



Log Analytics Workspace

A Log Analytics Workspace in Azure is a central repository where you can collect, analyze, and visualize log and telemetry data from various sources such as Azure resources, applications, and on-premises environments. It provides powerful querying capabilities, advanced analytics, and integration with other Azure services for monitoring, troubleshooting, and gaining insights into your environment.

The primary functions and benefits of a Log Analytics Workspace include:

1. **Data Collection:** Log Analytics Workspace collects log and telemetry data from a wide range of sources, including Azure services, virtual machines, containers, and custom applications. It supports structured and unstructured data, making it versatile for different types of logs and metrics.
2. **Advanced Querying:** It offers a powerful query language, Kusto Query Language (KQL), which allows users to perform complex queries and analysis on log data. With KQL, users can filter, aggregate, and visualize data to gain insights into system behavior, troubleshoot issues, and identify trends.
3. **Visualization and Dashboards:** Log Analytics Workspace enables users to create custom dashboards and visualizations to monitor and analyze their data effectively. Users can create charts, graphs, and tables to visualize key metrics and trends, providing a centralized view of their environment's health and performance.
4. **Alerting and Automation:** Users can set up alerts based on predefined conditions or custom queries to notify them of critical events or anomalies in their environment. Alerts can be configured to trigger actions such as sending notifications, executing Azure Automation runbooks, or integrating with third-party services for automated remediation.
5. **Integration with Azure Monitor:** Log Analytics Workspace is tightly integrated with Azure Monitor, providing seamless access to monitoring data and insights. It enhances Azure Monitor's capabilities by offering advanced log analytics and correlation, enabling comprehensive monitoring and management of Azure resources and applications.
6. **Compliance and Security:** Log Analytics Workspace helps organizations meet compliance requirements by providing centralized logging and auditing capabilities. It enables users to track and analyze security events, detect suspicious activities, and ensure adherence to regulatory standards such as GDPR, HIPAA, and PCI DSS.



Use cases of Log Analytics Workspace:

Log Analytics Workspace in Azure can be applied across various use cases to collect, analyze, and act on log and telemetry data from diverse sources. Here are some common use cases:

1. **Operational Insights:** Organizations can use Log Analytics Workspace to gain operational insights into their Azure environment and on-premises infrastructure. By collecting and analyzing logs from servers, virtual machines, and applications, they can

identify performance bottlenecks, troubleshoot issues, and optimize resource utilization.

2. **Security Monitoring and Threat Detection:** Log Analytics Workspace helps enhance security posture by collecting and analyzing security logs from Azure resources, network appliances, and security solutions. Organizations can detect and investigate security incidents, identify malicious activities, and respond to threats in real-time.
3. **Compliance and Audit:** Log Analytics Workspace supports compliance efforts by centralizing log data and providing auditing capabilities. Organizations can track user activities, monitor access to sensitive data, and generate audit reports to demonstrate compliance with regulatory requirements such as GDPR, HIPAA, and PCI DSS.
4. **Application Monitoring and Troubleshooting:** Developers can leverage Log Analytics Workspace to monitor the performance and availability of their applications. By collecting application logs, traces, and performance metrics, they can diagnose issues, optimize application performance, and improve the user experience.
5. **Infrastructure Optimization:** Log Analytics Workspace helps optimize infrastructure resources by analyzing operational data and identifying opportunities for optimization. Organizations can track resource utilization, identify underutilized resources, and right-size their infrastructure to improve cost efficiency.
6. **DevOps and Continuous Monitoring:** Log Analytics Workspace integrates seamlessly with DevOps processes, enabling continuous monitoring and feedback loops. Teams can use log data to monitor application deployments, track performance trends, and automate remediation actions to ensure continuous delivery and deployment.
7. **Predictive Analytics and Anomaly Detection:** By leveraging machine learning capabilities, Log Analytics Workspace can perform predictive analytics and anomaly detection on log data. Organizations can identify abnormal behavior, predict future trends, and proactively address potential issues before they impact operations.
8. **Business Intelligence and Decision Making:** Log Analytics Workspace provides insights into business operations by analyzing log data from various sources, including customer interactions, transactions, and user behavior. Organizations can gain actionable insights, make data-driven decisions, and drive business growth.

In this lab, we're setting up a Log Analytics Workspace in Azure and configuring data collection rules to gather log and telemetry data from various sources, such as virtual machines. The end goal is to centralize log data for analysis and monitoring, enabling users to gain operational insights, troubleshoot issues, ensure compliance, and enhance security across their Azure environment.

To begin with the Lab:

1. In your Azure Portal search for log analytics workspace and choose the service accordingly.

Log Analytics Workspace

Microsoft

The screenshot shows the 'Log Analytics Workspace' creation page. At the top, there's a Microsoft logo and a 'Log Analytics Workspace' title with a '3.0 (54 ratings)' rating. Below the title, there's a 'Plan' section with a dropdown menu set to 'Log Analytics Workspace' and a 'Create' button. The main area has tabs for 'Basics', 'Tags', and 'Review + Create'. A note about creating a workspace is displayed, followed by a description of what a Log Analytics workspace is. The 'Project details' section includes fields for 'Subscription' (set to 'Azure Pass - Sponsorship') and 'Resource group' (set to 'demo-resource-group'). The 'Instance details' section includes fields for 'Name' (set to 'vm-workspace120') and 'Region' (set to 'North Europe').

- Now you just need to choose your resource group and give it a name. You should also choose the same region as your resources or you might have to pay more.

Basics Tags Review + Create

i A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#) X

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * (i)	Azure Pass - Sponsorship
Resource group * (i)	demo-resource-group
	Create new

Instance details

Name * (i)	vm-workspace120
Region * (i)	North Europe

- Then just move to the review page and create your log analytics workspace.
- Once your deployment is completed go to resources.
- Now in your workspace you need to go to logs. You will see that currently your logs are empty.

The screenshot shows the Azure Log Analytics workspace interface. On the left, there's a sidebar with various navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Logs. The 'Logs' option is highlighted with a red box. The main content area has a search bar at the top, followed by a 'New Query 1' button, a 'Run' button, and a time range selector set to 'Last 24 hours'. Below these are tabs for Tables, Queries, Functions, etc., and a search bar. A message says 'No tables to display' with a note to change filters. To the right, there's a 'Query history' section with a message 'No queries history' and a note about starting queries.

6. Now we are going to define data collection rules. Navigate to Monitor service and then from the left pane scroll down to settings and choose data collection rules from here.

Settings

- Diagnostic settings
-  **Data Collection Rules** (This item is highlighted with a red box)
- Data Collection Endpoints
- Autoscale
- Private Link Scopes

7. Now first we need to choose our resource group then choose the region, after that our platform is Windows as of now and move to next option.

Create Data Collection Rule

Data collection rule management

Basics Resources Collect and deliver Tags Review + create

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources. [Learn more](#)

Rule details

Rule Name *	windows-rule
Subscription *	Azure Pass - Sponsorship
Resource Group *	demo-resource-group
	Create new
Region *	North Europe
Platform Type *	<input checked="" type="radio"/> Windows <input type="radio"/> Linux <input type="radio"/> All
Data Collection Endpoint	<none>

8. Now you need to click on add resources and choose your virtual machine.

Basics Resources Collect and deliver Tags Review + create

Pick a set of resources to collect data from. The Azure Monitor Agent will be automatically installed on virtual machines, scale sets, and Arc-enabled servers. For AKS clusters, managed Prometheus will automatically be enabled. For Windows 10 and 11 devices, [download the client installer](#) and follow the [guidance](#)

<p>This will also enable System Assigned Managed Identity on these resources, in addition to existing User Assigned Identities (if any).</p> <p>+ Add resources + Create endpoint</p> <p>Enable Data Collection Endpoints <input type="checkbox"/></p> <p>Only resources in the same region can be assigned to the same endpoint. Learn more</p>										
<table border="1"><thead><tr><th>Name</th><th>Type</th><th>Location</th><th>Resource group</th><th>Subscription</th></tr></thead><tbody><tr><td>appvm</td><td>Virtual machine</td><td>North Europe</td><td>demo-resource-group</td><td>Azure Pass - Sponsorship</td></tr></tbody></table>	Name	Type	Location	Resource group	Subscription	appvm	Virtual machine	North Europe	demo-resource-group	Azure Pass - Sponsorship
Name	Type	Location	Resource group	Subscription						
appvm	Virtual machine	North Europe	demo-resource-group	Azure Pass - Sponsorship						

9. Then in collect and deliver you need to click on Add data source.

Configure which data sources to collect, and where to send the data to.

+ Add data source

Data source

Destination(s)

No standard data sources or destinations found.

✖ This data collection rule doesn't have any data sources or destinations selected.

10. After that you need to choose performance counters in data source type and choose memory as your performance counter.
11. Then in the destination choose azure monitor metrics and azure monitor logs then click on add data source.

* Data source Destination

Select which data source type and the data to collect for your resource(s).

Data source type *

Performance Counters



Choose Basic to enable the collection of performance counters. Choose Custom if you want more control over which performance counters are collected.

None **Basic** Custom

Performance counter

Sample rate (seconds)

CPU

60

Memory

60

Disk

60

Network

60

* Data source **Destination**

Select the destination(s) for where the data will be delivered. Normal usage charges for the destination will occur. [Learn more about pricing.](#)

+ Add destination

* Destination type

Subscription

Account or namespace

Azure Monitor Metrics (preview)

Azure Pass - Sponsorship



Azure Monitor Logs

Azure Pass - Sponsorship



vm-workspace120 (demo-resourc...)



12. Once your data source is added then you are going to add another data source, this time you have to choose Windows event logs. Then choose the error, warning and information for the logs.

* Data source Destination

Select which data source type and the data to collect for your resource(s).

Data source type *

Windows Event Logs

Info If using Sentinel, use [the connector configuration](#) for collecting Windows Security events to **avoid unexpected increase in storage cost.** [Learn More](#)

System

Critical
 Error
 Warning
 Information
 Verbose

13. Then choose the destination respectively.

* Data source Destination

Select the destination(s) for where the data will be delivered. Normal usage charges for the destination will occur. [Learn more about pricing.](#)

+ Add destination

* Destination type	Subscription	Account or namespace
Azure Monitor Logs	Azure Pass - Sponsorship	vm-workspace120 (demo-resourc...)

14. Now you have created your collection and delivery. Then just move to the review page and create it.

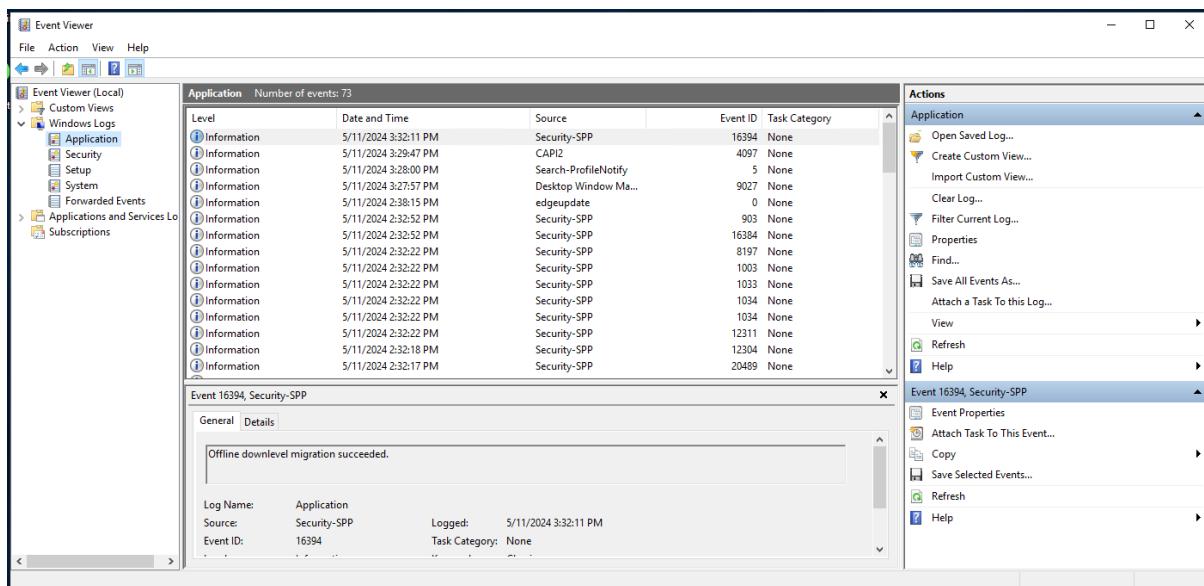
Basics Resources Collect and deliver Tags Review + create

Configure which data sources to collect, and where to send the data to.

+ Add data source

Data source	Destination(s)
Performance Counters	Azure Monitor Metrics (preview), Azure Monitor Logs
Windows Event Logs	Azure Monitor Logs

15. Now what you can do is connect to your machine. For that download the RDP file and use it to get connected with your Windows Virtual machine.
16. Now inside your VM you need to search for **Event Viewer**.
17. Here if you will expand Windows Logs you can see the application level logs, the security logs and the setup logs, etc.



18. What the data collection rule can do is it can take all of this information from the system, the security, and the application and send it all to the log analytics workspace. This is very important and onto the Windows OS ecosystem. The Windows OS collects these logs, and you can view them via the event viewer.
19. Now after 10 mins come back to your Log Analytics workspace and go to logs.
20. This time you can see that we have the logs here.

The screenshot shows the Microsoft Log Analytics workspace. The top navigation bar includes 'Feedback', 'Queries', 'Alerts', and 'Logs'. The main area has a search bar, a 'Run' button, and a 'Time range: Last 24 hours' selector. On the left, there's a sidebar with 'Tables', 'Queries', 'Functions', and a 'Favorites' section. Below that is a 'LogManagement' folder expanded, containing 'Event', 'Heartbeat', and 'Perf' logs. The main workspace shows a query editor with the placeholder text 'Type your query here or click one of the queries to start'.

21. Now if you want to see that logs you just need to write the name of the log and click on run then you'll be able to see the logs.

Run Time range : Last 24 hours Save Share New alert rule Export Pin to ...

1 Event

...

Results Chart

TimeGenerated [UTC]	Source	EventLog	Computer	EventLevel	EventLevelName	ParameterXml	Column
> 5/11/2024, 3:34:05.756 PM	Service Control Manager	System	appvm	4	Information	<Param>Microsoft	
> 5/11/2024, 3:33:56.459 PM	Service Control Manager	System	appvm	4	Information	<Param>AppX Dep	
> 5/11/2024, 3:33:56.286 PM	Service Control Manager	System	appvm	4	Information	<Param>Client Lice	
> 5/11/2024, 3:33:56.286 PM	Service Control Manager	System	appvm	4	Information	<Param>Capability	
> 5/11/2024, 3:32:43.136 PM	Service Control Manager	System	appvm	4	Information	<Param>Software F	
> 5/11/2024, 3:32:11.812 PM	Service Control Manager	System	appvm	4	Information	<Param>Software F	
> 5/11/2024, 3:30:30.451 PM	Service Control Manager	System	appvm	4	Information	<Param>Background	
> 5/11/2024, 3:30:30.325 PM	Service Control Manager	System	appvm	4	Information	<Param>Background	
> 5/11/2024, 3:30:15.184 PM	Service Control Manager	System	appvm	4	Information	<Param>Function D	
> 5/11/2024, 3:30:14.747 PM	Service Control Manager	System	appvm	4	Information	<Param>Function D	
> 5/11/2024, 3:30:14.512 PM	Service Control Manager	System	appvm	4	Information	<Param>Application	
> 5/11/2024, 3:30:01.189 PM	Service Control Manager	System	appvm	4	Information	<Param>Portable D	

1s 296ms | Display time (UTC+00:00) ▾ Query details | 1 - 12 of 39

Run Time range : Last 24 hours Save Share New alert rule Export Pin to ...

1 Heartbeat

...

Results Chart

TimeGenerated [UTC]	SourceComputerId	ComputerIP	Computer	Category
> 5/11/2024, 3:37:47.958 PM	c4f0e9e0-ada0-49a4-84c9-aa3...	40.69.34.28	appvm	Azure Monitor Ag
> 5/11/2024, 3:36:47.939 PM	c4f0e9e0-ada0-49a4-84c9-aa3...	40.69.34.28	appvm	Azure Monitor Ag
> 5/11/2024, 3:35:47.920 PM	c4f0e9e0-ada0-49a4-84c9-aa3...	40.69.34.28	appvm	Azure Monitor Ag
> 5/11/2024, 3:34:47.907 PM	c4f0e9e0-ada0-49a4-84c9-aa3...	40.69.34.28	appvm	Azure Monitor Ag
> 5/11/2024, 3:33:47.897 PM	c4f0e9e0-ada0-49a4-84c9-aa3...	40.69.34.28	appvm	Azure Monitor Ag
> 5/11/2024, 3:32:47.877 PM	c4f0e9e0-ada0-49a4-84c9-aa3...	40.69.34.28	appvm	Azure Monitor Ag
> 5/11/2024, 3:31:47.866 PM	c4f0e9e0-ada0-49a4-84c9-aa3...	40.69.34.28	appvm	Azure Monitor Ag
> 5/11/2024, 3:30:47.852 PM	c4f0e9e0-ada0-49a4-84c9-aa3...	40.69.34.28	appvm	Azure Monitor Ag
> 5/11/2024, 3:29:47.843 PM	c4f0e9e0-ada0-49a4-84c9-aa3...	40.69.34.28	appvm	Azure Monitor Ag