automatically enabled when you create a VM from command-line tools. Before enabling boot diagnostics, a storage account needs to be created for storing boot logs. If you enable boot diagnostics in the Azure portal, a storage account is automatically created for you.

If you didn't enable boot diagnostics when the VM was created, you can always enable it later by using [Azure CLI](#), [Azure PowerShell](#), or an [Azure Resource Manager template](#).

- **Enable the collection of guest OS diagnostics data.** When you create a VM, you have the opportunity on the settings screen to enable guest OS diagnostics. When you do enable the collection of diagnostics data, the [IaaS.Diagnostics extension for Linux](#) or the [IaaS.Diagnostics extension for Windows](#) is added to the VM, which enables you to collect additional disk, CPU, and memory data.

Using the collected diagnostics data, you can configure autoscaling for your VMs. You can also configure [Azure Monitor Logs](#) to store the data and set up alerts to let you know when performance isn't right.

## Azure Activity Log

The [Azure Activity Log](#) is a subscription log that provides insight into subscription-level events that have occurred in Azure. The log includes a range of data, from Azure Resource Manager operational data to updates on Service Health events. You can click Activity Log in the Azure portal to view the log for your VM.

Some of the things you can do with the activity log include:

- Create an [alert on an Activity Log event](#).
- [Stream it to an Event Hub](#) for ingestion by a third-party service or custom analytics solution such as Power BI.
- Analyze it in Power BI using the [Power BI content pack](#).
- [Save it to a storage account](#) for archival or manual inspection. You can specify the retention time (in days) using the Log Profile.

You can also access activity log data by using [Azure PowerShell](#), the [Azure CLI](#), or [Monitor REST APIs](#).

**[Azure Resource Logs](#) are logs emitted by your VM** that provide rich, frequent data about its operation. Resource logs differ from the activity log by providing insight about operations that were performed within the VM.

Some of the things you can do with diagnostics logs include:

- [Save them to a storage account](#) for auditing or manual inspection. You can specify the retention time (in days) using Resource Diagnostic Settings.
- [Stream them to Event Hubs](#) for ingestion by a third-party service or custom analytics solution such as Power BI.

- Analyze them with [Log Analytics](#).

## Advanced monitoring

For visibility of the application or service supported by the Azure VM and virtual machine scale sets, identification of issues with the guest OS or workload running in the VM to understand if it is impacting availability or performance of the application, or is an issue with the application, enable both [Azure Monitor for VMs](#) and [Application Insights](#).

Azure Monitor for VMs monitors your Azure virtual machines (VM) at scale by analyzing the performance and health of your Windows and Linux VMs, including the different processes and interconnected dependencies on other resources and external processes it discovers. It includes several trend performance charts to help during investigation of problems and assess capacity of your VMs. The dependency map shows monitored and unmonitored machines, failed and active network connections between processes and these machines, and shows trend charts with standard network connection metrics. Combined with Application Insights, you monitor your application and capture telemetry such as HTTP requests, exceptions, etc. so you can correlate issues between the VMs and your application. Configure [Azure Monitor alerts](#) to alert you on important conditions detected from monitoring data collected by Azure Monitor for VMs.

## Monitor Apps in Azure

With Azure Monitor Application Insights, you can easily monitor your website for availability, performance, and usage. You can also quickly identify and diagnose errors in your application without waiting for a user to report them. Application Insights provides both server-side monitoring as well as client/browser-side monitoring capabilities.

### Enable Application Insights

Application Insights can gather telemetry data from any internet-connected application, running on-premises or in the cloud. Use the following steps to start viewing this data.

1. Select **Create a resource > Management tools > Application Insights**. Or Select **Create a resource > Developer tools > Application Insights**.

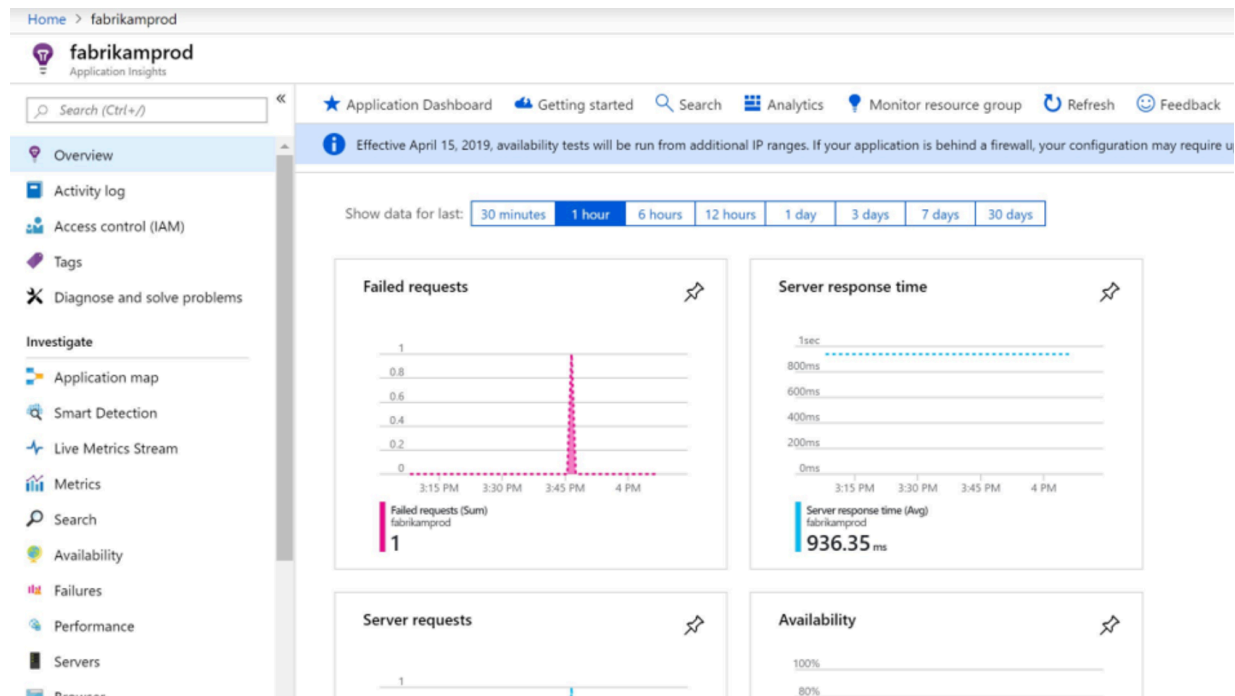
### Configure App Insights SDK

1. Select **Overview** and copy your application's **Instrumentation Key**.
2. Add the Application Insights SDK for Node.js/.NET/etc to your application.

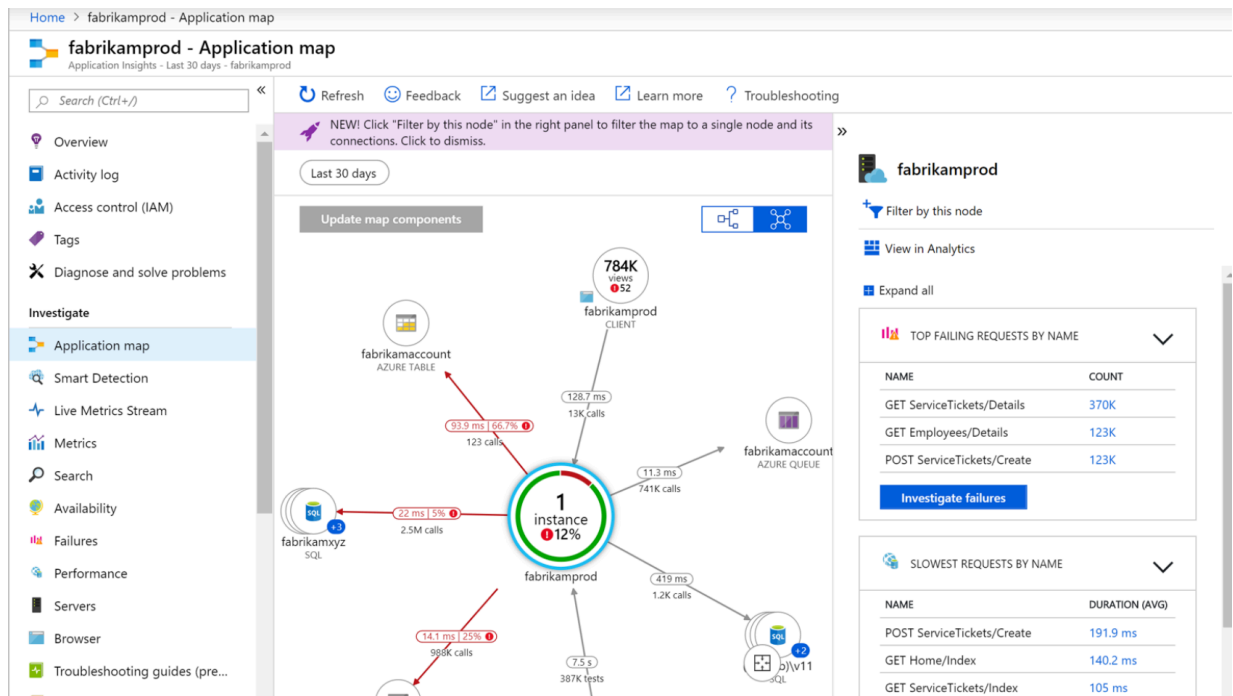
3. Edit your app and replace <instrumentation\_key> with your application's instrumentation key.
4. Restart your app

## Start monitoring in the Azure portal

1. You can now reopen the Application Insights **Overview** page in the Azure portal, where you retrieved your instrumentation key, to view details about your currently running application.



2. Select **Application map** for a visual layout of the dependency relationships between your application components. Each component shows KPIs such as load, performance, failures, and alerts.



3. Select the **App Analytics** icon **View in Analytics**. This opens **Application Insights Analytics**, which provides a rich query language for analyzing all data collected by Application Insights. In this case, a query is generated for you that renders the request count as a chart. You can write your own queries to analyze other data

