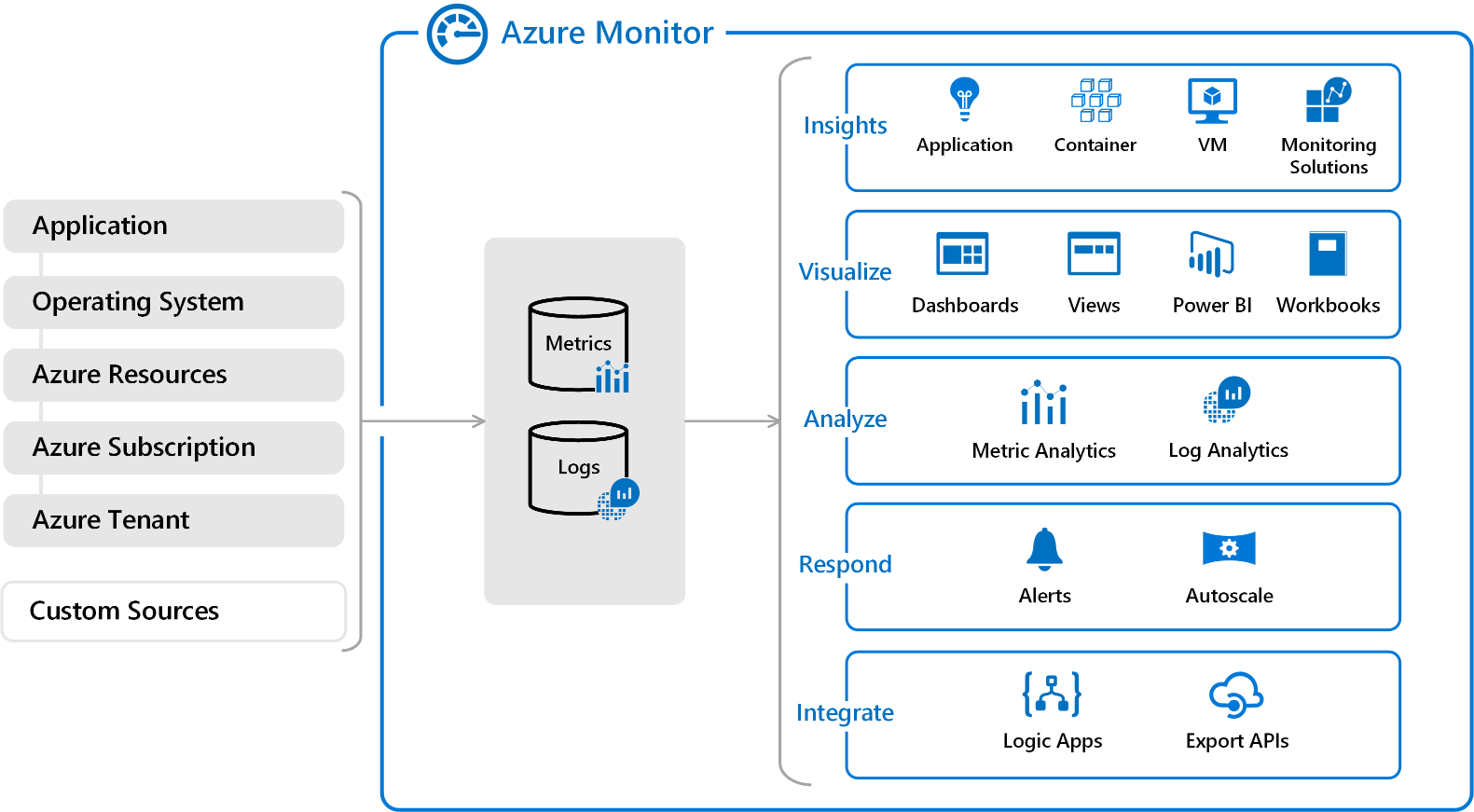
**Overview**

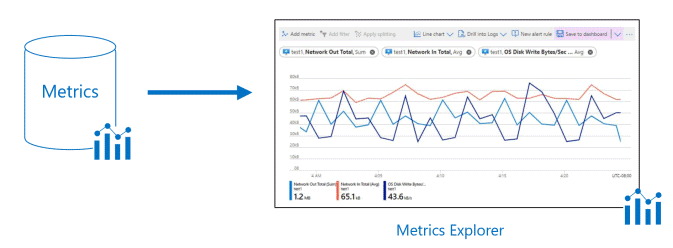
The following diagram gives a high-level view of Azure Monitor. At the center of the diagram are the data stores for metrics and logs, which are the two fundamental types of data used by Azure Monitor. On the left are the [sources of monitoring data](https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources) that populate these [data stores](https://docs.microsoft.com/en-us/azure/azure-monitor/data-platform). On the right are the different functions that Azure Monitor performs with this collected data. This includes such actions as analysis, alerting, and streaming to external systems.



**Monitoring data platform**

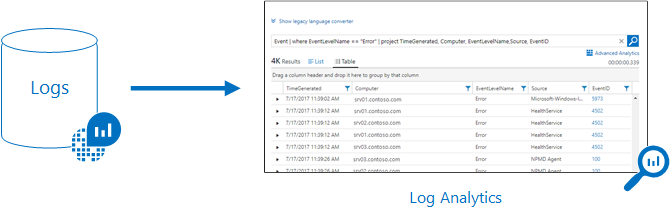
All data collected by Azure Monitor fits into one of two fundamental types, [metrics and logs](https://docs.microsoft.com/en-us/azure/azure-monitor/data-platform). [Metrics](https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/data-platform-metrics) are numerical values that describe some aspect of a system at a particular point in time. They are lightweight and capable of supporting near real-time scenarios. [Logs](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/data-platform-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](https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/metrics-charts) 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](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-query-overview) to quickly retrieve, consolidate, and analyze collected data. You can create and test queries using [Log Analytics](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-query-overview) in the Azure portal. You can then either directly analyze the data using different tools or save queries for use with [visualizations](https://docs.microsoft.com/en-us/azure/azure-monitor/best-practices-analysis) or [alert rules](https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-overview).

Azure Monitor uses a version of the [Kusto query language](https://docs.microsoft.com/en-us/azure/kusto/query/) that is suitable for simple log queries but also includes advanced functionality such as aggregations, joins, and smart analytics. You can quickly learn the query language using [multiple lessons](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries). Particular guidance is provided to users who are already familiar with [SQL](https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/sqlcheatsheet) and [Splunk](https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/splunk-cheat-sheet).



**What data does Azure Monitor collect?**

Azure Monitor can collect data from a [variety of sources](https://docs.microsoft.com/en-us/azure/azure-monitor/monitor-reference). This ranges 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. For a complete list of the resources that have metrics or logs, see [What can you monitor with Azure Monitor?](https://docs.microsoft.com/en-us/azure/azure-monitor/monitor-reference#azure-supported-services).
* **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](https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/platform-logs-overview) record when resources are created or modified. [Metrics](https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/data-platform-metrics) tell you how the resource is performing and the resources that it's consuming.

[Enable diagnostics](https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/platform-logs-overview) to extend the data you're collecting into the internal operation of the resources. [Add an agent](https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview) to compute resources to collect telemetry from their guest operating systems.

Enable monitoring for your application with [Application Insights](https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview) to collect detailed information including page views, application requests, and exceptions. Further verify the availability of your application by configuring an [availability test](https://docs.microsoft.com/en-us/azure/azure-monitor/app/monitor-web-app-availability) to simulate user traffic.

**Custom sources**

Azure Monitor can collect log data from any REST client using the [Data Collector API](https://docs.microsoft.com/en-us/azure/azure-monitor/logs/data-collector-api). This allows you to create custom monitoring scenarios and extend monitoring to resources that don't expose telemetry through other sources.

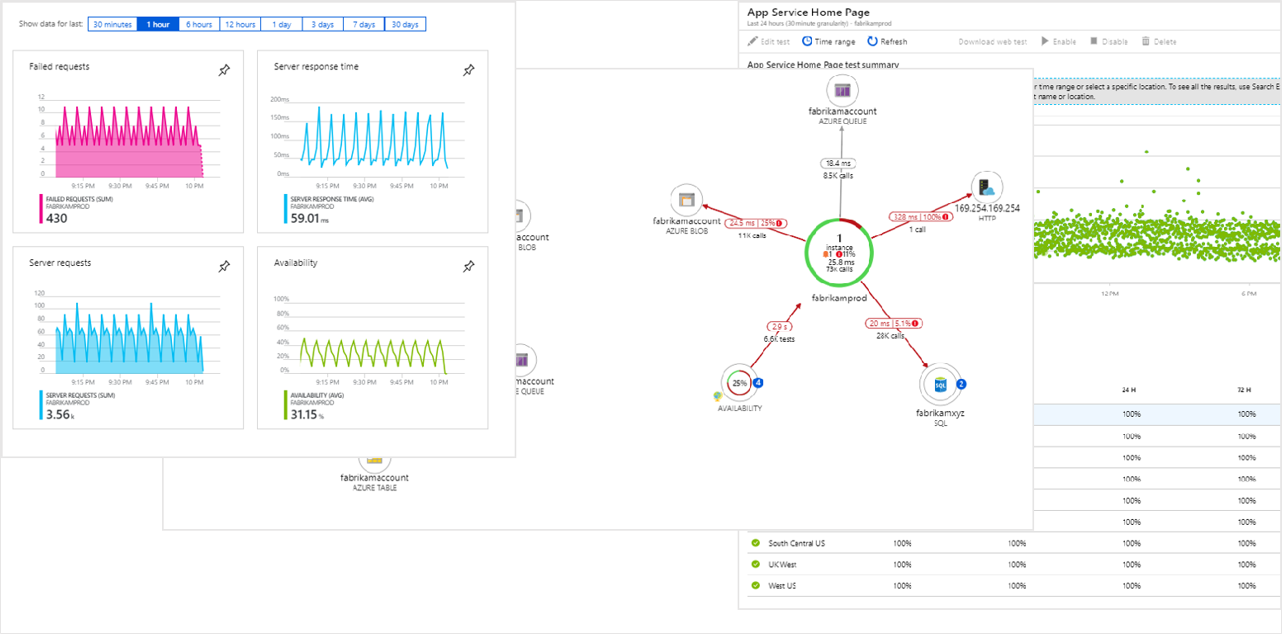
**Insights and curated visualizations**

Monitoring data is only useful if it can increase your visibility into the operation of your computing environment. Some Azure resource providers have a "curated visualization" which gives you a customized monitoring experience for that particular service or set of services. They generally require minimal configuration. Larger scalable curated visualizations are known as "insights" and marked with that name in the documentation and Azure portal.

For more information, see [List of insights and curated visualizations using Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/monitor-reference#insights-and-curated-visualizations). Some of the larger insights are also described below.

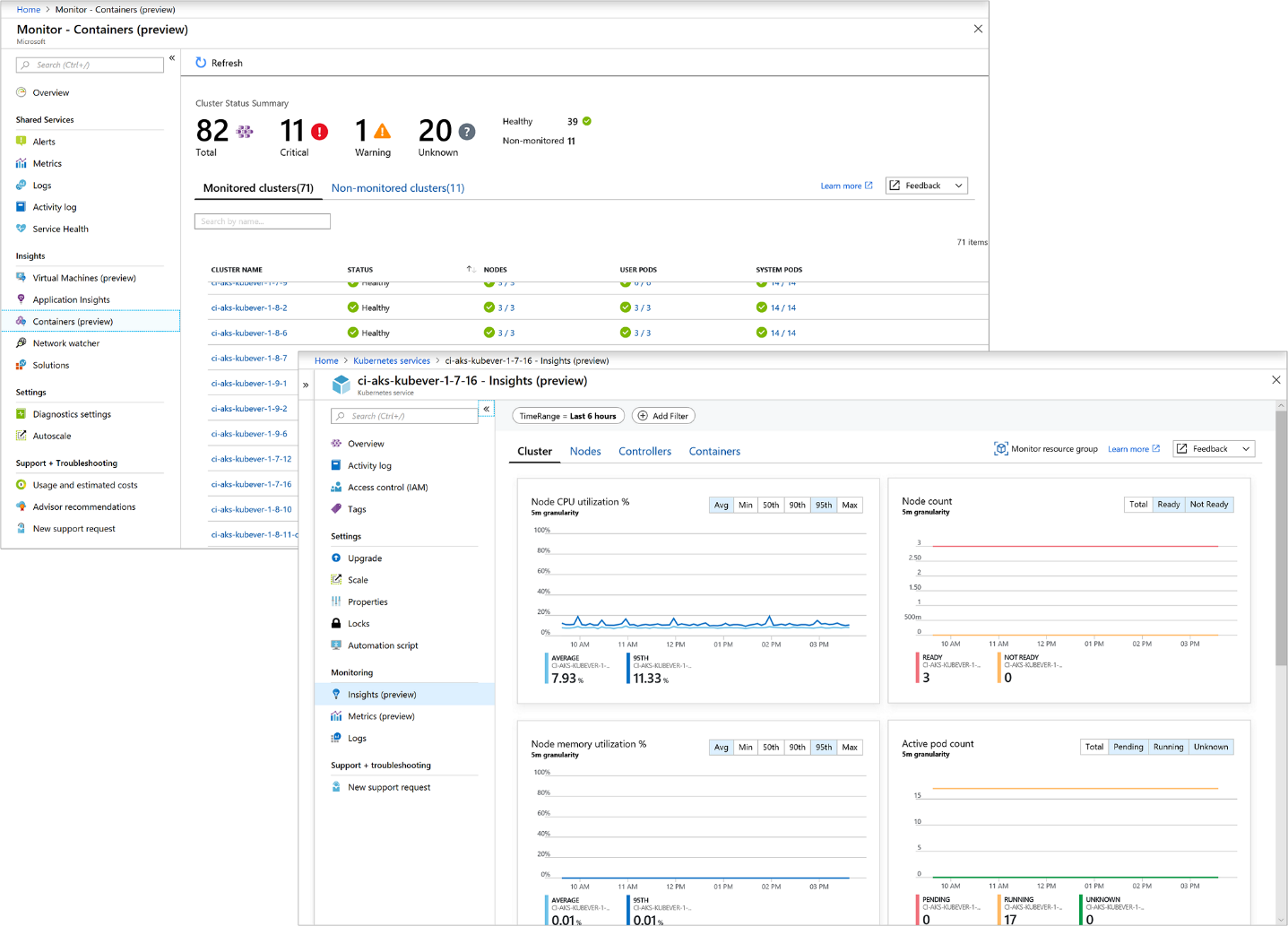
**Application Insights**

[Application Insights](https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview) 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. It enables you to 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.



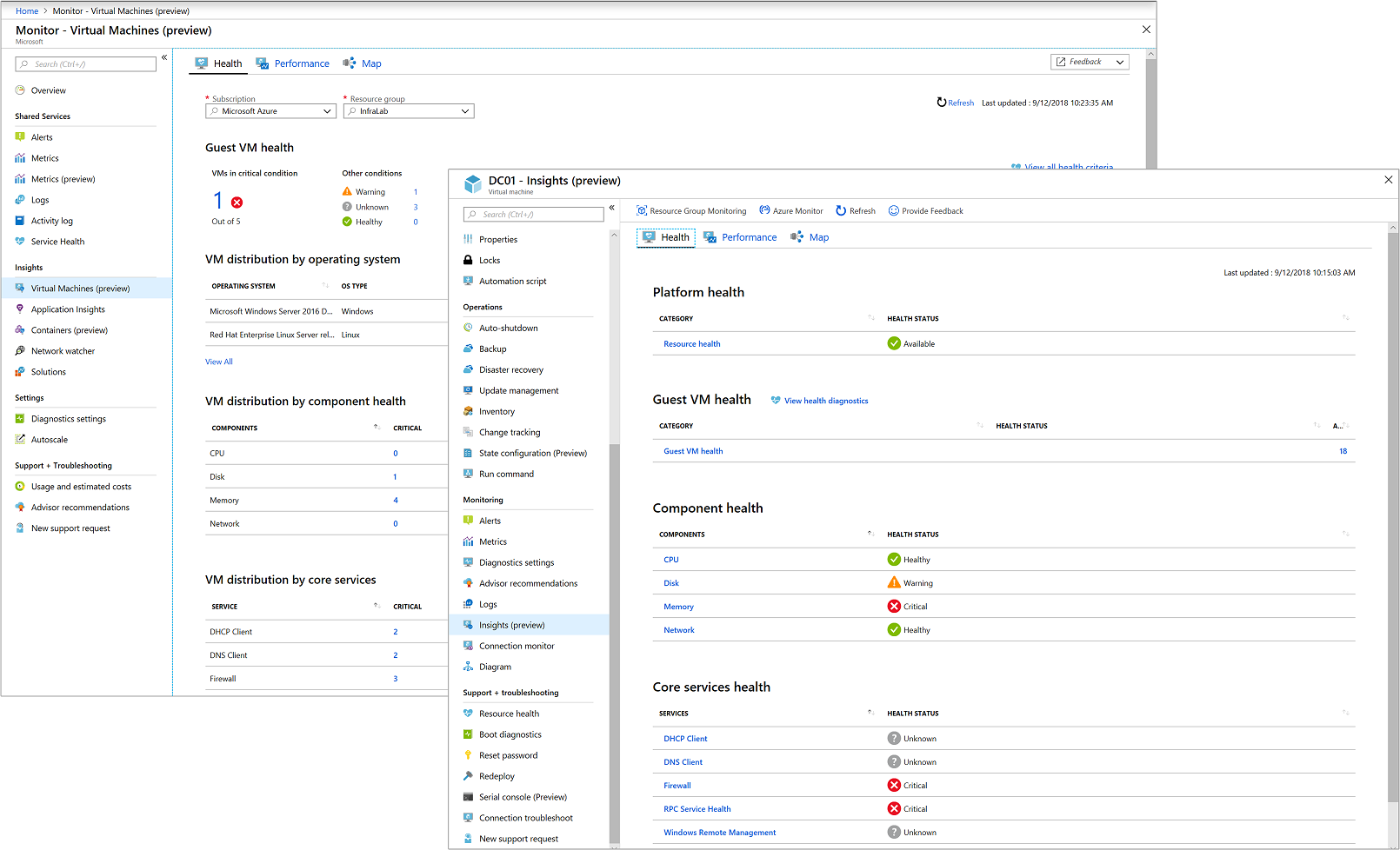
**Container insights**

[Container insights](https://docs.microsoft.com/en-us/azure/azure-monitor/containers/container-insights-overview) monitors the performance of container workloads that are deployed to managed Kubernetes clusters hosted on Azure Kubernetes Service (AKS). It gives you performance visibility by collecting 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.



**VM insights**

[VM insights](https://docs.microsoft.com/en-us/azure/azure-monitor/vm/vminsights-overview) monitors your Azure virtual machines (VM) at scale. It analyzes the performance and health of your Windows and Linux VMs and identifies their different processes and interconnected dependencies on external processes. The solution includes support for monitoring performance and application dependencies for VMs hosted on-premises or another cloud provider.



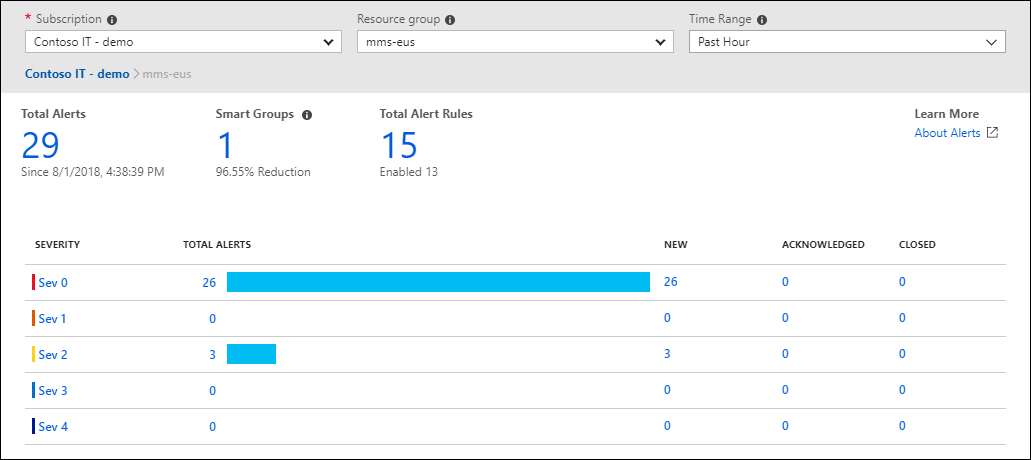
**Responding to critical situations**

In addition to allowing you to interactively analyze monitoring data, an effective monitoring solution must be able to proactively respond to critical conditions identified in the data that it collects. This could be sending a text or mail to an administrator responsible for investigating an issue. Or you could launch an automated process that attempts to correct an error condition.

**Alerts**

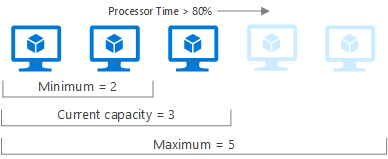
[Alerts in Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-overview) proactively notify you of critical conditions and potentially attempt to take corrective action. Alert rules based on metrics provide near real time alerts based on numeric values. Rules based on logs allow for complex logic across data from multiple sources.

Alert rules in Azure Monitor use [action groups](https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups), which contain unique sets of recipients and actions that can be shared across multiple rules. Based on your requirements, action groups can perform such actions as using webhooks to have alerts start external actions or to integrate with your ITSM tools.



**Autoscale**

Autoscale allows you to have the right amount of resources running to handle the load on your application. Create rules that use metrics collected by Azure Monitor to determine when to automatically add resources when load increases. Save money by removing resources that are sitting idle. You specify a minimum and maximum number of instances and the logic for when to increase or decrease resources.

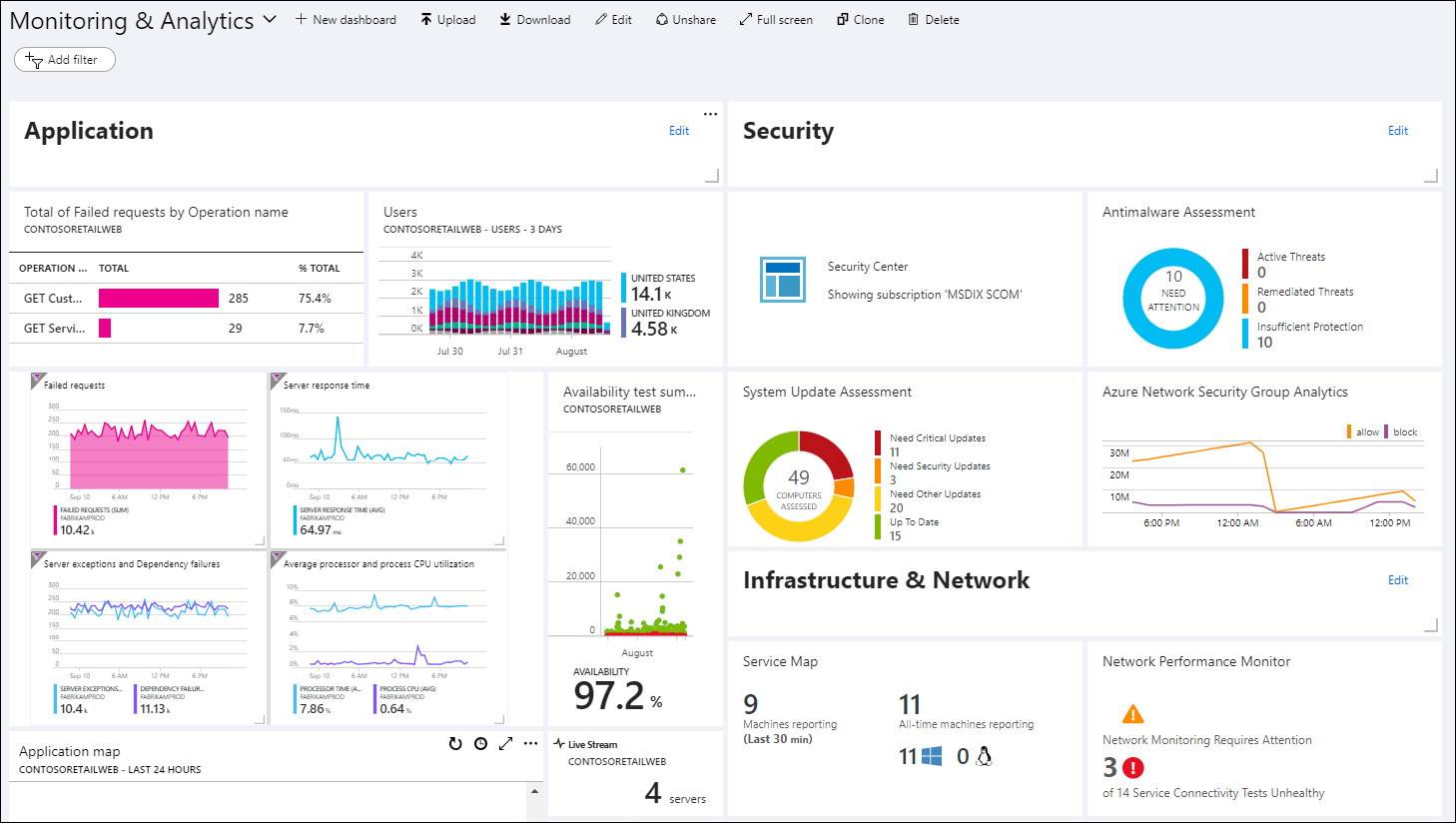


**Visualizing monitoring data**

[Visualizations](https://docs.microsoft.com/en-us/azure/azure-monitor/best-practices-analysis) 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](https://docs.microsoft.com/en-us/azure/azure-portal/azure-portal-dashboards) allow you to combine different kinds of data into a single pane in the [Azure portal](https://portal.azure.com/). You can optionally share the dashboard with other Azure users. Add the output of any log query or metrics chart to an Azure dashboard. 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.



**Workbooks**

[Workbooks](https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview) provide a flexible canvas for data analysis and the creation of rich visual reports in the Azure portal. They allow you to tap into multiple data sources from across Azure, and combine them into unified interactive experiences. Use workbooks provided with Insights or create your own from predefined templates.

