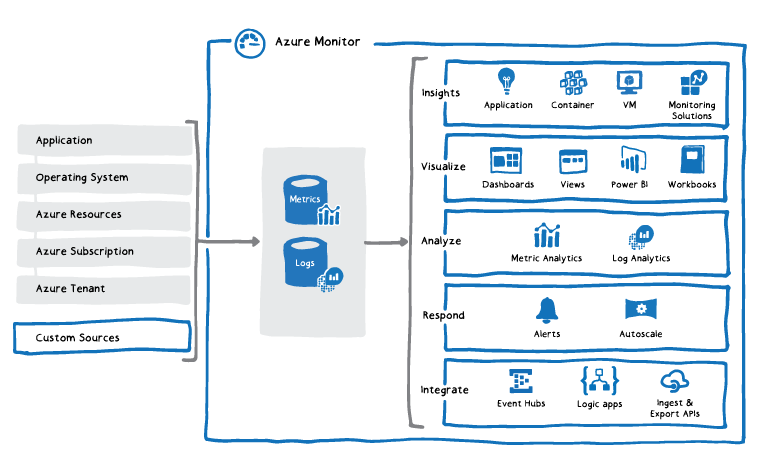
***Introducing Azure Monitoring Services***

*Monitoring is the act of collecting and analyzing data to determine the performance, health, and availability of your business application and the resources that it depends on. An effective monitoring strategy helps you understand the detailed operation of the components of your application. It also helps you increase your uptime by proactively notifying you of critical issues so that you can resolve them before they become problems.*

*Azure includes multiple services that individually perform a specific role or task in the monitoring space. Together, these services deliver a comprehensive solution for collecting, analyzing, and acting on telemetry from your application and the Azure resources that support them. They can also work to monitor critical on-premises resources to provide a hybrid monitoring environment. Understanding the tools and data that are available is the first step in developing a complete*monitoring strategy for your application.

The next 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.



Azure Monitor Documentation- <https://docs.microsoft.com/en-us/azure/azure-monitor/>

### Overview of Azure Monitor

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.

For more information, you can see: Monitoring Azure applications and resources - <https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview>

#### 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 Metric 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 is stored in Log Analytics which includes a rich query language to quickly retrieve, consolidate, and analyze collected data. You can create and test queries using the Log Analytics page 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 Data Explorer query language 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. Particular guidance is provided to users who are already familiar with SQL and Splunk.

#### 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.

Add an instrumentation package to your 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 Container Insights 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.

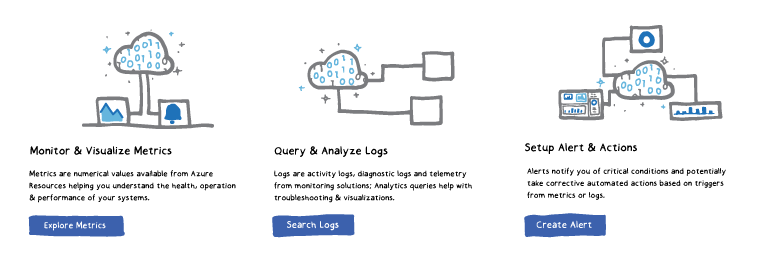
### *Azure Monitor: Key Capabilities*

*Azure Monitor enables core monitoring for Azure services by allowing the collection of metrics, activity logs, and diagnostic logs. For example, the activity log tells you when new resources are created or modified.*

*Metrics are available that provide performance statistics for different resources and even the operating system inside a virtual machine. You can view this data with one of the explorers in the Azure portal and create alerts based on these metrics. Azure Monitor provides the fastest metrics pipeline (5 minute down to 1 minute), so you should use it for time critical alerts and notifications.*

*Azure Monitor provides three main capabilities.*

* ***Monitor and visualize metrics****. Metrics are numerical values available from Azure resources helping you understand the health, operation and performance of your system.*
* ***Query and analyze logs****. Logs are activity logs, diagnostic logs, and telemetry from monitoring solutions; analytics queries help with troubleshooting and visualizations.*
* ***Setup alerts and actions****. Alerts notify you of critical conditions and potentially take automated corrective actions based on triggers from metrics or logs.*



*You can also send these metrics and logs to Azure Log Analytics for trending and detailed analysis, or create additional alert rules to proactively notify you of critical issues as a result of that analysis.*

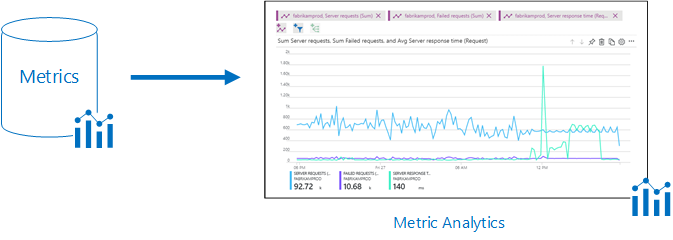
*For more information, see: Get started with Azure Monitor –*[*https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-get-started*](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-get-started)

### 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/platform/data-collection).

* **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.

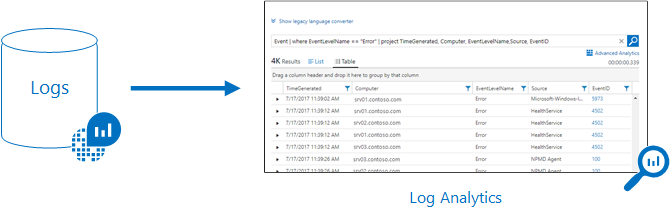
For many Azure resources, you'll see data collected by Azure Monitor right in their Overview page in the Azure portal. Have a look at any virtual machine for example, and you'll see several charts displaying performance metrics. Click on any of the graphs to open the data in Metric explorer in the Azure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

Log data collected by Azure Monitor is stored in Log Analytics which includes a [rich query language](https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview) to quickly retrieve, consolidate, and analyze collected data. You can create and test queries using the Log Analytics page 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 [Data Explorer](https://docs.microsoft.com/en-us/azure/kusto/query/) query language 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. Particular guidance is provided to users who are already familiar with SQL and Splunk.



### *Data Types*

*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 systems.*

*✔️ 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.*

*For more information, you can see:*

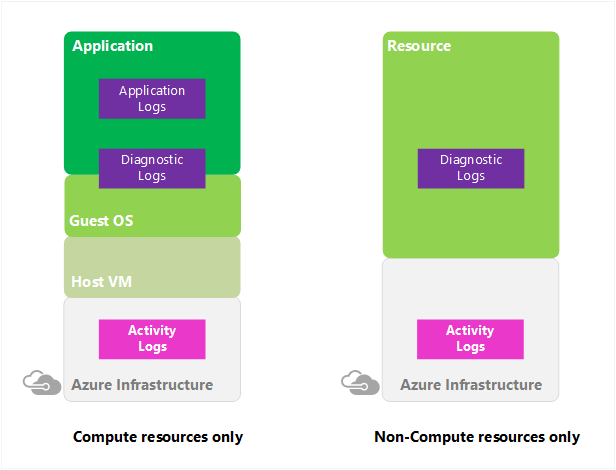
*Azure Fridays, Azure Monitor -*[*https://channel9.msdn.com/Shows/Azure-Friday/Azure-Monitor/player*](https://channel9.msdn.com/Shows/Azure-Friday/Azure-Monitor/player)

### *Activity Log*

*The Azure Activity Log is a subscription log that provides insight into subscription-level events that have occurred in Azure. This includes a range of data, from Azure Resource Manager operational data to updates on Service Health events.*

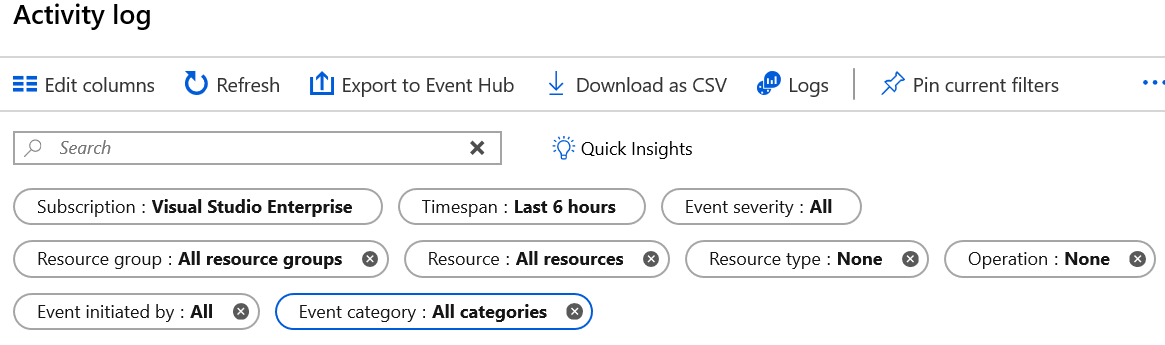
*With the Activity Log, you can determine the ‘what, who, and when’ for any write operations (PUT, POST, DELETE) taken on the resources in your subscription. You can also understand the status of the operation and other relevant properties. Through activity logs, you can determine:*

* *What operations were taken on the resources in your subscription.*
* *Who started the operation.*
* *When the operation occurred.*
* *The status of the operation.*
* *The values of other properties that might help you research the operation.*



*✔️ Activity logs are kept for 90 days. You can query for any range of dates, as long as the starting date isn't more than 90 days in the past. You can retrieve events from your Activity Log using the Azure portal, CLI, PowerShell cmdlets, and Azure Monitor REST API.*

### *Query the Activity Log*



*In the Azure portal, you can filter your Activity Log by these fields:*

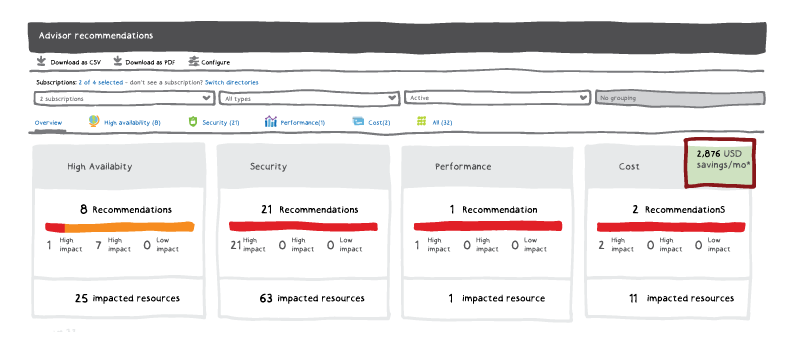
* ***Subscription****. One or more Azure subscription names.*
* ***Timespan****. The start and end time for events.*
* ***Event Severity****. The severity level of the event (Informational, Warning, Error, Critical).*
* ***Resource group****. One or more resource groups within those subscriptions.*
* ***Resource (name)****. The name of a specific resource.*
* ***Resource type****. The type of resource, for example, Microsoft.Compute/virtualmachines.*
* ***Operation name****. The name of an Azure Resource Manager operation, for example, Microsoft.SQL/servers/Write.*
* ***Event initiated by****. The ‘caller,’ or user who performed the operation.*
* ***Event Category****. The event category is described in the next topic.*
* ***Search****. This is an open text search box that searches for that string across all fields in all events.*

*✔️ Once you have defined a set of filters, you can pin the filtered state to the dashboard or download the search results as a CSV file.*

### *Azure Advisor*

*Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azure resources.*

*The Advisor cost recommendations page helps you optimize and reduce your overall Azure spend by identifying idle and underutilized resources.*



*Select the recommended action for a recommendation to implement the recommendation. A simple interface will open that enables you to implement the recommendation or refer you to documentation that assists you with implementation.*

*✔️ Advisor provides recommendations for virtual machines, availability sets, application gateways, App Services, SQL servers, and Redis Cache.*

*For more information, you can see:*

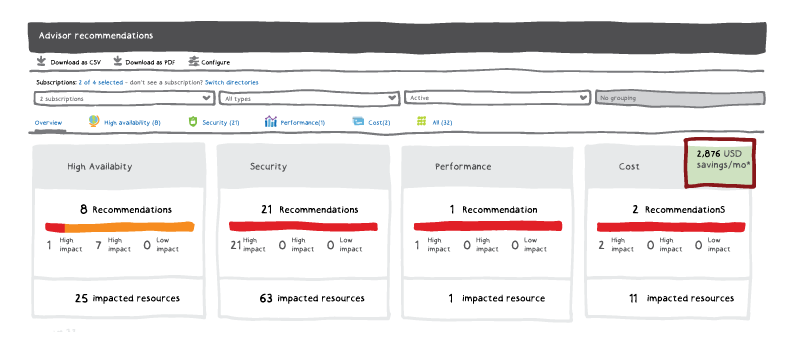
*Introduction to Azure Advisor -*[*https://docs.microsoft.com/en-us/azure/advisor/advisor-overview*](https://docs.microsoft.com/en-us/azure/advisor/advisor-overview)

*Advisor Cost recommendations -*[*https://docs.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations*](https://docs.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations)

### *Azure Advisor*

*Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azure resources.*

*The Advisor cost recommendations page helps you optimize and reduce your overall Azure spend by identifying idle and underutilized resources.*



*Select the recommended action for a recommendation to implement the recommendation. A simple interface will open that enables you to implement the recommendation or refer you to documentation that assists you with implementation.*

*✔️ Advisor provides recommendations for virtual machines, availability sets, application gateways, App Services, SQL servers, and Redis Cache.*

*For more information, you can see:*

*Introduction to Azure Advisor -*[*https://docs.microsoft.com/en-us/azure/advisor/advisor-overview*](https://docs.microsoft.com/en-us/azure/advisor/advisor-overview)

*Advisor Cost recommendations -*[*https://docs.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations*](https://docs.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations)

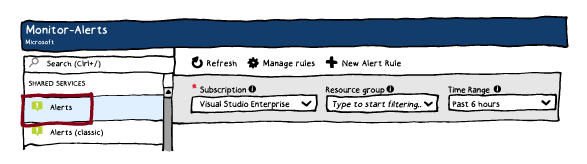
### *Event Categories*

*The Activity Log provides several event categories. You may select one or more.*

* ***Administrative****. This category contains the record of all create, update, delete, and action operations performed through Resource Manager. Examples of the types of events you would see in this category include “create virtual machine” and "delete network security group". The Administrative category also includes any changes to role-based access control in a subscription.*
* ***Service Health****. This category contains the record of any service health incidents that have occurred in Azure. An example of the type of event you would see in this category is “SQL Azure in East US is experiencing downtime.” Service health events come in five varieties: Action Required, Assisted Recovery, Incident, Maintenance, Information, or Security.*
* ***Alert****. This category contains the record of all activations of Azure alerts. An example of the type of event you would see in this category is “CPU % on myVM has been over 80 for the past 5 minutes.”*
* ***Autoscale****. This category contains the record of any events related to the operation of the autoscale engine based on any autoscale settings you have defined in your subscription. An example of the type of event you would see in this category is “Autoscale scale up action failed.”*
* ***Recommendation****. This category contains recommendation events from certain resource types, such as web sites and SQL servers. These events offer recommendations for how to better utilize your resources.*
* ***Security****. This category contains the record of any alerts generated by Azure Security Center. An example of the type of event you would see in this category is “Suspicious double extension file executed.”*
* ***Policy and Resource Health****. These categories do not contain any events; they are reserved for future use.*

### *Azure Monitor Alerts*

*Alerting is now available with Azure Monitor.*



*The Monitor Alerts experience has many benefits.*

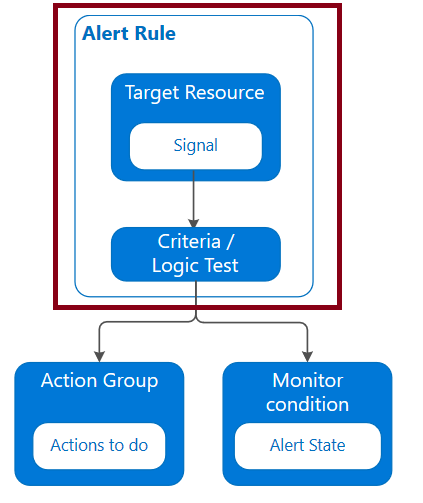
* ***Better notification system****. All newer alerts use action groups, which are named groups of notifications and actions that can be reused in multiple alerts.*
* ***A unified authoring experience****. All alert creation for metrics, logs and activity log across Azure Monitor, Log Analytics, and Application Insights is in one place.*
* ***View Log Analytics alerts in Azure portal****. You can now also see Log Analytics alerts in your subscription. Previously these were in a separate portal.*
* ***Separation of Fired Alerts and Alert Rules****. Alert Rules (the definition of the condition that triggers an alert), and Fired Alerts (an instance of the alert rule firing) are differentiated, so the operational and configuration views are separated.*
* ***Better workflow****. The new alerts authoring experience guides the user along the process of configuring an alert rule, which makes it simpler to discover the right things to get alerted on.*

*For more information, you can see:*

*The new alerts experience in Azure Monitor -*[*https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-unified-alerts*](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-unified-alerts)

### *Creating Alert Rules*

*Alerts proactively notify you when important conditions are found in your monitoring data. They allow you to identify and address issues before the users of your system notice them. Alerts consists of alert rules, action groups, and monitor conditions.*

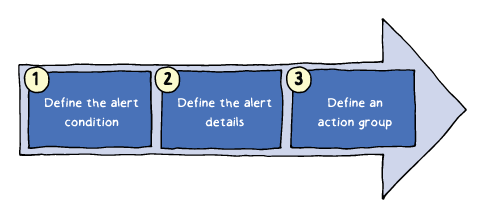


*Alert rules are separated from alerts and the actions that are taken when an alert fires. The alert rule captures the target and criteria for alerting. The alert rule can be in an enabled or a disabled state. Alerts only fire when enabled. The key attributes of an alert rule are:*

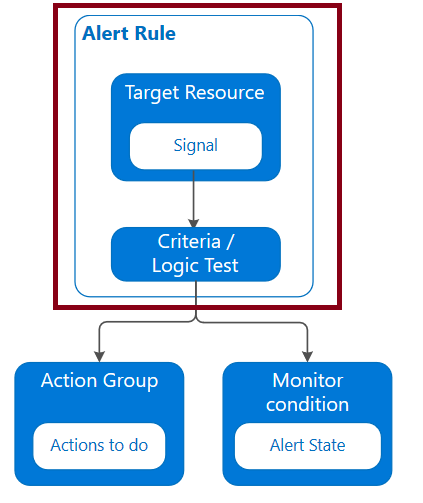
* ***Target Resource****– Defines the scope and signals available for alerting. A target can be any Azure resource. Example targets: a virtual machine, a storage account, a virtual machine scale set, a Log Analytics workspace, or an Application Insights resource. For certain resources (like Virtual Machines), you can specify multiple resources as the target of the alert rule.*
* ***Signal****– Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.*
* ***Criteria****– Criteria is a combination of Signal and Logic applied on a Target resource. Examples: + Percentage CPU > 70%; Server Response Time > 4 ms; and Result count of a log query > 100.*
* ***Alert Name****– A specific name for the alert rule configured by the user.*
* ***Alert Description****– A description for the alert rule configured by the user.*
* ***Severity****– The severity of the alert once the criteria specified in the alert rule is met. Severity can range from 0 to 4.*
* ***Action****– A specific action taken when the alert is fired. See the Action Groups topic coming up.*

### *Alert Rules*

*Creating an alert is a three-step task: define the alert condition, define alert details, and define an action group.*



*Alerts proactively notify you when important conditions are found in your monitoring data. They allow you to identify and address issues before the users of your system notice them. Alerts consists of alert rules, action groups, and monitor conditions.*



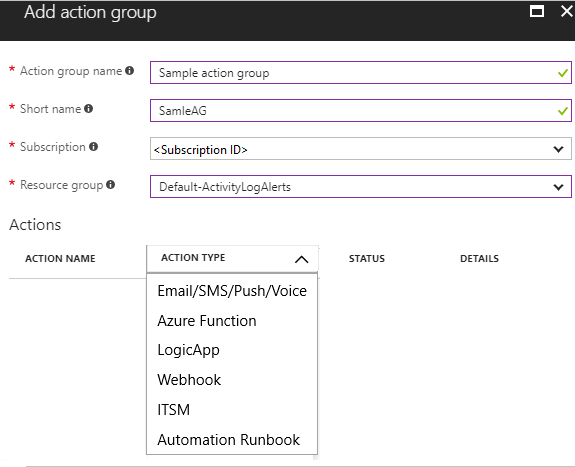
*Alert rules are separated from alerts and the actions that are taken when an alert fires. The alert rule captures the target and criteria for alerting. The alert rule can be in an enabled or a disabled state. Alerts only fire when enabled. The key attributes of an alert rule are:*

* ***Target Resource****– Defines the scope and signals available for alerting. A target can be any Azure resource. Example targets: a virtual machine, a storage account, a virtual machine scale set, a Log Analytics workspace, or an Application Insights resource. For certain resources (like Virtual Machines), you can specify multiple resources as the target of the alert rule.*
* ***Signal****– Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.*
* ***Criteria****– Criteria is a combination of Signal and Logic applied on a Target resource. Examples: + Percentage CPU > 70%; Server Response Time > 4 ms; and Result count of a log query > 100.*
* ***Alert Name****– A specific name for the alert rule configured by the user.*
* ***Alert Description****– A description for the alert rule configured by the user.*
* ***Severity****– The severity of the alert once the criteria specified in the alert rule is met. Severity can range from 0 to 4.*
* ***Action****– A specific action taken when the alert is fired. See the Action Groups topic coming up.*

### *Action Groups*

*An action group is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor and Service Health alerts use action groups to notify users that an alert has been triggered. Various alerts may use the same action group or different action groups depending on the user's requirements.*

*When an action is configured to notify a person by email or SMS the person will receive a confirmation indicating he / she has been added to the action group.*



* ***Email****– Emails will be sent to the email addresses. Ensure that your email filtering is configured appropriately. You may have up to 1000 email actions in an Action Group.*
* ***ITSM****– You may have up to 10 ITSM actions in an Action Group ITSM Action requires an ITSM Connection.*
* ***Logic App****– You may have up to 10 Logic App actions in an Action Group.*
* ***Function App****– The function keys for Function Apps configured as actions are read through the Functions API.*
* ***Runbook****– You may have up to 10 Runbook actions in an Action Group.*
* ***SMS****– You may have up to 10 SMS actions in an Action Group.*
* ***Voice****– You may have up to 10 Voice actions in an Action Group.*
* ***Webhook****– You may have up to 10 Webhook actions in an Action Group. Retry logic - The timeout period for a response is 10 seconds. The webhook call will be retried a maximum of 2 times when the following HTTP status codes are returned: 408, 429, 503, 504 or the HTTP endpoint does not respond. The first retry happens after 10 seconds. The second and last retry happens after 100 seconds.*

*✔️ You may have up to 10 Azure app actions in an Action Group. At this time the Azure app action only supports ServiceHealth alerts.*

***Managing Alerts***

*You can alert on metrics and logs as described in monitoring data sources. These include but are not limited to:*

* *Metric values*
* *Log search queries*
* *Activity Log events*
* *Health of the underlying Azure platform*
* *Tests for web site availability*

***Alert states***

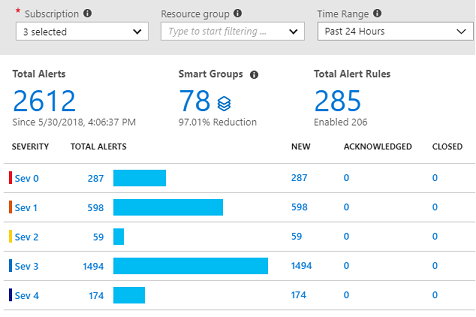
*You can set the state of an alert to specify where it is in the resolution process. When the criteria specified in the alert rule is met, an alert is created or fired, it has a status of****New****. You can change the status when you acknowledge an alert and when you close it. All state changes are stored in the history of the alert. The following alert states are supported.*

| ***State*** | ***Description*** |
| --- | --- |
| ***New*** | *The issue has just been detected and has not yet been reviewed.* |
| ***Acknowledged*** | *An administrator has reviewed the alert and started working on it.* |
| ***Closed*** | *The issue has been resolved. After an alert has been closed, you can reopen it by changing it to another state.* |

*✔️ Alert state is different and independent of the monitor condition. Alert state is set by the user. Monitor condition is set by the system. When an alert fires, the alert's monitor condition is set to fired. When the underlying condition that caused the alert to fire clears, the monitor condition is set to resolved. The alert state isn't changed until the user changes it.*

### *Alerts Experience*

*The default Alerts page provides a summary of alerts that are created within a particular time window. It displays the total alerts for each severity with columns that identify the total number of alerts in each state for each severity.*

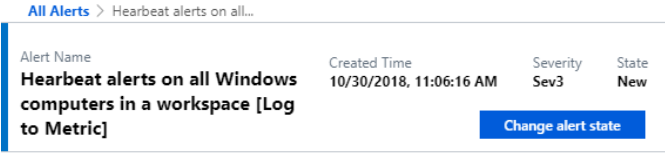


| ***Column*** | ***Description*** |
| --- | --- |
| *Subscription* | *Select up to five Azure subscriptions. Only alerts in the selected subscriptions are included in the view.* |
| *Resource group* | *Select a single resource group. Only alerts with targets in the selected resource group are included in the view.* |
| *Time range* | *Only alerts fired within the selected time window are included in the view. Supported values are the past hour, the past 24 hours, the past 7 days, and the past 30 days.* |

*✔️ You can select Total Alerts, Smart Groups, and Total Alert Rules to open a new page.*

### *Alert*Detail Page

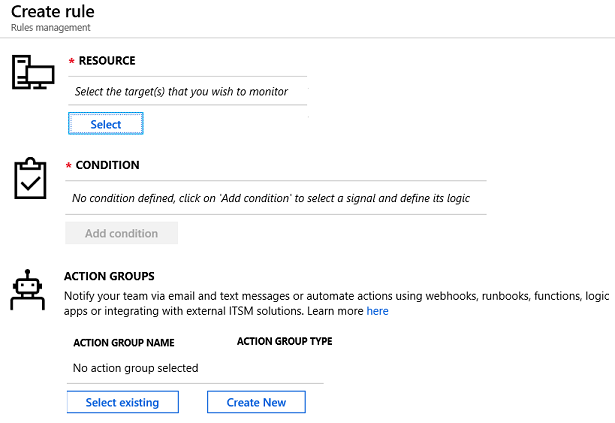
The Alert detail page is displayed when you select an alert. It provides details of the alert and enables you to change its state.



| **Section** | **Description** |
| --- | --- |
| Essentials | Displays the properties and other significant information about the alert. |
| History | Lists each action taken by the alert and any changes made to the alert. Currently limited to state changes. |
| Smart group | Information about the smart group the alert is included in. The alert count refers to the number of alerts that are included in the smart group. Includes other alerts in the same smart group that were created in the past 30 days regardless of the time filter in the alerts list page. Select an alert to view its detail. |
| More details | Displays further contextual information for the alert, which is typically specific to the type of source that created the alert. |

### *Create an Alert*

*Alerts can be authored in a consistent manner regardless of the monitoring service or signal type. All fired alerts and related details are available in single page. You create a new alert rule with the following three steps:*



* ***Resource****. Select the resource you want to monitor. For example, resource group, virtual machine, or storage account.*
* ***Condition****. Select the signal and define its logic. The signal could be All, Metrics, or Activity log.*
* ***Action Group****. Notify your team via email and text messages or automate actions using webhooks, runbooks, functions, logic apps or integrating with external ITSM solutions.*
* ***Alert rule name****. Specify a name to identify your alert.*
* ***Description****. Provide a description for your alert rule.*
* ***Enable rule upon creation****. You can enable and disable your alert rules.*

*✔️ We currently support configuring only two metrics signals or one log search signal or one activity log signal per alert rule. An alert will be triggered when the conditions for all the above configured criteria are met.*

***Demonstration - Alerts***

*In this demonstration, we will create an alert rule.*

***Create an alert rule***

1. *In Azure portal, click on****Monitor****. The Monitor blade consolidates all your monitoring settings and data in one view.*
2. *Click****Alerts****then click****+ New alert rule****. As most resource blades also have Alerts in their resource menu under Monitoring, you could create alerts from there as well.*

***Explore alert targets***

1. *Click****Select****under Target, to select a target resource that you want to alert on. Use****Subscription****and****Resource type****drop-downs to find the resource you want to monitor. You can also use the search bar to find your resource.*
2. *If the selected resource has metrics you can create alerts on, Available signals on the bottom right will include metrics. You can view the full list of resource types supported for metric alerts in this article.*
3. *Click****Done****when you have made your selection.*

***Explore alert conditions***

1. *Once you have selected a target resource, click on****Add condition****.*
2. *You will see a list of signals supported for the resource, select the metric you want to create an alert on.*
3. *Optionally, refine the metric by adjusting Period and Aggregation. If the metric has dimensions, you will see the Dimensions table presented.*
4. *You will see a chart for the metric for the last 6 hours. Adjust the****Show history****drop-down.*
5. *Define the****Alert logic****. This will determine the logic which the metric alert rule will evaluate.*
6. *If you are using a static threshold, the metric chart can help determine what might be a reasonable threshold. If you are using a Dynamic Thresholds, the metric chart will display the calculated thresholds based on recent data.*
7. *Click****Done****.*
8. *Optionally, add another criteria if you want to monitor a complex alert rule.*

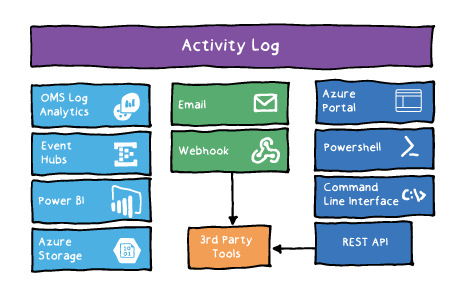
***Explore alert details***

1. *Fill in Alert details like****Alert Rule Name****,****Description****and****Severity****.*
2. *Add an action group to the alert either by selecting an existing action group or creating a new action group.*
3. *Click****Done****to save the metric alert rule.*

### *Overview of Activity Log*

*The Azure Activity Log is a subscription log that provides insight into subscription-level events that have occurred in Azure. This includes a range of data, from Azure Resource Manager operational data to updates on Service Health events. The Activity Log was previously known as “Audit Logs” or “Operational Logs”.*

*Using the Activity Log, you can determine the ‘what, who, and when’ for any write operation taken on the resources in your subscription. For example, who stopped a service. It provides an audit trail of the activities or operations performed on your resources by someone working on the Azure platform. You can also understand the status of the operation and other relevant properties.*



*This diagram shows many of the things you can do with the activity log including:*

* *Send data to Log Analytics for advanced search and alerts*
* *Query or manage events in the Portal, PowerShell, CLI, and REST API*
* *Stream information to Event Hub*
* *Archive data to a storage account*
* *Analyze data with Power BI*

*✔️ The Activity Log differs from*[*Diagnostic Logs*](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-of-diagnostic-logs)*. Activity Logs provide data about the operations on a resource from the outside (the “control plane”). Diagnostics Logs are emitted by a resource and provide information about the operation of that resource (the "data plane").*

*For more information, you can see:*

*Monitor Subscription Activity with the Azure Activity Log -*[*https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs*](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs)

#### Categories in the Activity Log

*The Activity Log contains several categories of data. For full details on the schemata of these categories,*[*see this article*](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-schema)*. These include:*

* ***Administrative****- This category contains the record of all create, update, delete, and action operations performed through Resource Manager. Examples of the types of events you would see in this category include "create virtual machine" and "delete network security group" Every action taken by a user or application using Resource Manager is modeled as an operation on a particular resource type. If the operation type is Write, Delete, or Action, the records of both the start and success or fail of that operation are recorded in the Administrative category. The Administrative category also includes any changes to role-based access control in a subscription.*
* ***Service Health****- This category contains the record of any service health incidents that have occurred in Azure. An example of the type of event you would see in this category is "SQL Azure in East US is experiencing downtime." Service health events come in five varieties: Action Required, Assisted Recovery, Incident, Maintenance, Information, or Security, and only appear if you have a resource in the subscription that would be impacted by the event.*
* ***Resource Health****- This category contains the record of any resource health events that have occurred to your Azure resources. An example of the type of event you would see in this category is "Virtual Machine health status changed to unavailable." Resource health events can represent one of four health statuses: Available, Unavailable, Degraded, and Unknown. Additionally, resource health events can be categorized as being Platform Initiated or User Initiated.*
* ***Alert****- This category contains the record of all activations of Azure alerts. An example of the type of event you would see in this category is "CPU % on myVM has been over 80 for the past 5 minutes." A variety of Azure systems have an alerting concept -- you can define a rule of some sort and receive a notification when conditions match that rule. Each time a supported Azure alert type 'activates,' or the conditions are met to generate a notification, a record of the activation is also pushed to this category of the Activity Log.*
* ***Autoscale****- This category contains the record of any events related to the operation of the autoscale engine based on any autoscale settings you have defined in your subscription. An example of the type of event you would see in this category is "Autoscale scale up action failed." Using autoscale, you can automatically scale out or scale in the number of instances in a supported resource type based on time of day and/or load (metric) data using an autoscale setting. When the conditions are met to scale up or down, the start and succeeded or failed events are recorded in this category.*
* ***Recommendation****- This category contains recommendation events from Azure Advisor.*
* ***Security****- This category contains the record of any alerts generated by Azure Security Center. An example of the type of event you would see in this category is "Suspicious double extension file executed."*
* ***Policy****- This category does not contain any events; it is reserved for future use.*

### *Query the Activity Log in Azure*

#### Query the Activity Log in the Azure portal

*Within the Azure portal, you can view your Activity Log in several places:*

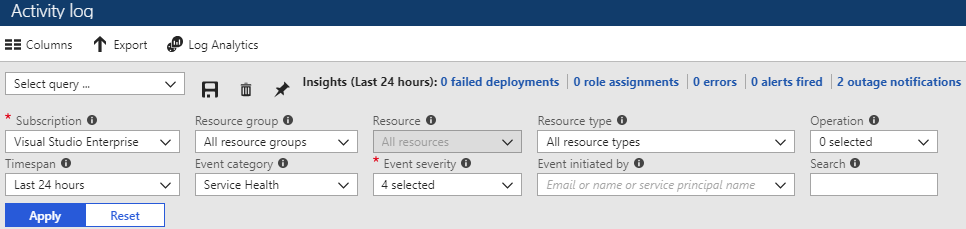
* *The****Activity Log****that you can access by searching for the Activity Log under****All services****in the left-hand navigation pane.*
* ***Monitor****appears by default in the left-hand navigation pane. The Activity Log is one section of Azure Monitor.*
* *Most****resources****, for example, the configuration blade for a Virtual Machine. The Activity Log is a section on most resource blades, and clicking on it automatically filters the events to those related to that specific resource.*

*In the Azure portal, you can filter your Activity Log by these fields:*

* *Timespan - The start and end time for events.*
* *Category - The event category as described above.*
* *Subscription - One or more Azure subscription names.*
* *Resource group - One or more resource groups within those subscriptions.*
* *Resource (name) - The name of a specific resource.*
* *Resource type - The type of resource, for example, Microsoft.Compute/virtualmachines.*
* *Operation name - The name of an Azure Resource Manager operation, for example, Microsoft.SQL/servers/Write.*
* *Severity - The severity level of the event (Informational, Warning, Error, Critical).*
* *Event initiated by - The 'caller,' or user who performed the operation.*
* *Open search - This is an open text search box that searches for that string across all fields in all events.*

*✔️ Once you have defined a set of filters, you can save it as a query that is persisted across sessions if you ever need to perform the same query with those filters applied again in the future. You can also pin a query to your Azure dashboard to always keep an eye on specific events.*

*For even more power, you can click the****Logs****icon, which displays your Activity Log data in the*[*Log Analytics Activity Log Analytics solution*](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/collect-activity-logs)*. The Activity Log blade offers a basic filter/browse experience on logs, but Log Analytics enables you to pivot, query, and visualize your data in more powerful ways.*



#### Export the Activity Log with a Log Profile

*A****Log Profile****controls how your Activity Log is exported. Using a Log Profile, you can configure:*

* *Where the Activity Log should be sent (Storage Account or Event Hubs)*
* *Which event categories (Write, Delete, Action) should be sent. The meaning of "category" in Log Profiles and Activity Log events is different. In the Log Profile, "Category" represents the operation type (Write, Delete, Action). In an Activity Log event, the "category" property represents the source or type of event (for example, Administration, ServiceHealth, Alert, and more).*
* *Which regions (locations) should be exported. Make sure to include "global," as many events in the Activity Log are global events.*
* *How long the Activity Log should be retained in a Storage Account.*
* *A retention of zero days means logs are kept forever. Otherwise, the value can be any number of days between 1 and 2147483647.*  
    
  *If retention policies are set but storing logs in a Storage Account is disabled (for example, if only Event Hubs or Log Analytics options are selected), the retention policies have no effect.*
* *Retention policies are applied per-day, so at the end of a day (UTC), logs from the day that is now beyond the retention policy are deleted. For example, if you had a retention policy of one day, at the beginning of the day today the logs from the day before yesterday would be deleted. The delete process begins at midnight UTC, but note that it can take up to 24 hours for the logs to be deleted from your storage account.*

*You can use a storage account or event hub namespace that is not in the same subscription as the one emitting logs. The user who configures the setting must have the appropriate RBAC access to both subscriptions.*

*For more information, you can see:****Query the Activity Log in the Azure portal****-*[*https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs#query-the-activity-log-in-the-azure-portal*](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs)

### *Log Analytics Scenarios*

*One of the challenges with any broad data analytics solution is figuring out where you’re going to see value for your organization. Out of all the things that are possible, what does your business need? What we hear from customers is that the following areas all have the potential to deliver significant business value:*

***Example 1 - Assessing updates***

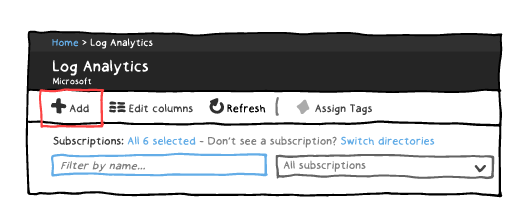
*An important part of the daily routine for any IT administrator is assessing systems update requirements and planning patches. Accurate scheduling is critical, as it directly relates to SLAs to the business and can seriously impact business functions. In the past, you had to schedule an update with only limited knowledge of how long the patching would take. Operations Management Suite collects data from all customers performing patches and uses that data to provide an average patching time for specific missing updates. This use of “crowd-sourced” data is unique to cloud systems, and is a great example of how Log Analytics can help meet strict SLAs.*

***Example 2 - Change tracking***

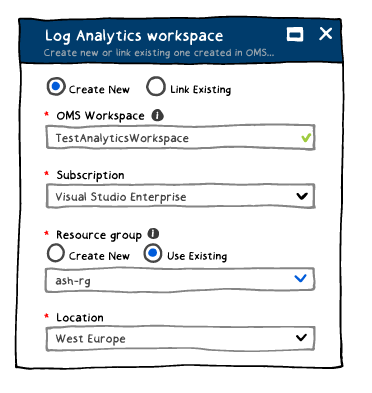
*Troubleshooting an operational incident is a complex process, requiring access to multiple data streams. With Operations Management Suite, you can easily perform analysis from multiple angles, using data from a wide variety of sources through a single interface for correlation of information. By tracking changes throughout the environment, Log Analytics helps to easily identify things like abnormal behavior from a specific account, users installing unapproved software, unexpected system reboots or shutdowns, evidence of security breaches, or specific problems in loosely coupled applications.*

### *Create a Workspace*

*To get started with Log Analytics you need to add a workspace. In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics.*



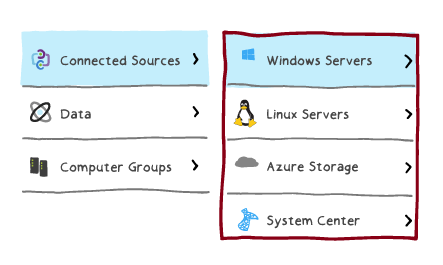
*You can them click Create and select your choices for the new workspace.*



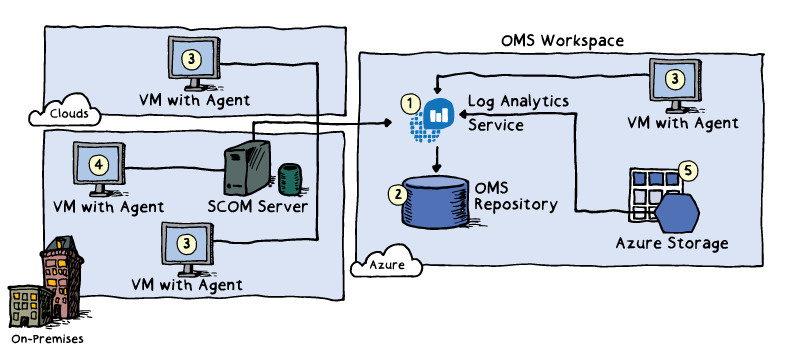
* *Provide a name for the new Log Analyics workspace, such as DefaultLAWorkspace.*
* *Select a Subscription from the drop-down list.*
* *For Resource Group, select an existing resource group that contains one or more Azure virtual machines.*
* *Select the Location your VMs are deployed to. See which regions*[*Log Analytics is available in*](https://azure.microsoft.com/regions/services/)*.*
* *The workspace will automatically use the Per GB pricing plan.*

### *Connected Sources*

*Connected sources are the computers and other resources that generate data collected by Log Analytics. This can include agents installed on*[*Windows*](https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-windows-agents)*and*[*Linux*](https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-linux-agents)*computers that connect directly or agents in a connected*[*System Center Operations Manager management group*](https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-om-agents)*. Log Analytics can also collect data from*[*Azure storage*](https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-azure-storage)*.*



*This following diagram shows how Connected Sources flow data to the Log Analytics service.*



*Ensure you can locate each of the following.*

* + *The Log Analytics service (1) collects data and stores it in the OMS repository (2). The OMS Repository is hosted in Azure. Connected Sources provide information to the Log Analytics service.*
  + *Computer agents (3) generate data to the Log Analytics service. These agents can run on Windows or Linux computers, virtual or physical computers, on-premises or cloud computers, and Azure or other cloud providers.*
  + *A System Center Operations Manager (SCOM) management group can be connected to Log Analytics. SCOM agents (4) communicate with management servers which forward events and performance data to Log Analytics.*
  + *An Azure storage account (5) can also collect Azure Diagnostics data from a worker role, web role, or virtual machine in Azure. This information can be sent to the Log Analytics service.*

*For more information, you can see:*

*Connecting Computers to the Log Analytics Service -*[*https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-windows-agents#system-requirements-and-required-configuration*](https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-windows-agents)