

Azure API Training <> Revanture

Day 5

Log Analytics Workspace

What is Log Analytics Workspace?

A Log Analytics workspace is a data store into which you can collect any type of log data from all of your Azure and non-Azure resources and applications. Workspace configuration options let you manage all of your log data in one workspace to meet the operations, analysis, and auditing needs of different personas in your organization through

- Azure Monitor features, such as built-in insights experiences, alerts, and automatic actions
- Other Azure services, such as Microsoft Sentinel, Microsoft Defender for Cloud, and Logic Apps
- Microsoft tools, such as Power BI and Excel
- Integration with custom and third-party applications

Advantages

- Single source of truth for logs
- Real-time monitoring and alerting
- Cross-resource correlation
- Integration with Azure Security and Automation tools
- Cost-efficient data retention and analysis

Common Use Cases

Security Monitoring

- Detect anomalies and threats using Microsoft Sentinel.

Performance Troubleshooting

- Analyze slow applications or failing services using KQL.

Operational Insights

- Monitor infrastructure health (VMs, containers, databases).

Compliance and Auditing

- Centralize audit logs for compliance tracking.

Cost

The cost of your workspace depends on the volume of data ingested and how long it is retained.

Common Use Cases

Feature	Older (Individual Logs)	Log Analytics Workspace
Storage	Logs stored separately per resource	Centralized storage for all logs
Querying	Manual or per-resource search	Unified querying via KQL
Visualization	Limited dashboards	Advanced charts and dashboards in Azure Portal
Alerting	Basic rule-based alerts	Intelligent alerts and correlation
Integration	Minimal	Deep integration with Sentinel, Defender, App Insights
Scalability	Manual scaling	Automatically scales with data ingestion

Project

Create a Log Analytics Workspace

Enable diagnostics settings

Only for this class purposes

The screenshot shows the Azure portal interface for a resource named 'sfsdfsdf'. The left-hand navigation pane lists various management options, with 'Diagnostic settings' highlighted at the bottom. The main content area is titled 'sfsdfsdf | Diagnostic settings' and includes a search bar, 'Refresh' and 'Feedback' buttons, and three informational links. Below this, a paragraph explains that diagnostic settings are used for streaming export of logs and metrics. A table titled 'Diagnostic settings' displays a single configuration named 'my-diag' which is set to export data to the 'sfsdfsdf' Log Analytics workspace. An '+ Add diagnostic setting' link is provided below the table. Further down, a note instructs the user to click 'Add Diagnostic setting' to configure data collection, followed by a bulleted list of available data types: Audit, Summary Logs, Job Logs, and AllMetrics.

Home > sfsdfsdf

sfsdfsdf | Diagnostic settings ☆ ⋮

Log Analytics workspace

Can you explain how to send diagnostic logs to Azure Monitor? What is the purpose of diagnostic settings? How do diagnostic settings differ from other Azure services?

Search ◊ << Refresh Feedback

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Tables
Agents
Usage and estimated costs
Data export
Network isolation
Identity
Linked storage accounts
Properties
Locks
Classic
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
Advisor recommendations
Workbooks

Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. [Learn more about diagnostic settings](#)

Diagnostic settings

Name	Storage account	Event hub	Log Analytics workspace	Partner solution	Edit setting
my-diag	-	-	sfsdfsdf	-	Edit setting

[+ Add diagnostic setting](#)

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- Audit
- Summary Logs
- Job Logs
- AllMetrics

Add or remove favorites by pressing Cmd+Shift+F or F6

Log Ingestions and Data Sources

Log Ingestion and Data Sources

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources

The screenshot displays the Azure Log Analytics workspace interface. The left sidebar contains a navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Logs, Resource visualizer, Settings, Tables, Agents, Usage and estimated costs, Data export, Network isolation, Identity, Linked storage accounts, Properties, Locks, Classic, Monitoring, Insights, Alerts, Metrics, Diagnostic settings, Advisor recommendations, and Workbooks. The main content area shows the 'Overview' tab for a workspace named 'sfdsfsdf'. It includes a search bar, a delete button, and a notification about the migration of Log Analytics agents from MMA to Azure Monitor Agent. Below this, the 'Essentials' section provides details about the resource group, status, location, subscription, and tags. A 'Get started with Log Analytics' section offers guidance on connecting data sources, configuring monitoring solutions, and monitoring workspace health. At the bottom, there are four tiles for maximizing the Log Analytics experience: Search and analyze logs, Manage alert rules, Manage usage and costs, and Create and Share Workbooks.

Home > Log Analytics workspaces >

sfdsfsdf Log Analytics workspace

What is exports failed (preview) in this Log Analytics workspace? Show me records exported metrics for this Log Analytics workspace. How do I troubleshoot issues with this Log Analytics workspace?

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Logs

Resource visualizer

Settings

Tables

Agents

Usage and estimated costs

Data export

Network isolation

Identity

Linked storage accounts

Properties

Locks

Classic

Monitoring

Insights

Alerts

Metrics

Diagnostic settings

Advisor recommendations

Workbooks

Delete

The Log Analytics agents (MMA,OMS) used to collect logs from virtual machines and servers will no longer be supported from August 31, 2024. Plan to migrate to Azure Monitor Agent before this date. [Learn more about migrating to Azure Monitor Agent](#)

Essentials

Resource group (move) : rg-01

Status : Active

Location : East US

Subscription (move) : Azure subscription 1

Subscription ID : de26e49-edfc-474b-909e-f6b723b0c139

Tags (edit) : Add tags

Workspace Name : sfdsfsdf

Workspace ID : 50221236-b710-4b26-90d0-3b5c8458215f

Pricing tier : Pay-as-you-go

Access control mode : Use resource or workspace permissions

Operational issues : OK

Get Started Recommendations

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

- 1 Connect a data source**
Select one or more data sources to connect to the workspace
[Azure virtual machines \(VMs\)](#)
[Windows and Linux Agents management](#)
[Storage account log](#)
[System Center Operations Manager](#)
- 2 Configure monitoring solutions**
Add monitoring solutions that provide insights for applications and services in your environment
[View solutions](#)
- 3 Monitor workspace health**
Create alerts to proactively detect any issue that arise in your workspace
[Learn more about monitor workspace health](#)

Useful links

[Documentation site](#)

[Community](#)

Maximize your Log Analytics experience

- 1 Search and analyze logs**
Use Log Analytics rich query language to analyze logs
[View logs](#)
- 2 Manage alert rules**
Notify or take action in response to important information in your data
[Set alerts](#)
- 3 Manage usage and costs**
Understand your usage of Log Analytics and estimate your costs for each month
[Manage costs](#)
- 4 Create and Share Workbooks**
Use Workbooks to create rich interactive reports with your data
[Create Workbooks](#)

Add or remove favorites by pressing Ctrl+Shift+F

Basics of Kusto Query Language (KQL)

What is KQL?

- KQL (Kusto Query Language) is used to query, analyze, and visualize data stored in Azure Log Analytics Workspaces.
- It's a read-only language — you can't modify or delete data.

Optimized for:

- Log search
- Data exploration
- Performance troubleshooting
- Security analytics

Think of it as SQL for logs, but simpler and faster.

KQL Query Structure

TableName

| where Condition

| summarize Aggregation by Field

| order by Field desc

KQL Basic Queries

LAQueryLogs

| where TimeGenerated > ago(5m)

LAQueryLogs

| where TimeGenerated > ago(5m)

| summarize p50=percentile(ResponseDurationMs,50), p90=percentile(ResponseDurationMs,90),
p99=percentile(ResponseDurationMs,99) by bin(TimeGenerated, 1m)

| render timechart

KQL Basic Queries

LAQueryLogs

| where TimeGenerated > ago(5m)

| project TimeGenerated, AADEmail, _ResourceId, _SubscriptionId, ScannedGB,
ResponseDurationMs, ResponseCode, ShortQuery = substring(QueryText,0,400)

| order by TimeGenerated desc

| take 50

KQL Basic Queries

LAQueryLogs

| where TimeGenerated > ago(5m)

| summarize QueryCount = count() by bin(TimeGenerated, 30s)

| render timechart

KQL Basic Queries

LAQueryLogs

| where TimeGenerated > ago(5m)

| summarize Queries = count() by AADEmail

| order by Queries desc

| render barchart

KQL Basic Queries

LAQueryLogs

| where TimeGenerated > ago(5m)

| summarize AvgDurationMs = avg(ResponseDurationMs) by AADEmail

| order by AvgDurationMs desc

| render columnchart

KQL Basic Queries

LAQueryLogs

| where TimeGenerated > ago(5m)

| summarize p50 = percentile(ResponseDurationMs, 50),

p90 = percentile(ResponseDurationMs, 90),

p99 = percentile(ResponseDurationMs, 99)

by bin(TimeGenerated, 30s)

| render timechart

Common Functions

`ago()` - Returns a datetime value a specified time span before now.

`now()` - Returns the current UTC date and time.

`datetime_add()` - Adds or subtracts a time unit (hour, day, etc.) from a datetime.

`datetime_diff()` - Returns the difference between two datetimes.

`startofminute()` - Truncates a datetime to the start of the minute.

`startofday()` - Truncates a datetime to the start of the day.

`bin()` - Rounds datetime values into fixed-size bins for aggregation.

Common Functions

`tolower()` / `toupper()` - Converts text to lowercase or uppercase.

`trim()` - Removes leading and trailing characters (usually spaces).

`substring()` - Extracts a portion of a string.

`strlen()` - Returns the length of a string.

`replace()` - Replaces a substring or pattern with another string.

`split()` - Splits a string into an array using a delimiter.

`extract()` - Extracts a substring using a regular expression.

`startswith()` / `endswith()` / `contains()` - Checks if a string starts, ends, or contains a substring.

Common Functions

`count()` - Counts the number of rows.

`sum()` - Calculates the total of a numeric column.

`avg()` - Calculates the average value.

`max()` / `min()` - Returns the maximum or minimum value.

`percentile()` - Calculates the Nth percentile value.

`stdev()` - Calculates standard deviation.

`rand()` - Generates a random number.

Common Functions

[List of all functions](#)

Workbook and Basic Visualization

Workbook

An Azure Workbook is an interactive dashboard and reporting tool inside the Azure Portal that lets you:

visualize data,

monitor metrics,

and analyze logs — all in one unified view.

Think of it as a custom report builder for your Log Analytics queries (KQL), metrics, and monitoring data.

Workbook

Home > Log Analytics workspaces > sfsdfsdf

sfsdfsdf | Workbooks | Gallery ☆ ☆ ...

Log Analytics workspace

Search

+ New Refresh Feedback ? Help Community Git repo Browse across galleries Open recycle bin

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Logs

Resource visualizer

Settings

Classic

Monitoring

Insights

Alerts

Metrics

Diagnostic settings

Advisor recommendations

Workbooks

Automation

Tasks

Export template

Help

All Workbooks Public Templates My Templates

Filter by name or category

Subscription: All Resource Group: All Reset filters

Quick start

Default Template
A report with text and query sections.

Empty
A completely empty workbook.

Dashboard (Preview)
An empty dashboard (preview)

Recently modified workbooks (0)
No items found.

Log Analytics Workspace Insights (7)

Insights

Overview

Usage

Health

Agents

Query Audit

Change Log

Activity Logs Insights (1)

Activity Logs Insights
Activity Logs Insights

View Designer Guides (8)

View Designer Transition ...
Quick start guide to use Workbooks f...

Vertical Overview
Combines multiple views into a vertic...

Tabbed Overview
Combines multiple views into a tabbe...

Two Numbers & List
Outline of the Two Numbers & List Til...

Timeline & List
Outline of the Timeline & List Tile fro...

Number & List
Outline of the Number & List Tile fro...

Line Chart, Callout, & List
Outline of the Line Chart, Callout, & Li...

Donut & List
Outline of the Donut & List Tile from ...

Azure Monitor essentials (1)

Log Analytics Agent Health

Workspace Reports (2)

Add or remove favorites by pressing Cmd+Shift+F

Creating Custom WorkBook

Workbook

Home > sfsdfsdf



sfsdfsdf | Unsaved Dashboard

Log Analytics workspace | sfsdfsdf

Help me create my first Azure Workbook

Query recent Azure Monitor workbooks changes

How do enterprises leverage Workbooks?

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Logs

Resource visualizer

Settings

Classic

Monitoring

Insights

Alerts

Metrics

Diagnostic settings

Advisor recommendations

Workbooks

Automation

Tasks

Export template

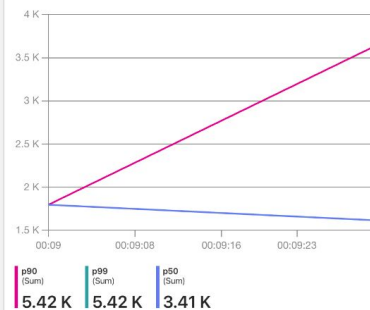
Help

Workbooks Done Editing Save Add Widget

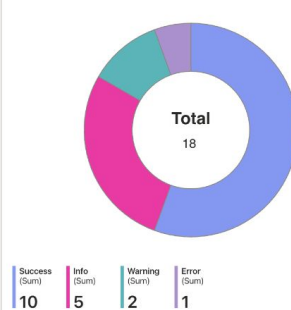
Welcome to the dashboard preview! [What's new in the preview?](#) [View the previous version.](#)

Time Range: Last hour

Counts by table names



Jobs by status



Text Item

Text items support markdown text, and can be styled to look like info, success, warning, and error messages.


Alert Rules and Notifications

Alert Rules

You create an alert rule by combining the resources to be monitored, the monitoring data from the resource, and the conditions that you want to trigger the alert. You can then define action groups and alert processing rules to determine what happens when an alert is triggered.

Alert Rules and Notifications

[Home](#) > [sfsdfsdf](#)

 **sfsdfsdf** | Alerts

Log Analytics workspace

Help me setup a new alert rule

Summarize alerts fired in last 24 hours

Which alerts require my immediate attention

Search

View as timeline (preview) | Create | Set up recommended alerts | Alert rules | Action groups | Alert processing rules | Change user response | Actions | Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Logs

Resource visualizer

Settings

Tables

Agents

Usage and estimated costs

Data export

Network isolation

Identity

Linked storage accounts

Properties

Locks

Classic

Monitoring

Insights

Alerts

Metrics

Diagnostic settings

Advisor recommendations

Workbooks


Set up recommended alert rules

Add commonly-used alert rules for resources like this to get notified on important events happening on this resource.

View + set up

 or

Create custom alert rule



Add or remove favorites by pressing Cmd+Shift+F

Cost Management for Log Retention

Data Retention

During the interactive retention period, you retrieve the data from the table through queries, and the data is available for visualizations, alerts, and other features and services, based on the table plan.

Each table in your Log Analytics workspace lets you retain data up to 12 years in low-cost, long-term retention.

Cost Management

There is no cost for creation of log analytics workspace, you will only be charged for the data which is ingested in log analytics workspace.

You are also charged based on the retention period that you choose.

Cost varies from Region to Region

[Latest Pricing](#)

Cost Optimization Checklist

- Determine whether to combine your operational data and your security data in the same Log Analytics workspace.
- Configure pricing tier for the amount of data that each Log Analytics workspace typically collects.
- Configure data retention and archiving.
- Configure tables used for debugging, troubleshooting, and auditing as Basic Logs.
- Limit data collection from data sources for the workspace.
- Regularly analyze collected data to identify trends and anomalies.
- Create an alert when data collection is high.
- Consider a daily cap as a preventative measure to ensure that you don't exceed a particular budget.
- Set up alerts on Azure Advisor cost recommendations for Log Analytics workspaces.

Data Retention

Home > sfsdfsdf
sfsdfsdf | Usage and estimated costs ☆ ...

Log Analytics workspace

Search

Overview
Usage details
Cost optimization
Insights
Daily cap
Data Retention
Help

You're here

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Logs
- Resource visualizer
- Settings
 - Tables
 - Agents
 - Usage and estimated costs**
 - Data export
 - Network isolation
 - Identity
 - Linked storage accounts
 - Properties
 - Locks
- Classic
- Monitoring
 - Insights
 - Alerts
 - Metrics
 - Diagnostic settings
 - Advisor recommendations

Pricing Tiers

<

Pay-as-you-go

>

Per GB

This Pay-as-you-go pricing tier offers flexible consumption pricing in which you are charged per GB of data ingested. This only includes estimated costs from data ingestion to aid selecting the optimal pricing.

Item type	Price	Monthly usage (last 31 days)	Estimated monthly data ingestion cost
Analytics Logs data ingestion	US\$2.30	0.00 GB	US\$0.00
Basic Logs data ingestion	US\$0.50	0.00 GB	US\$0.00
Auxiliary Logs data ingestion	US\$0.05	0.00 GB	US\$0.00
Total			US\$0.00

i This is the current pricing tier.

Select

- ✓ **100 GB/day Commitment Tier**
15% discount over Pay-as-you-go
- ✓ **200 GB/day Commitment Tier**
20% discount over Pay-as-you-go
- ✓ **300 GB/day Commitment Tier**
22% discount over Pay-as-you-go

Usage Charts

Billable data ingestion by table (last 31 days)

Table

No data

Data Retention

31 days of retention is included with your pricing plan. Longer retention will incur additional charges. Retention can also be configured individually for specific data types.

Data Retention (Days)



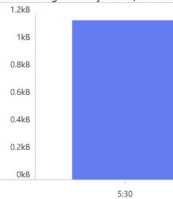
Retention for Application Insights data types default to 90 days and will get the workspace retention if it is over 90 days. To set the retention on these types to be less than 90 days, set the retention on each of these data types. [Learn more.](#)

In addition to setting the default retention for tables in this workspace here, you can configuration data retention and data archive on a per-table basis on the [Tables](#) page of this workspace.

OK



Billable data ingestion by table (last 31 days)



Data ingested by table (last 90 days)

Table

No data

Manage for Individual Table

Home > sfsdfsdf

sfsdfsdf | Tables ☆ ...

Log Analytics workspace

Search

+ Create | Delete

Filter by name

Type: All Plan: All

Showing 13 results

No grouping

<input type="checkbox"/> Table name ↑↓	Type ↑↓	Plan ↑↓	Analytics retention ↑↓	Total retention ↑↓	
<input type="checkbox"/> Alert	Azure table	Analytics	Workspace default (60 days)	30 days	<div><div>Manage table</div><div>Create transformation</div><div>Edit schema</div><div>Access control (IAM)</div></div>
<input type="checkbox"/> AppCenterError	Azure table	Analytics	Workspace default (60 days)	30 days	
<input type="checkbox"/> AzureMetrics	Azure table	Analytics	Workspace default (60 days)	30 days	
<input type="checkbox"/> AzureMetricsV2	Azure table	Analytics	Workspace default (60 days)	30 days	
<input type="checkbox"/> ComputerGroup	Azure table	Analytics	Workspace default (60 days)	30 days	
<input type="checkbox"/> Event	Azure table	Analytics	Workspace default (60 days)	30 days	...
<input type="checkbox"/> InsightsMetrics	Azure table	Analytics	Workspace default (60 days)	30 days	...
<input type="checkbox"/> LAJobLogs	Azure table	Analytics	Workspace default (60 days)	30 days	...
<input type="checkbox"/> LAQueryLogs	Azure table	Analytics	Workspace default (60 days)	30 days	...
<input type="checkbox"/> LASummaryLogs	Azure table	Analytics	Workspace default (60 days)	30 days	...
<input type="checkbox"/> Operation	Azure table	Analytics	Workspace default (60 days)	30 days	...
<input type="checkbox"/> Syslog	Azure table	Analytics	Workspace default (60 days)	30 days	...
<input type="checkbox"/> Usage	Azure table	Analytics	90 days	90 days	...

Add or remove favorites by pressing Cmd+Shift+F

Daily Cap

You can control your costs by applying a cap to the amount of data that you collect per day.

[Home](#) > [sfdsfdfs](#)
Usage and estimated costs ☆☆☆

Log Analytics workspace

 Search

[Usage details](#)
[Cost optimization](#)
[Insights](#)
[Daily cap](#)
[Data Retention](#)
[Help](#)

Access control (IAM)

- Tags
- Determine and solve problems
- Logs
- Resource visualizer
- Settings
 - Tables
 - Agents
 - Usage and estimated costs**
 - Data export
 - Network isolation
 - Identity
 - Linked storage accounts
 - Properties
 - Locks
- Classic
- Monitoring
 - Insights
 - Alerts
 - Metrics
 - Diagnostic settings
 - Advisor recommendations
 - Workbooks
- Automation

Your Log Analytics cost depends on your choice of pricing tier, data retention and which solutions are used. Here you can see the estimated monthly data ingestion cost for each of the available pricing tiers, based on your last 31-days of Log Analytics data ingested. These cost estimates can be used to help you select the best pricing tier based on your data ingestion patterns. This page does not reflect your actual billed usage. To view that, use Cost Management ([learn more](#)).

These estimated costs do not include Microsoft Defender or Microsoft Sentinel costs, but any benefits received from the Defender 500 MB/node/day data allowance or Sentinel Microsoft 365 offer are factored into the estimate of Log Analytics costs ([learn more](#)).

Learn more about [Log Analytics pricing](#) and the many techniques to [optimize your cost](#). If you have questions about using this page, [contact us](#).

Pricing Tiers

Pay-as-you-go

Per GB

The Pay-as-you-go pricing tier offers flexible consumption pricing in which you are charged per GB of data ingested. This only includes estimated costs from data ingestion to aid selecting the optimal pricing.

Item type	Price	Monthly usage (last 31 days)	Estimated monthly data ingestion cost
Analytics Logs data ingestion	US\$2.30	0.00 GB	US\$0.00
Basic Logs data ingestion	US\$0.50	0.00 GB	US\$0.00
Auxiliary Logs data ingestion	US\$0.05	0.00 GB	US\$0.00
Total			US\$0.00

i This is the current pricing tier.

Select

- ✓ **100 GB/day Commitment Tier**
15% discount over Pay-as-you-go
- ✓ **200 GB/day Commitment Tier**
20% discount over Pay-as-you-go
- ✓ **300 GB/day Commitment Tier**
22% discount over Pay-as-you-go

Usage Charts

Billable data ingestion by table (last 31 days)

Table

No data

Daily cap

You can control your costs by applying a cap to the amount of data that you collect per day. Tables in the Auxiliary table plan are not subject to any daily cap. Note that there can be some latency in applying the daily cap, so stopping data ingestion precisely at the specified cap cannot be guaranteed. [?](#)

ON OFF

! Be sure to create an alert so you know if your workspace is capped. [Learn more](#)

OK