

Create a Memory Alert for Virtual machines Configure Alerts/thresholds /Action groups on the resources Database monitoring

This article is part of the guide Monitor virtual machines and their workloads in Azure Monitor. Alerts in Azure Monitor proactively notify you of interesting data and patterns in your monitoring data. There are no preconfigured alert rules for virtual machines, but you can create your own based on data you collect from Azure Monitor Agent. This article presents alerting concepts specific to virtual machines and common alert rules used by other Azure Monitor customers.

This scenario describes how to implement complete monitoring of your Azure and hybrid virtual machine environment:

- To get started monitoring your first Azure virtual machine, see Monitor Azure virtual machines.
- To quickly enable a recommended set of alerts, see Enable recommended alert rules for an Azure virtual machine.

Data collection

Alert rules inspect data that's already been collected in Azure Monitor. You need to ensure that data is being collected for a particular scenario before you can create an alert rule. See Monitor virtual machines with Azure Monitor: Collect data for guidance on configuring data collection for various scenarios, including all the alert rules in this article.

Recommended alert rules

Azure Monitor provides a set of recommended alert rules that you can quickly enable for any Azure virtual machine. These rules are a great starting point for basic monitoring. But alone, they won't provide sufficient alerting for most enterprise implementations for the following reasons:

- Recommended alerts only apply to Azure virtual machines and not hybrid machines.
- Recommended alerts only include host metrics and not guest metrics or logs. These metrics are useful to monitor the health of the machine itself. But they give you minimal visibility into the workloads and applications running on the machine.

- Recommended alerts are associated with individual machines that create an excessive number of alert rules. Instead of relying on this method for each machine, see [Scaling alert rules](#) for strategies on using a minimal number of alert rules for multiple machines.

Alert types

The most common types of alert rules in Azure Monitor are metric alerts and log search alerts. The type of alert rule that you create for a particular scenario depends on where the data that you're alerting on is located.

You might have cases where data for a particular alerting scenario is available in both Metrics and Logs. If so, you need to determine which rule type to use. You might also have flexibility in how you collect certain data and let your decision of alert rule type drive your decision for data collection method.

Metric alerts

Common uses for metric alerts:

- Alert when a particular metric exceeds a threshold. An example is when the CPU of a machine is running high.

Data sources for metric alerts:

- Host metrics for Azure virtual machines, which are collected automatically
- Metrics collected by Azure Monitor Agent from the guest operating system

Log search alerts

Common uses for log search alerts:

- Alert when a particular event or pattern of events from Windows event log or Syslog are found. These alert rules typically measure table rows returned from the query.
- Alert based on a calculation of numeric data across multiple machines. These alert rules typically measure the calculation of a numeric column in the query results.

Data sources for log search alerts:

- All data collected in a Log Analytics workspace

Scaling alert rules

Because you might have many virtual machines that require the same monitoring, you don't want to have to create individual alert rules for each one. You also want to ensure there are different strategies to limit the number of alert rules you need to manage, depending on the type of rule. Each of these strategies depends on understanding the target resource of the alert rule.

Metric alert rules

Virtual machines support multiple resource metric alert rules as described in Monitor multiple resources. This capability allows you to create a single metric alert rule that applies to all virtual machines in a resource group or subscription within the same region.

Start with the recommended alerts and create a corresponding rule for each by using your subscription or a resource group as the target resource. You need to create duplicate rules for each region if you have machines in multiple regions.

As you identify requirements for more metric alert rules, follow this same strategy by using a subscription or resource group as the target resource to:

- Minimize the number of alert rules you need to manage.
- Ensure that they're automatically applied to any new machines.

Log search alert rules

If you set the target resource of a log search alert rule to a specific machine, queries are limited to data associated with that machine, which gives you individual alerts for it. This arrangement requires a separate alert rule for each machine.

If you set the target resource of a log search alert rule to a Log Analytics workspace, you have access to all data in that workspace. For this reason, you can alert on data from all machines in the workgroup with a single rule. This arrangement gives you the option of creating a single alert for all machines. You can then use dimensions to create a separate alert for each machine.

For example, you might want to alert when an error event is created in the Windows event log by any machine. You first need to create a data collection rule as described in Collect events and performance counters from virtual machines with Azure Monitor Agent to send these events to the Event table in the Log Analytics workspace. Then you create an alert rule that queries this table by using the workspace as the target resource and the condition shown in the following image.

The query returns a record for any error messages on any machine. Use the **Split by dimensions** option and specify **_Resourceid** to instruct the rule to create an alert for each machine if multiple machines are returned in the results.

Home > Monitor | Logs >

Create an alert rule

Scope Condition Actions Details Tags Review + create

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Define the logic for triggering an alert. Use the chart to view trends in the data. [Learn more](#)

Log query

The query to run on this resource's logs. The results returned by this query are used to populate the alert definition below.

Search query *

```
Event
| where EventLog == "Application"
| where Source == "my-application"
| where EventLog == "Error"
```

[View result and edit query in Logs](#)

Measurement

Select how to summarize the results. We try to detect summarized data from the query results automatically.

Measure Table rows

Aggregation type Count

Aggregation granularity 5 minutes

Split by dimensions

Resource ID column _Resourceid

Use dimensions to monitor specific time series and provide context to the fired alert. Dimensions can be either number or string columns. If you select more than one dimension value, each time series that results from the combination will trigger its own alert and will be charged separately.

Dimension name	Operator	Dimension values	Include all future values
----------------	----------	------------------	---------------------------

Review + create

Previous

Next: Actions >

Dimensions

Depending on the information you want to include in the alert, you might need to split by using different dimensions. In this case, make sure the necessary dimensions are projected in the query by using the project or extend operator. Set the **Resource ID**

column field to **Don't split** and include all the meaningful dimensions in the list. Make sure **Include all future values** is selected so that any value returned from the query is included.

Split by dimensions

Resource ID column ⓘ

Don't split ▼

Use dimensions to monitor specific time series and provide context to the fired alert. Dimensions can be either number or string columns. If you select more than one dimension value, each time series that results from the combination will trigger its own alert and will be charged separately. ⓘ

Dimension name	Operator	Dimension values	Include all future values	
Computer	=	0 selected	<input checked="" type="checkbox"/>	
memorySizeMB	=	0 selected	<input checked="" type="checkbox"/>	
freePercentage	=	0 selected	<input checked="" type="checkbox"/>	
percThreshold	=	0 selected	<input checked="" type="checkbox"/>	
freeMb	=	0 selected	<input checked="" type="checkbox"/>	
<div>mbThreshold ▼</div>	<div>= ▼</div>	<div>0 selected ▼</div>	<input checked="" type="checkbox"/>	

Add custom value

Dynamic thresholds

Another benefit of using log search alert rules is the ability to include complex logic in the query for determining the threshold value. You can hardcode the threshold, apply it to all resources, or calculate it dynamically based on some field or calculated value. The threshold is applied to resources only according to specific conditions. For example, you might create an alert based on available memory but only for machines with a particular amount of total memory.

Common alert rules

The following section lists common alert rules for virtual machines in Azure Monitor. Details for metric alerts and log search alerts are provided for each. For guidance on which type of alert to use, see Alert types. If you're unfamiliar with the process for creating alert rules in Azure Monitor, see the instructions to create a new alert rule.

Dynamic thresholds

Another benefit of using log search alert rules is the ability to include complex logic in the query for determining the threshold value. You can hardcode the threshold, apply it

to all resources, or calculate it dynamically based on some field or calculated value. The threshold is applied to resources only according to specific conditions. For example, you might create an alert based on available memory but only for machines with a particular amount of total memory.

Common alert rules

The following section lists common alert rules for virtual machines in Azure Monitor. Details for metric alerts and log search alerts are provided for each. For guidance on which type of alert to use, see [Alert types](#). If you're unfamiliar with the process for creating alert rules in Azure Monitor, see the [instructions to create a new alert rule](#).

Target	Metric
Host	Percentage CPU (included in recommended alerts)
Windows guest	\Processor Information(_Total)% Processor Time
Linux guest	cpu/usage_active

Log search alert rules

CPU utilization

```
InsightsMetrics | where Origin == "vm.azm.ms" | where Namespace == "Processor" and Name == "UtilizationPercentage" | summarize CPUPercentageAverage = avg(Val) by bin(TimeGenerated, 15m), Computer, _ResourceId
```

Memory alerts

This section describes memory alerts.

Metric alert rules

Expand table

Target	Metric
Host	Available Memory Bytes (preview) (included in recommended alerts)
Windows guest	\Memory% Committed Bytes in Use \Memory\Available Bytes
Linux guest	mem/available mem/available_percent

Log search alert rules

Available memory in MB

InsightsMetrics | where Origin == "vm.azm.ms" | where Namespace == "Memory" and Name == "AvailableMB" | summarize AvailableMemoryInMBAverage = avg(Val) by bin(TimeGenerated, 15m), Computer, _ResourceId

Available memory in percentage

InsightsMetrics | where Origin == "vm.azm.ms" | where Namespace == "Memory" and Name == "AvailableMB" | extend TotalMemory = toreal(todynamic(Tags)["vm.azm.ms/memorySizeMB"]) | extend AvailableMemoryPercentage = (toreal(Val) / TotalMemory) * 100.0 | summarize AvailableMemoryInPercentageAverage = avg(AvailableMemoryPercentage) by bin(TimeGenerated, 15m), Computer, _ResourceId

Disk alerts

This section describes disk alerts.

Metric alert rules

Target	Metric
Windows guest	\Logical Disk(_Total)% Free Space \Logical Disk(_Total)\Free Megabytes
Linux guest	disk/free disk/free_percent

Log search alert rules

Logical disk used - all disks on each computer

InsightsMetrics | where Origin == "vm.azm.ms" | where Namespace == "LogicalDisk" and Name == "FreeSpacePercentage" | summarize LogicalDiskSpacePercentageFreeAverage = avg(Val) by bin(TimeGenerated, 15m), Computer, _ResourceId

Logical disk used - individual disks

InsightsMetrics | where Origin == "vm.azm.ms" | where Namespace == "LogicalDisk" and Name == "FreeSpacePercentage" | extend Disk=tostring(todynamic(Tags)["vm.azm.ms/mountId"]) | summarize LogicalDiskSpacePercentageFreeAverage = avg(Val) by bin(TimeGenerated, 15m), Computer, _ResourceId, Disk

Logical disk IOPS

InsightsMetrics | where Origin == "vm.azm.ms" | where Namespace == "LogicalDisk" and Name == "TransfersPerSecond" | extend Disk=tostring(todynamic(Tags)["vm.azm.ms/mountId"]) | summarize DiskIOPSAverage = avg(Val) by bin(TimeGenerated, 15m), Computer, _ResourceId, Disk

Logical disk data rate

InsightsMetrics | where Origin == "vm.azm.ms" | where Namespace == "LogicalDisk" and Name == "BytesPerSecond" | extend Disk=tostring(todynamic(Tags)["vm.azm.ms/mountId"]) | summarize DiskBytesPerSecondAverage = avg(Val) by bin(TimeGenerated, 15m), Computer, _ResourceId, Disk

Network alerts

Metric alert rules

Target	Metric
Host	Network In Total, Network Out Total (included in recommended alerts)
Windows guest	\Network Interface\Bytes Sent/sec \Logical Disk(_Total)\Free Megabytes
Linux guest	disk/free disk/free_percent

Log search alert rules

Network interfaces bytes received - all interfaces

```
InsightsMetrics | where Origin == "vm.azm.ms" | where Namespace == "Network" and Name == "ReadBytesPerSecond" | summarize BytesReceivedAverage = avg(Val) by bin(TimeGenerated, 15m), Computer, _ResourceId
```

Network interfaces bytes received - individual interfaces

```
InsightsMetrics | where Origin == "vm.azm.ms" | where Namespace == "Network" and Name == "ReadBytesPerSecond" | extend  
NetworkInterface=tostring(todynamic(Tags)["vm.azm.ms/networkDeviceId"]) | summarize  
BytesReceivedAverage = avg(Val) by bin(TimeGenerated, 15m), Computer, _ResourceId,  
NetworkInterface
```

Network interfaces bytes sent - all interfaces

```
InsightsMetrics | where Origin == "vm.azm.ms" | where Namespace == "Network" and Name == "WriteBytesPerSecond" | summarize BytesSentAverage = avg(Val) by bin(TimeGenerated, 15m),  
Computer, _ResourceId
```

Network interfaces bytes sent - individual interfaces

```
InsightsMetrics | where Origin == "vm.azm.ms" | where Namespace == "Network" and Name == "WriteBytesPerSecond" | extend  
NetworkInterface=tostring(todynamic(Tags)["vm.azm.ms/networkDeviceId"]) | summarize
```

BytesSentAverage = avg(Val) by bin(TimeGenerated, 15m), Computer, _ResourceId, NetworkInterface

Windows and Linux events

The following sample creates an alert when a specific Windows event is created. It uses a metric measurement alert rule to create a separate alert for each computer.

- **Create an alert rule on a specific Windows event.** This example shows an event in the Application log. Specify a threshold of 0 and consecutive breaches greater than 0.
 - KustoCopy
 - Event | where EventLog == "Application" | where EventID == 123 | summarize NumberOfEvents = count() by Computer, bin(TimeGenerated, 15m)
- **Create an alert rule on Syslog events with a particular severity.** The following example shows error authorization events. Specify a threshold of 0 and consecutive breaches greater than 0.
 - KustoCopy
 - Syslog | where Facility == "auth" | where SeverityLevel == "err" | summarize NumberOfEvents = count() by Computer, bin(TimeGenerated, 15m)

Custom performance counters

- **Create an alert on the maximum value of a counter.**
 - Perf | where CounterName == "My Counter" | summarize AggregatedValue = max(CounterValue) by Computer
- **Create an alert on the average value of a counter.**
 - Perf | where CounterName == "My Counter" | summarize AggregatedValue = avg(CounterValue) by Computer