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

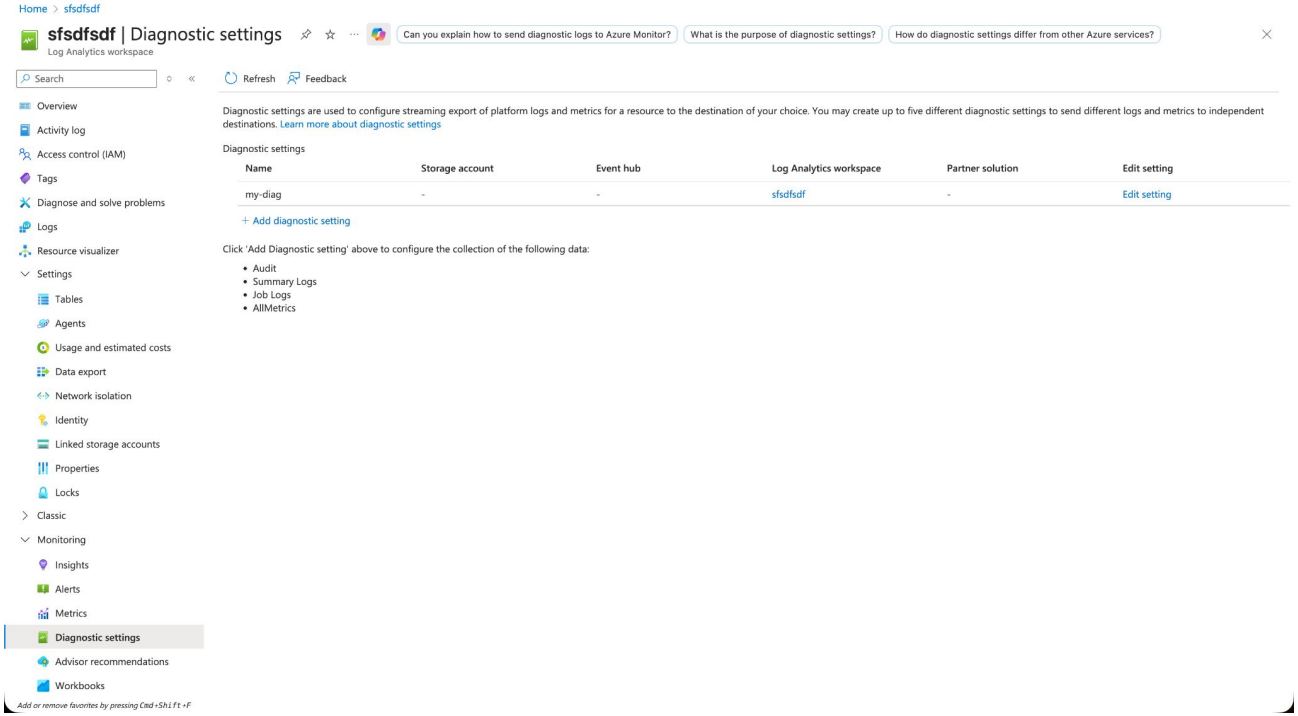
Feature	Older (Individual Logs)	Log Analytics Workspace
Storage	Logs stored separately per resource	Centralized storage for all logs
Querying	Manual or per-resource search	Unified querying via KQL
Visualization	Limited dashboards	Advanced charts and dashboards in Azure Portal
Alerting	Basic rule-based 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

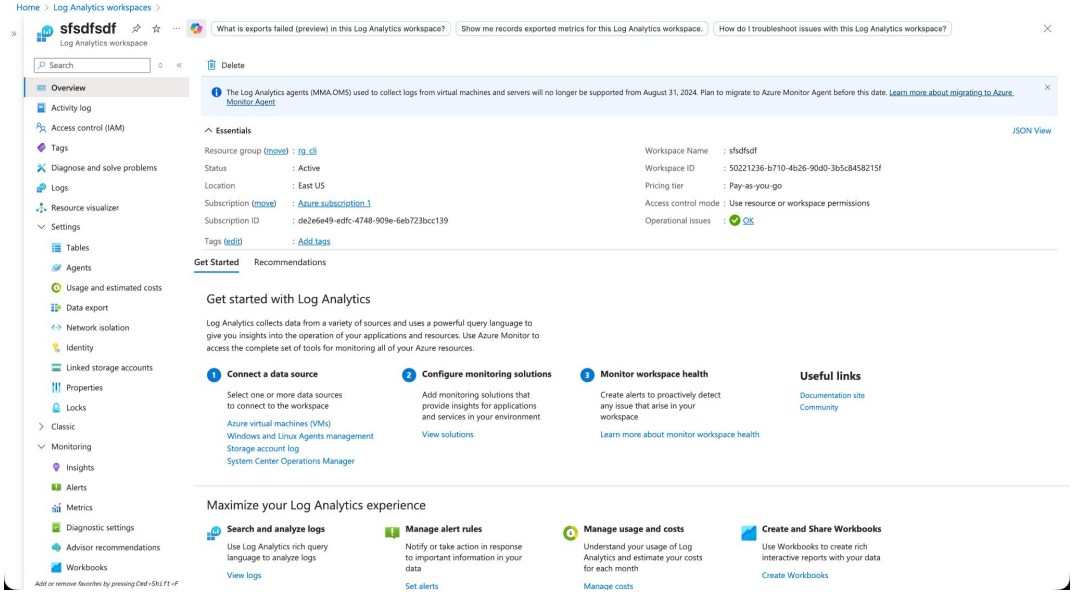
Only for this class purposes



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



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:

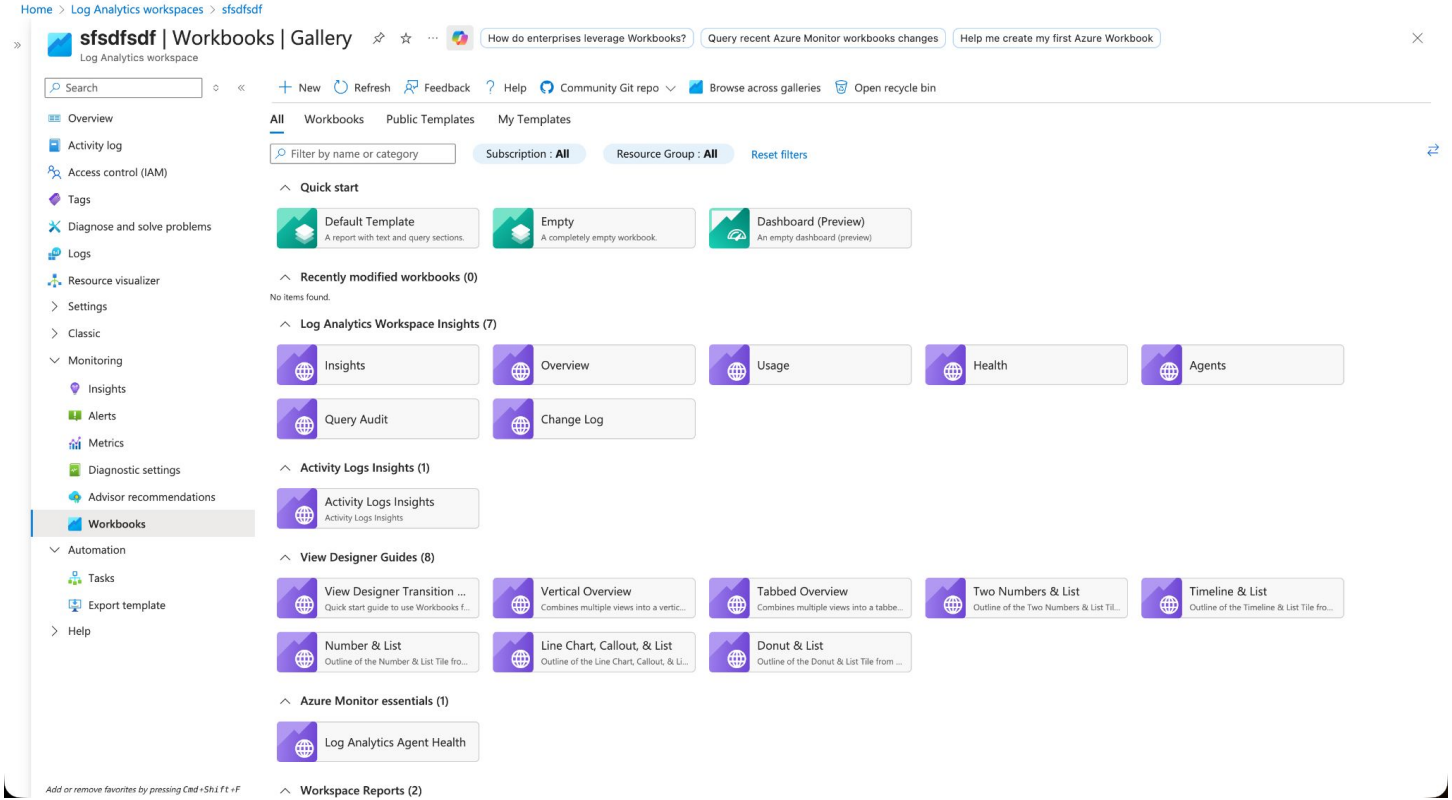
visualize data,

monitor metrics,

and analyze logs — all in one unified view.

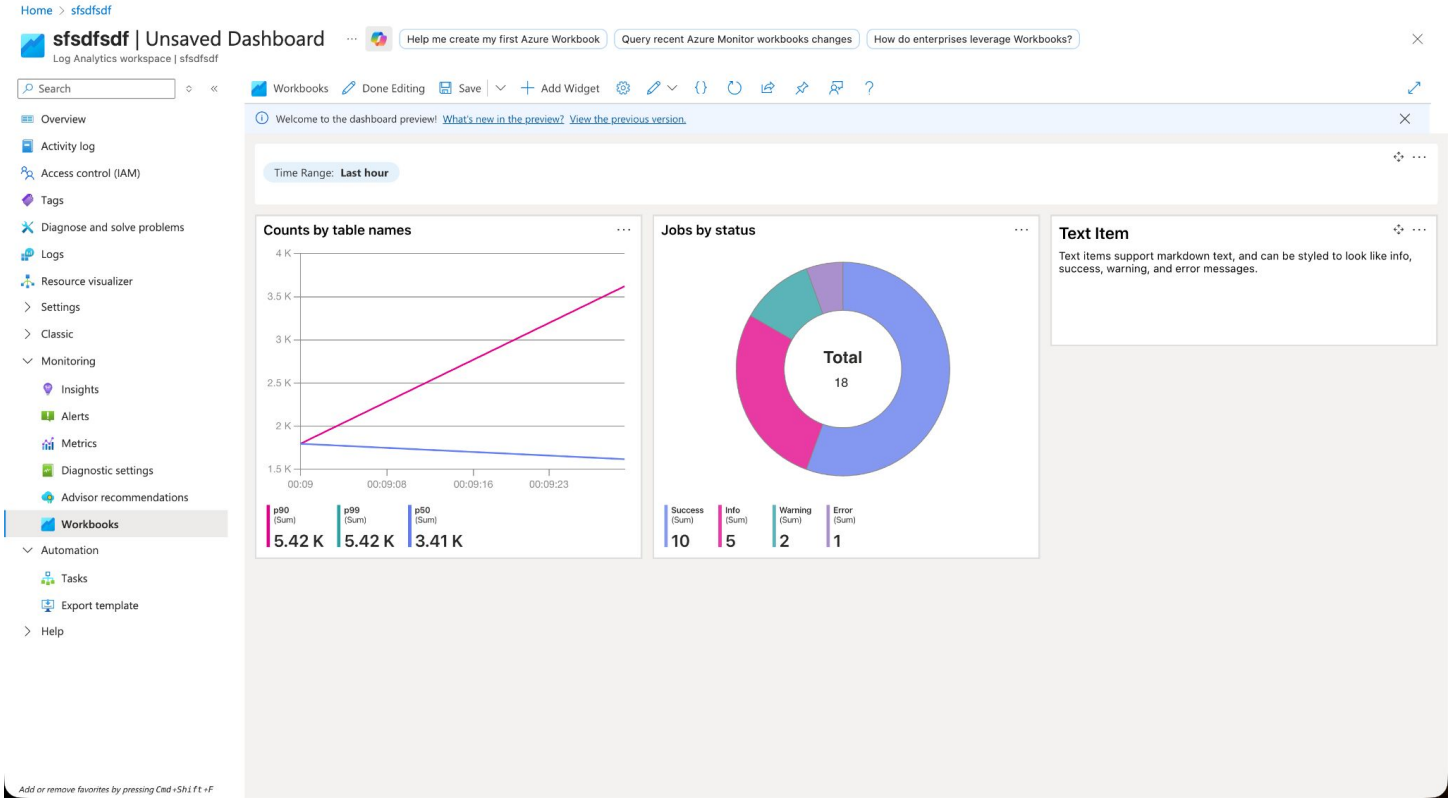
Think of it as a custom report builder for your Log Analytics queries (KQL), metrics, and monitoring data.

Workbook


Home > Log Analytics workspaces > sfsdfsdf
sfsdfsdf | Workbooks | Gallery
Log Analytics workspace
How do enterprises leverage Workbooks?
Query recent Azure Monitor workbooks changes
Help me create my first Azure Workbook
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
Add or remove favorites by pressing Cmd+Shift+F
New
Refresh
Feedback
Help
Community Git repo
Browse across galleries
Open recycle bin
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)

Creating Custom WorkBook

Workbook

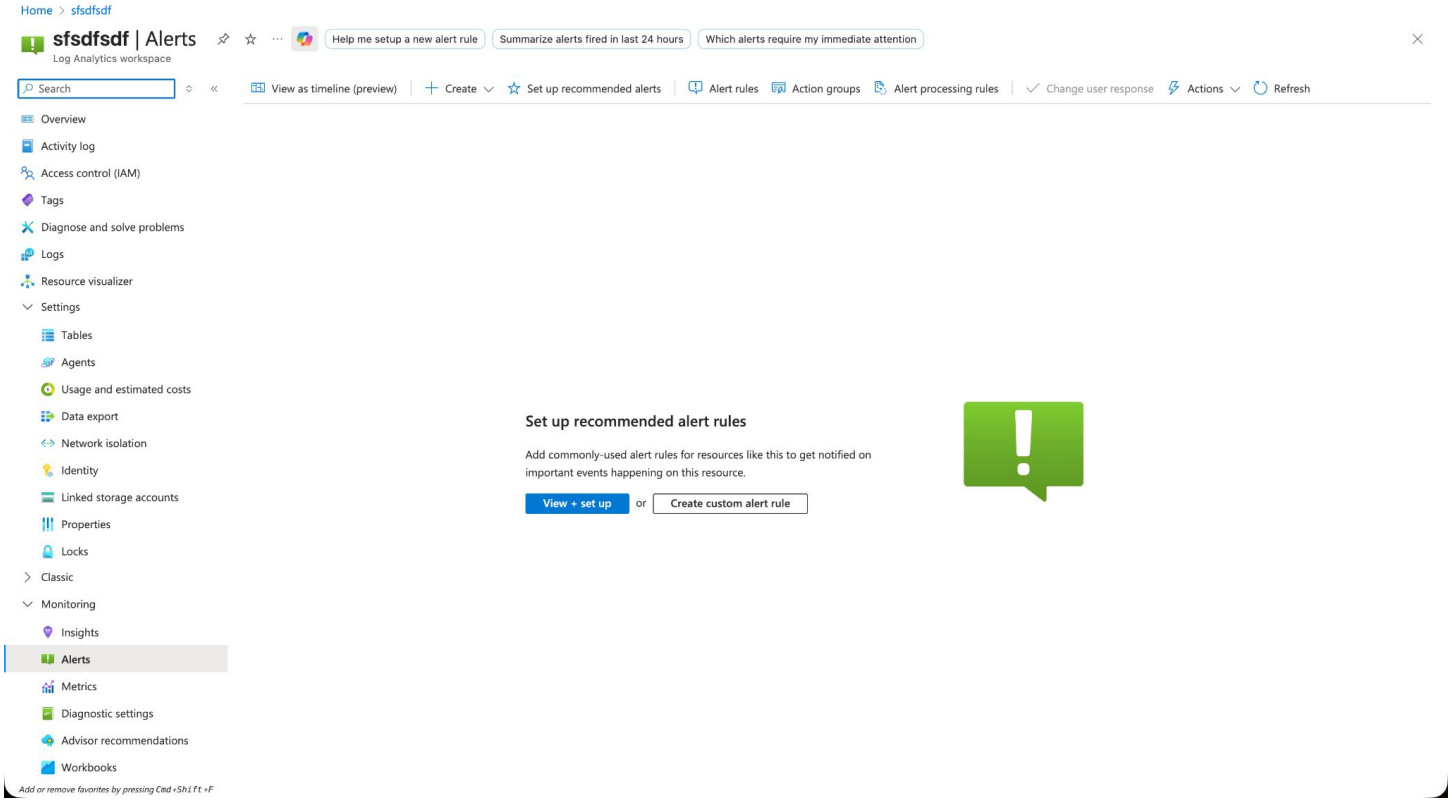

Home > sfsdfsdf
sfsdfsdf | Unsaved Dashboard
Log Analytics workspace | sfsdfsdf
Help me create my first Azure Workbook
Query recent Azure Monitor workbooks changes
How do enterprises leverage Workbooks?
Search
Workbooks
Done Editing
Save
Add Widget
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Logs
Resource visualizer
Settings
Classic
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
Advisor recommendations
Workbooks
Automation
Tasks
Export template
Help
Welcome to the dashboard preview! What's new in the preview? View the previous version.
Time Range: Last hour
Counts by table names
4 K
3.5 K
3 K
2.5 K
2 K
1.5 K
00:09
00:09:08
00:09:16
00:09:23
p90 (Sum) 5.42 K
p99 (Sum) 5.42 K
p50 (Sum) 3.41 K
Jobs by status
Total
18
Success (Sum) 10
Info (Sum) 5
Warning (Sum) 2
Error (Sum) 1
Text Item
Text items support markdown text, and can be styled to look like info, success, warning, and error messages.
Add or remove favorites by pressing Cmd+Shift+F

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



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
- 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

Add or remove favorites by pressing Cmd+Shift+F

Usage details | Cost optimization | Insights | Daily cap | Data Retention | Help

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 Recommended Tier

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.

Estimated costs

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**

This is the current pricing tier.

Select

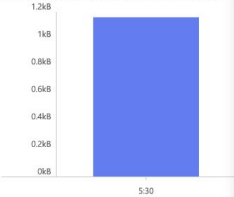
100 GB/day Commitment Tier
15% discount over Pay-as-you-go

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)



Data ingested by table (last 90 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) 30

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

Manage for Individual Table

Home > sfsdfsdf

sfsdfsdf | Tables
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

Add or remove favorites by pressing Ctrl+Shift+F

Create | Delete

Filter by name | Type : All | Plan : All

Showing 13 results

No grouping

Table name	Type	Plan	Analytics retention	Total retention
Alert	Azure table	Analytics	Workspace default (60 days)	30 days
AppCenterError	Azure table	Analytics	Workspace default (60 days)	30 days
AzureMetrics	Azure table	Analytics	Workspace default (60 days)	30 days
AzureMetricsV2	Azure table	Analytics	Workspace default (60 days)	30 days
ComputerGroup	Azure table	Analytics	Workspace default (60 days)	30 days
Event	Azure table	Analytics	Workspace default (60 days)	30 days
InsightsMetrics	Azure table	Analytics	Workspace default (60 days)	30 days
LAJobLogs	Azure table	Analytics	Workspace default (60 days)	30 days
LAQueryLogs	Azure table	Analytics	Workspace default (60 days)	30 days
LASummaryLogs	Azure table	Analytics	Workspace default (60 days)	30 days
Operation	Azure table	Analytics	Workspace default (60 days)	30 days
Syslog	Azure table	Analytics	Workspace default (60 days)	30 days
Usage	Azure table	Analytics	90 days	90 days

- Manage table
- Create transformation
- Edit schema
- Access control (IAM)

Daily Cap

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