Azure Monitor overview

01/26/2019 • 9 minutes to read • +1

In this article

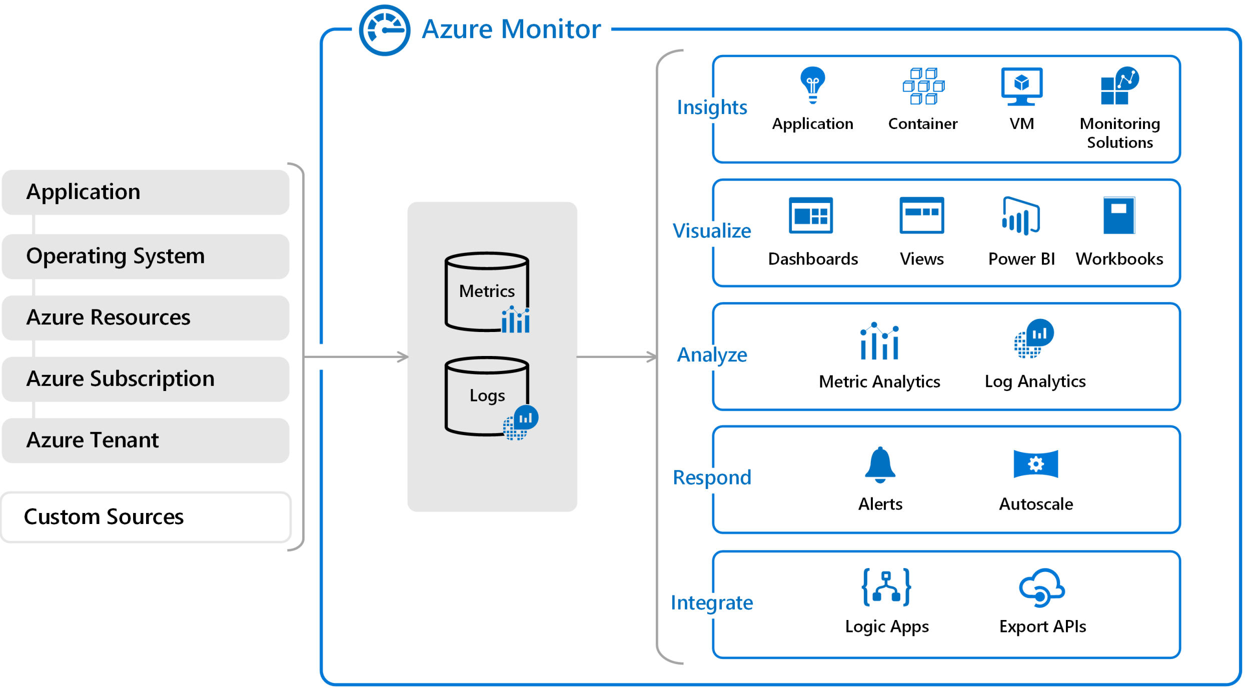
Azure Monitor maximizes the availability and performance of your applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies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

Introducing Azure Monitor

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.

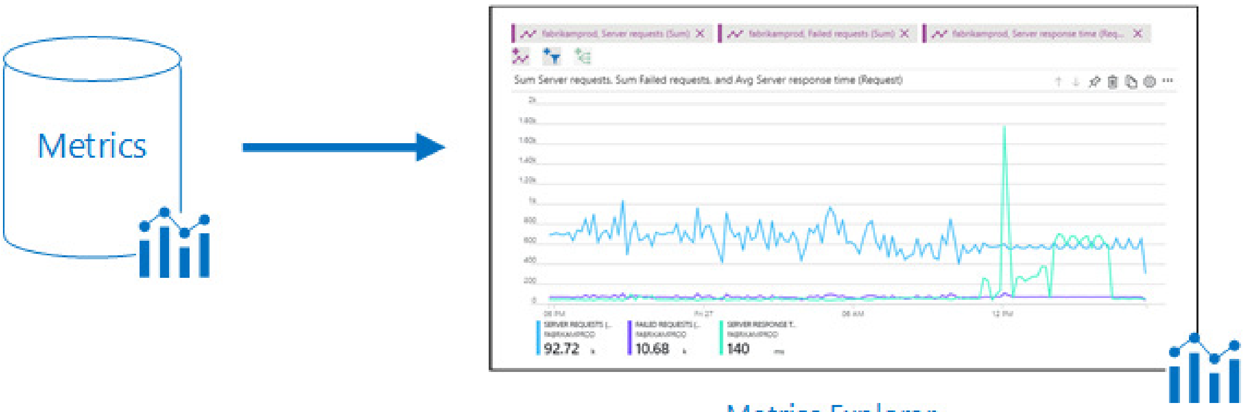
> ⓘ Note
>
> This article was recently updated to use the term Azure Monitor logs instead of Log Analytics. Log data is still stored in a Log Analytics workspace and is still collected and analyzed by the same Log Analytics service. We are updating the terminology to better reflect the role of logs in Azure Monitor. See Azure Monitor terminology changes for details.



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.

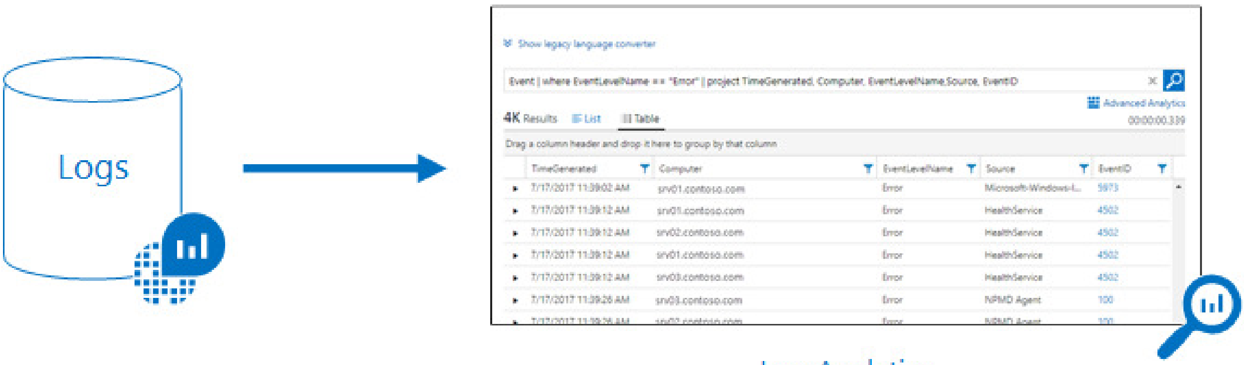
For many Azure resources, you'll see data collected by Azure Monitor right in their Overview page in the Azure portal. Have a look at any virtual machine for example, and you'll see several charts displaying performance metrics. Click on any of the graphs to open the data in metrics explorer in the Azure 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.


Metrics
fabrikamprod, Server requests (Sum)
fabrikamprod, Failed requests (Sum)
fabrikamprod, Server response time (Req...
Sum Server requests, Sum Failed requests, and Avg Server response time (Request)
2k
1.80k
1.60k
1.40k
1.20k
1k
800
600
400
200
0
06 PM
Fri 27
06 AM
12 PM
SERVER REQUESTS (...
FABRIKAMPROD
92.72
FAILED REQUESTS (...
FABRIKAMPROD
10.68
SERVER RESPONSE T...
FABRIKAMPROD
140
ms

Metrics Explorer

Log data collected by Azure Monitor can be analyzed with [queries](https://) to quickly retrieve, consolidate, and analyze collected data. You can create and test queries using [Log Analytics](https://) in the Azure portal and then either directly analyze the data using these tools or save queries for use with [visualizations](https://) or [alert rules](https://).

Azure Monitor uses a version of the [Kusto query language](https://) used by Azure Data Explorer 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://). Particular guidance is provided to users who are already familiar with [SQL](https://) and [Splunk](https://).


Logs
Show legacy language converter
Advanced Analytics
4K Results
List
Table
00:00:00.339
Drag a column header and drop it here to group by that column

```
Event | where EventLevelName == "Error" | project TimeGenerated, Computer, EventLevelName,Source, EventID
```

TimeGenerated	Computer	EventLevelName	Source	EventID
7/17/2017 11:39:02 AM	srv01.contoso.com	Error	Microsoft-Windows-I...	5973
7/17/2017 11:39:12 AM	srv01.contoso.com	Error	HealthService	4502
7/17/2017 11:39:12 AM	srv02.contoso.com	Error	HealthService	4502
7/17/2017 11:39:12 AM	srv01.contoso.com	Error	HealthService	4502
7/17/2017 11:39:12 AM	srv03.contoso.com	Error	HealthService	4502
7/17/2017 11:39:26 AM	srv03.contoso.com	Error	NPMD Agent	100
7/17/2017 11:39:26 AM	srv02.contoso.com	Error	NPMD Agent	100

Log 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.

Custom sources

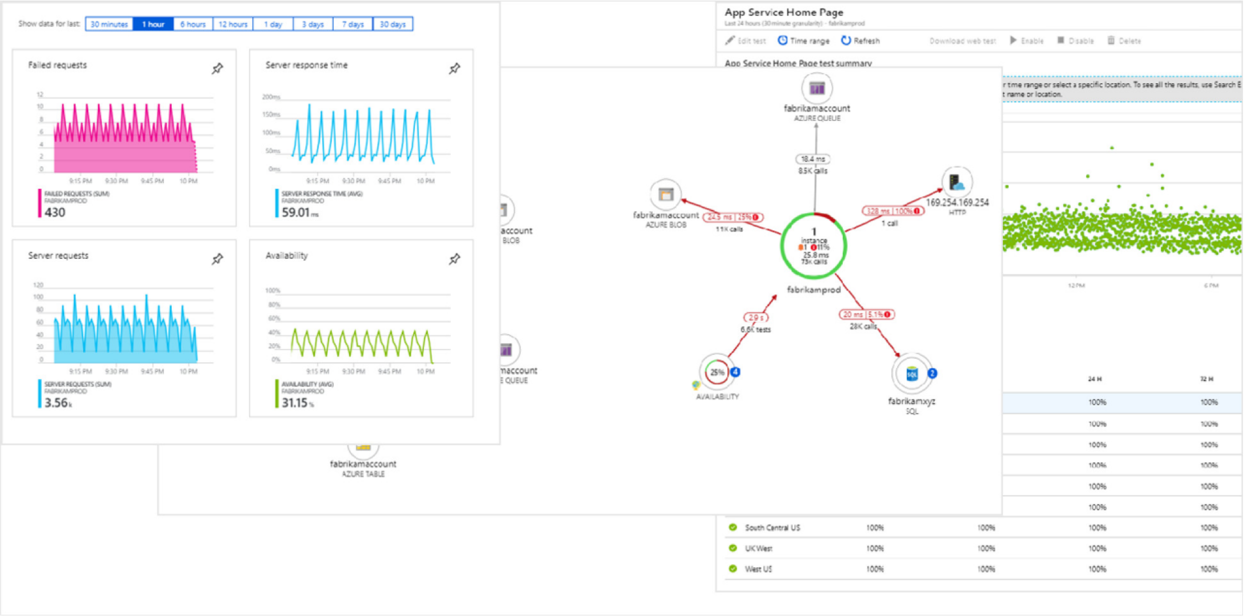
Azure Monitor can collect log data from any REST client using the Data Collector API. This allows you to create custom monitoring scenarios and extend monitoring to resources that don't expose telemetry through other sources.

Insights

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.

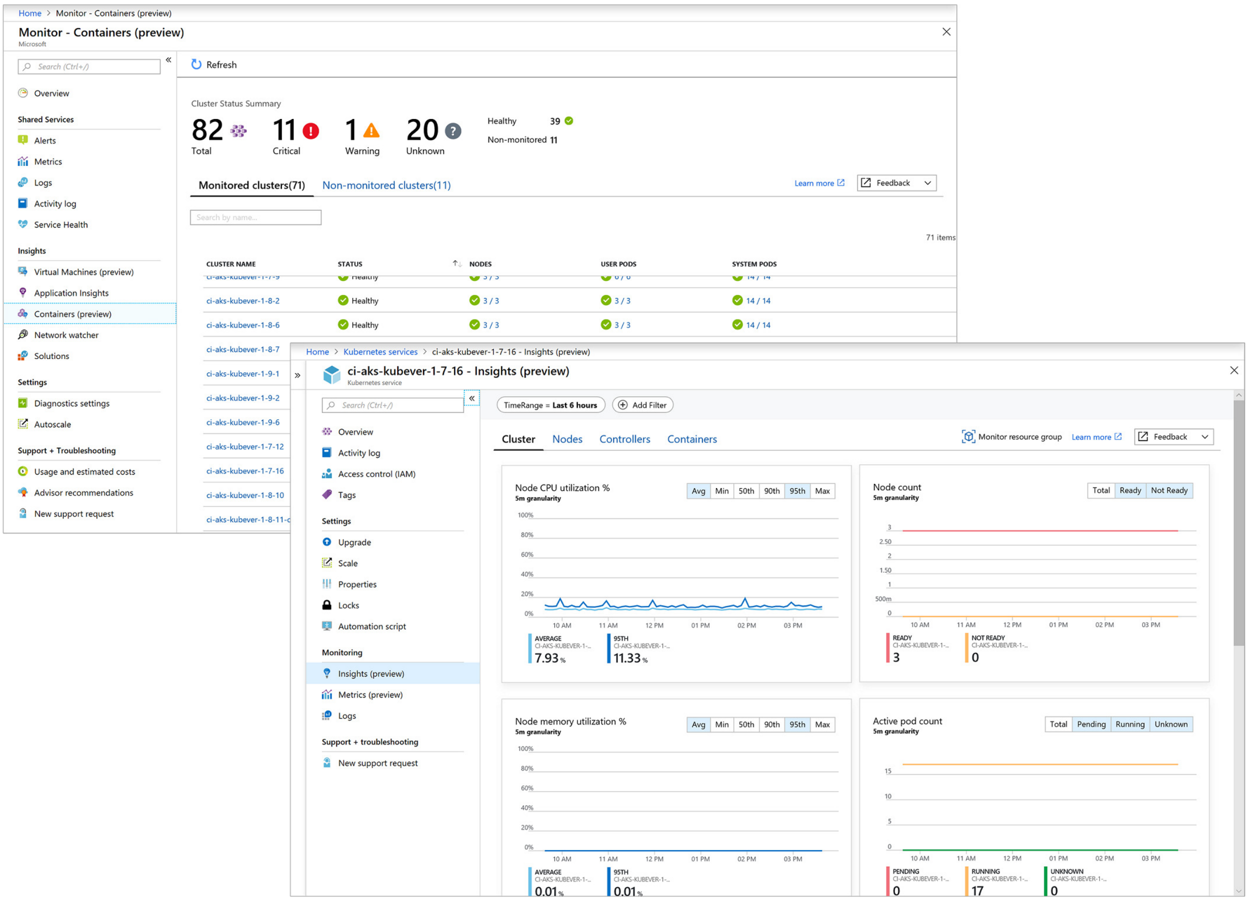
Application Insights

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.



Cluster Status Summary

82 Total · 11 Critical · 1 Warning · 20 Unknown

Healthy 39

Non-monitored 11

71 items

CLUSTER NAME	STATUS	NODES	USER PODS	SYSTEM PODS
ci-aks-kubever-1-7-9	✓ Healthy	✓ 3 / 3	✓ 6 / 6	✓ 14 / 14
ci-aks-kubever-1-8-2	✓ Healthy	✓ 3 / 3	✓ 3 / 3	✓ 14 / 14
ci-aks-kubever-1-8-6	✓ Healthy	✓ 3 / 3	✓ 3 / 3	✓ 14 / 14
ci-aks-kubever-1-8-7				
ci-aks-kubever-1-9-1				
ci-aks-kubever-1-9-2				
ci-aks-kubever-1-9-6				
ci-aks-kubever-1-7-12				
ci-aks-kubever-1-7-16				
ci-aks-kubever-1-8-10				
ci-aks-kubever-1-8-11-c				

TimeRange = **Last 6 hours**

Node CPU utilization %: AVERAGE CI-AKS-KUBEVER-1-... 7.93 % · 95TH CI-AKS-KUBEVER-1-... 11.33 %

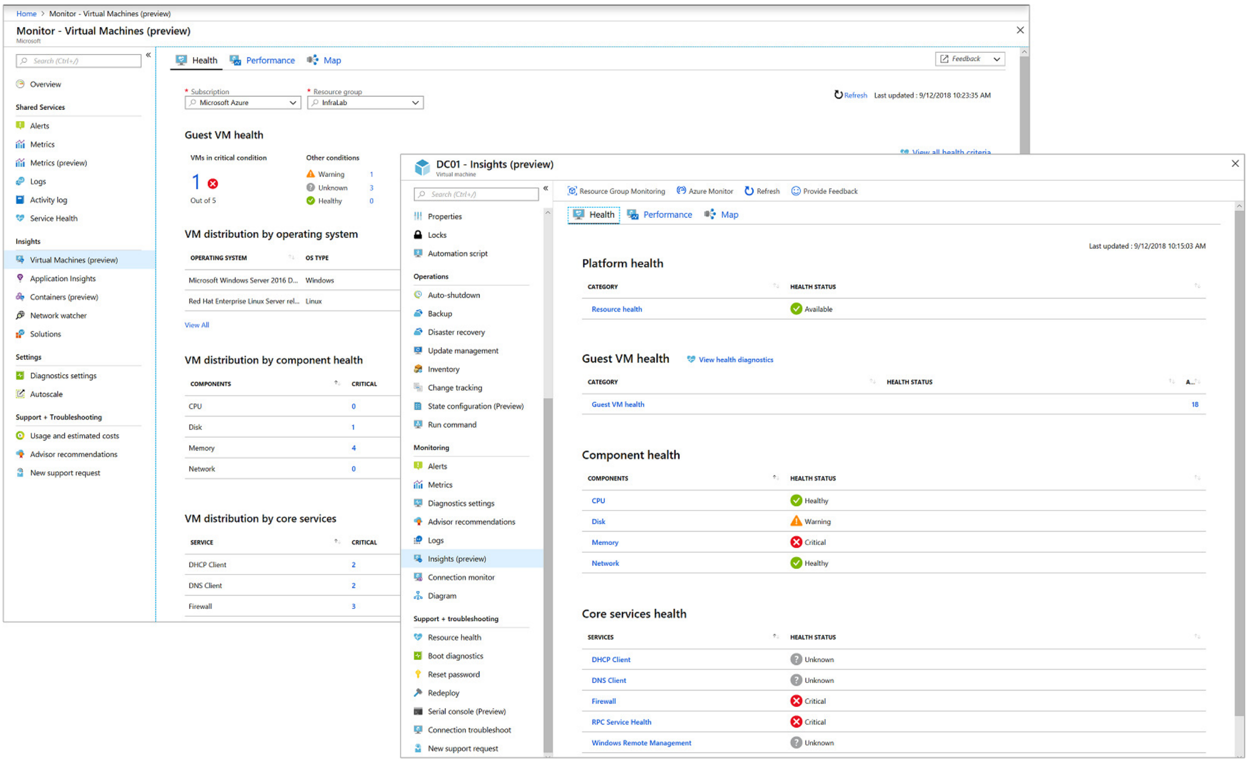
Node count: READY CI-AKS-KUBEVER-1-... 3 · NOT READY CI-AKS-KUBEVER-1-... 0

Node memory utilization %: AVERAGE CI-AKS-KUBEVER-1-... 0.01 % · 95TH CI-AKS-KUBEVER-1-... 0.01 %

Active pod count: PENDING CI-AKS-KUBEVER-1-... 0 · RUNNING CI-AKS-KUBEVER-1-... 17 · UNKNOWN CI-AKS-KUBEVER-1-... 0

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.



* Subscription: Microsoft Azure

* Resource group: InfraLab

Last updated : 9/12/2018 10:23:35 AM

Guest VM health

VMs in critical condition: 1 ✖ Out of 5

Other conditions:

Warning	1
Unknown	3
Healthy	0

VM distribution by operating system

OPERATING SYSTEM	OS TYPE
Microsoft Windows Server 2016 D...	Windows
Red Hat Enterprise Linux Server rel...	Linux

VM distribution by component health

COMPONENTS	CRITICAL
CPU	0
Disk	1
Memory	4
Network	0

VM distribution by core services

SERVICE	CRITICAL
DHCP Client	2
DNS Client	2
Firewall	3

Last updated : 9/12/2018 10:15:03 AM

Platform health

CATEGORY	HEALTH STATUS
Resource health	✓ Available

Guest VM health

CATEGORY	HEALTH STATUS	A...
Guest VM health		18

Component health

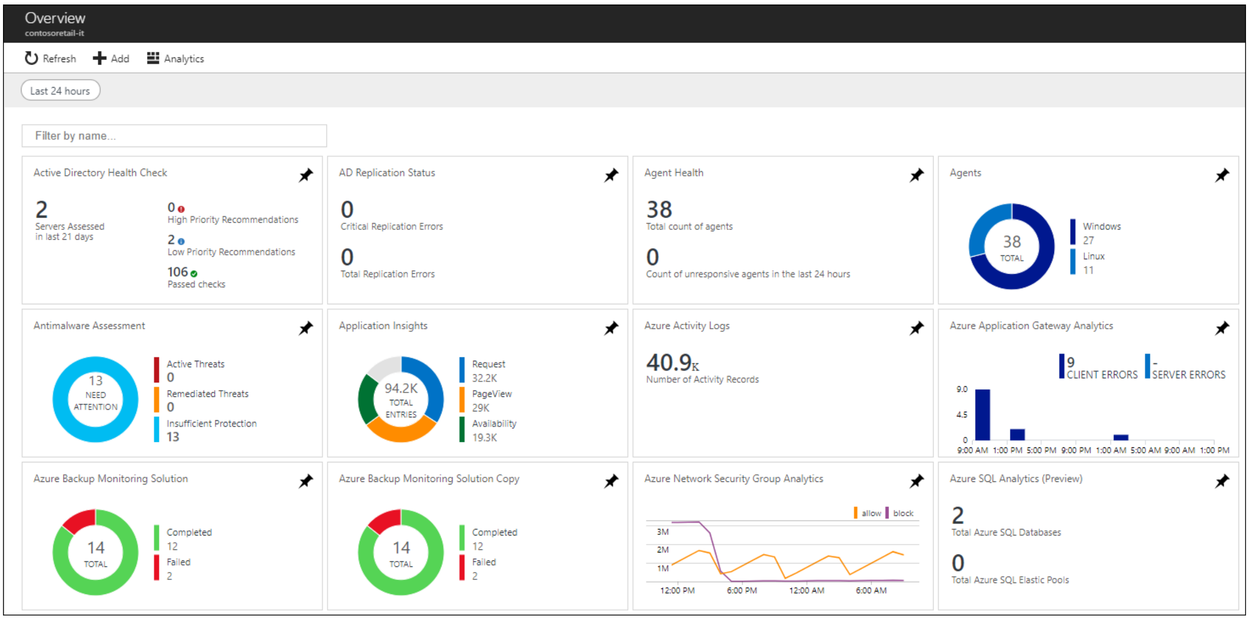
COMPONENTS	HEALTH STATUS
CPU	✓ Healthy
Disk	⚠ Warning
Memory	✖ Critical
Network	✓ Healthy

Core services health

SERVICES	HEALTH STATUS
DHCP Client	? Unknown
DNS Client	? Unknown
Firewall	✖ Critical
RPC Service Health	✖ Critical
Windows Remote Management	? Unknown

Monitoring solutions

Monitoring solutions in Azure Monitor are packaged sets of logic that provide insights for 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.



Active Directory Health Check: 2 Servers Assessed in last 21 days; 0 High Priority Recommendations; 2 Low Priority Recommendations; 106 Passed checks

AD Replication Status: 0 Critical Replication Errors; 0 Total Replication Errors

Agent Health: 38 Total count of agents; 0 Count of unresponsive agents in the last 24 hours

Azure Activity Logs: 40.9K Number of Activity Records

Azure SQL Analytics (Preview): 2 Total Azure SQL Databases; 0 Total Azure SQL Elastic Pools

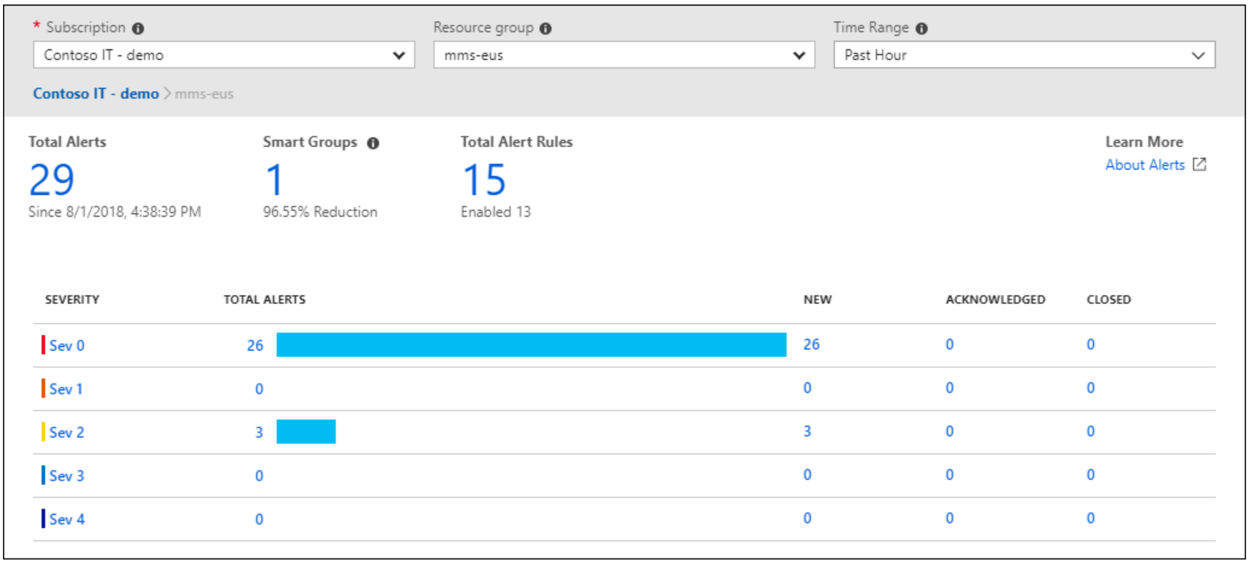
Responding to critical situations

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 proactively notify you of critical conditions and potentially attempt to take corrective action. Alert rules based on metrics provide near real time alerting based on numeric values, while rules based on logs allow for complex logic across data from multiple sources.

Alert rules in Azure Monitor use 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.



* Subscription: Contoso IT - demo

Resource group: mms-eus

Time Range: Past Hour

Contoso IT - demo > mms-eus

Total Alerts: 29 (Since 8/1/2018, 4:38:39 PM)

Smart Groups: 1 (96.55% Reduction)

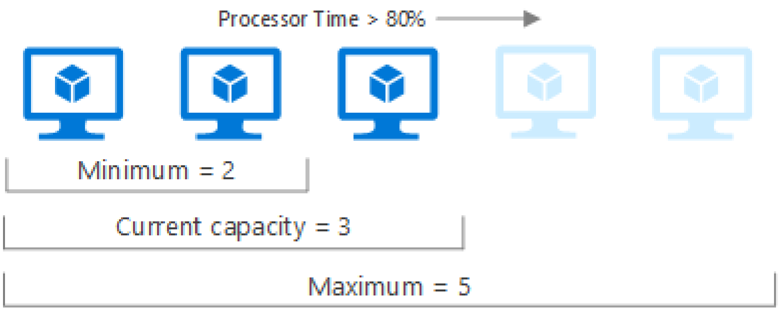
Total Alert Rules: 15 (Enabled 13)

Learn More: About Alerts

SEVERITY	TOTAL ALERTS	NEW	ACKNOWLEDGED	CLOSED
Sev 0	26	26	0	0
Sev 1	0	0	0	0
Sev 2	3	3	0	0
Sev 3	0	0	0	0
Sev 4	0	0	0	0

Autoscale

Autoscale allows you to have the right amount of resources running to handle the load on your application. It allows you to create rules that use metrics collected by Azure Monitor to determine when to automatically add resources to handle increases in load and also 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.

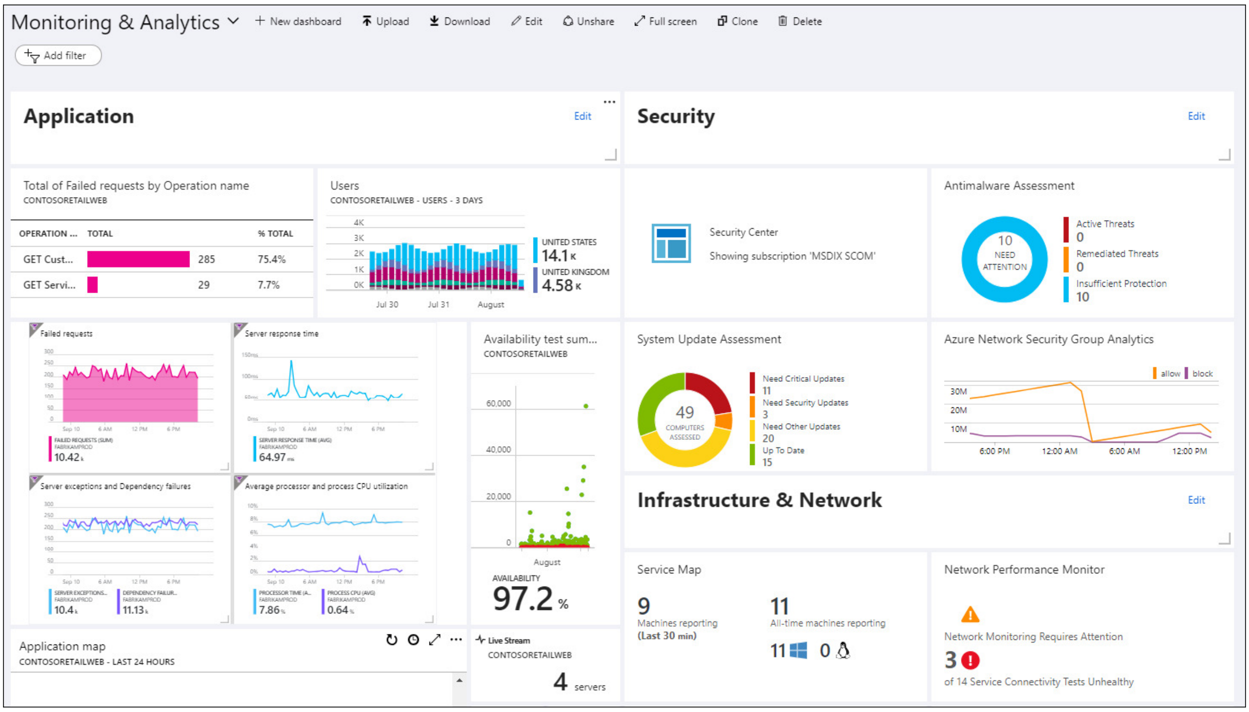


Visualizing monitoring data

Visualizations 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.

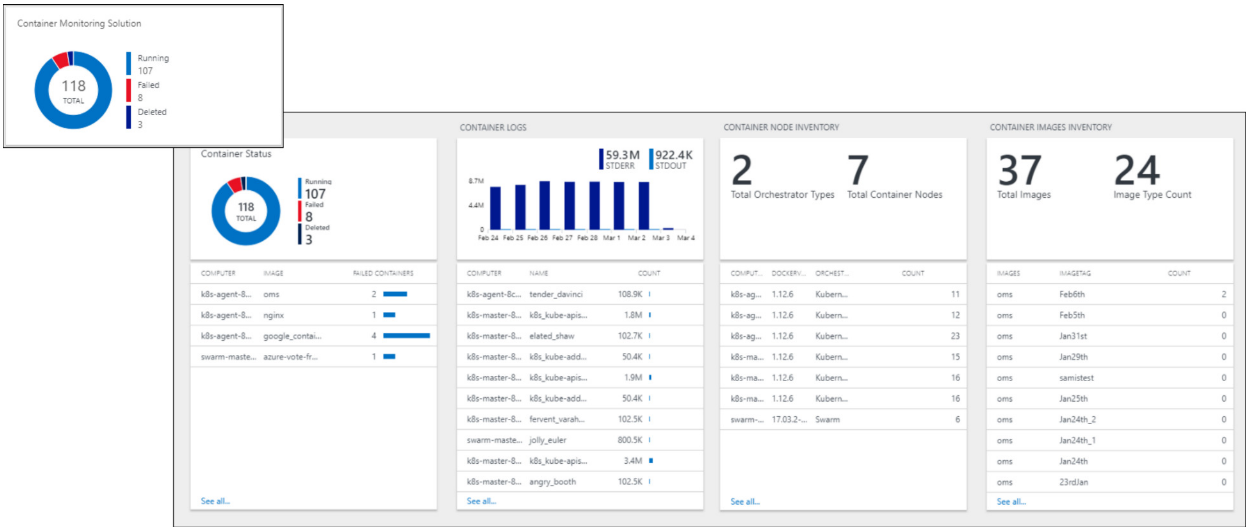
Dashboards

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.



Views

Views visually present log data in Azure Monitor. Each view includes a single tile that drills down to a combination of visualizations such as bar and line charts in addition to lists summarizing critical data. Monitoring solutions include views that summarize data for a particular application, and you can create your own views to present data from any log query. Like other elements in Azure Monitor, views can be added to Azure dashboards.



COMPUTER	IMAGE	FAILED CONTAINERS
k8s-agent-8...	oms	2
k8s-agent-8...	nginx	1
k8s-agent-8...	google_contai...	4
swarm-maste...	azure-vote-fr...	1

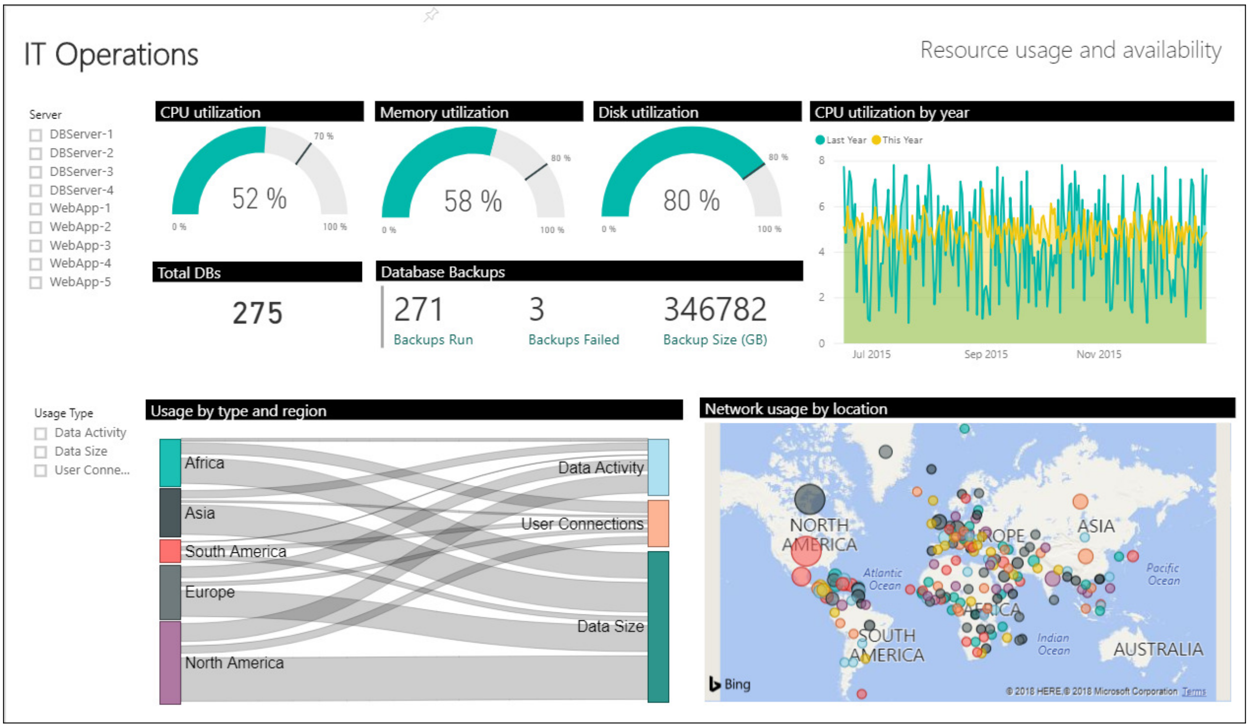
COMPUTER	NAME	COUNT
k8s-agent-8c...	tender_davinci	108.9K
k8s-master-8...	k8s_kube-apis...	1.8M
k8s-master-8...	elated_shaw	102.7K
k8s-master-8...	k8s_kube-add...	50.4K
k8s-master-8...	k8s_kube-apis...	1.9M
k8s-master-8...	k8s_kube-add...	50.4K
k8s-master-8...	fervent_varah...	102.5K
swarm-maste...	jolly_euler	800.5K
k8s-master-8...	k8s_kube-apis...	3.4M
k8s-master-8...	angry_booth	102.5K

COMPUT...	DOCKERV...	ORCHEST...	COUNT
k8s-ag...	1.12.6	Kubern...	11
k8s-ag...	1.12.6	Kubern...	12
k8s-ag...	1.12.6	Kubern...	23
k8s-ma...	1.12.6	Kubern...	15
k8s-ma...	1.12.6	Kubern...	16
k8s-ma...	1.12.6	Kubern...	16
swarm-...	17.03.2-...	Swarm	6

IMAGES	IMAGETAG	COUNT
oms	Feb6th	2
oms	Feb5th	0
oms	Jan31st	0
oms	Jan29th	0
oms	samistest	0
oms	Jan25th	0
oms	Jan24th_2	0
oms	Jan24th_1	0
oms	Jan24th	0
oms	23rdJan	0

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.

Next steps

Learn more about:

- Metrics and logs for the data collected by Azure Monitor.
- Data sources for how the different components of your application send telemetry.
- Log queries for analyzing collected data.