

Build the Log Analytics Workspace

- Go to Azure Portal → Create Resource → Log Analytics Workspace
- Resource Group: RG-Sentinel
- Workspace Name: SentinelLogWorkspace
- Region: East US
- Click **Review + Create** → **Create**



Microsoft Azure

Home > Create a resource > Marketplace >

Log Analytics Workspace

Microsoft

Log Analytics Workspace [Add to Favorites](#)

Microsoft | Azure Service

★ 3.0 (55 ratings)

[Azure benefit eligible](#)

Subscription: Azure subscription 1 Plan: Log Analytics Workspace [Create](#)

Overview Plans Usage Information + Support Ratings + Reviews

About Azure Monitor Log Analytics

With Azure Monitor Log Analytics 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.

A Log Analytics workspace is the basic management unit of Log Analytics.

Create a new workspace

A Log Analytics workspace is an Azure resource and a container where data is collected, aggregated, and serves as an administrative boundary. Creating an Azure Monitor Log Analytics workspace has some specific considerations you need to account for before choosing to create a new workspace.

Please refer to the following documentation to learn more about the consideration you need to take before creating a new Log Analytics workspace.

Click on the 'Create' button to create an Azure Log Analytics workspace.

Microsoft Azure

Home > Create a resource > Marketplace > Log Analytics Workspace >

Create Log Analytics workspace

Validation passed

Basics Tags [Review + Create](#)

Log Analytics workspace by Microsoft

Basics

Subscription: Azure subscription 1
Resource group: RG-Sentinel
Name: SentinelLogWorkspace
Region: East US

Pricing

Pricing tier: Pay-as-you-go (Per GB 2018)

The cost of your workspace depends on the volume of data ingested and how long it is retained. Regional pricing details are available on the [Azure Monitor pricing page](#). You can change to a different pricing tier after the workspace is created.

Tags

None

 Pricing Note: Sentinel charges only when data is ingested. First 10 GB/day are free for 30 days.

Microsoft Azure

Home >

Microsoft.LogAnalyticsOMS | Overview

Deployment

Search [Delete](#) [Cancel](#) [Redeploy](#) [Download](#) [Refresh](#)

Overview

Inputs

Outputs

Template

✓ Your deployment is complete

Deployment name: Microsoft.LogAnalyticsOMS
Subscription: Azure subscription 1
Resource group: RG-Sentinel

[Deployment details](#)

[Next steps](#)

[Go to resource](#)

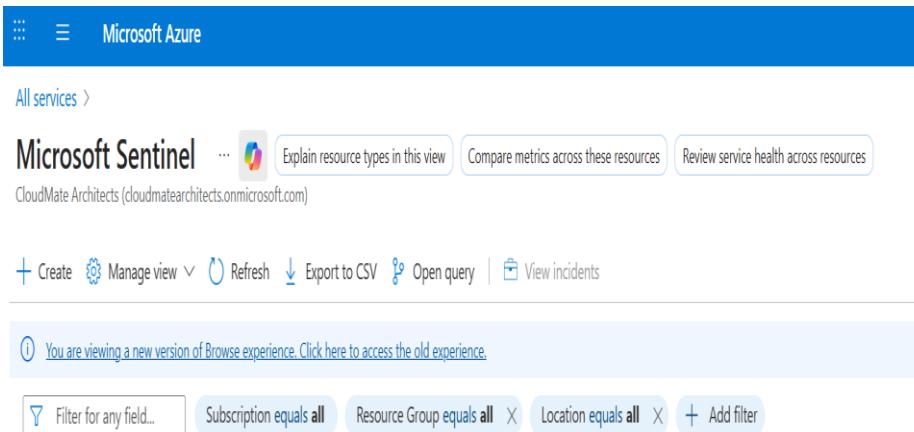
[Give feedback](#)

[Tell us about your experience with deployment](#)

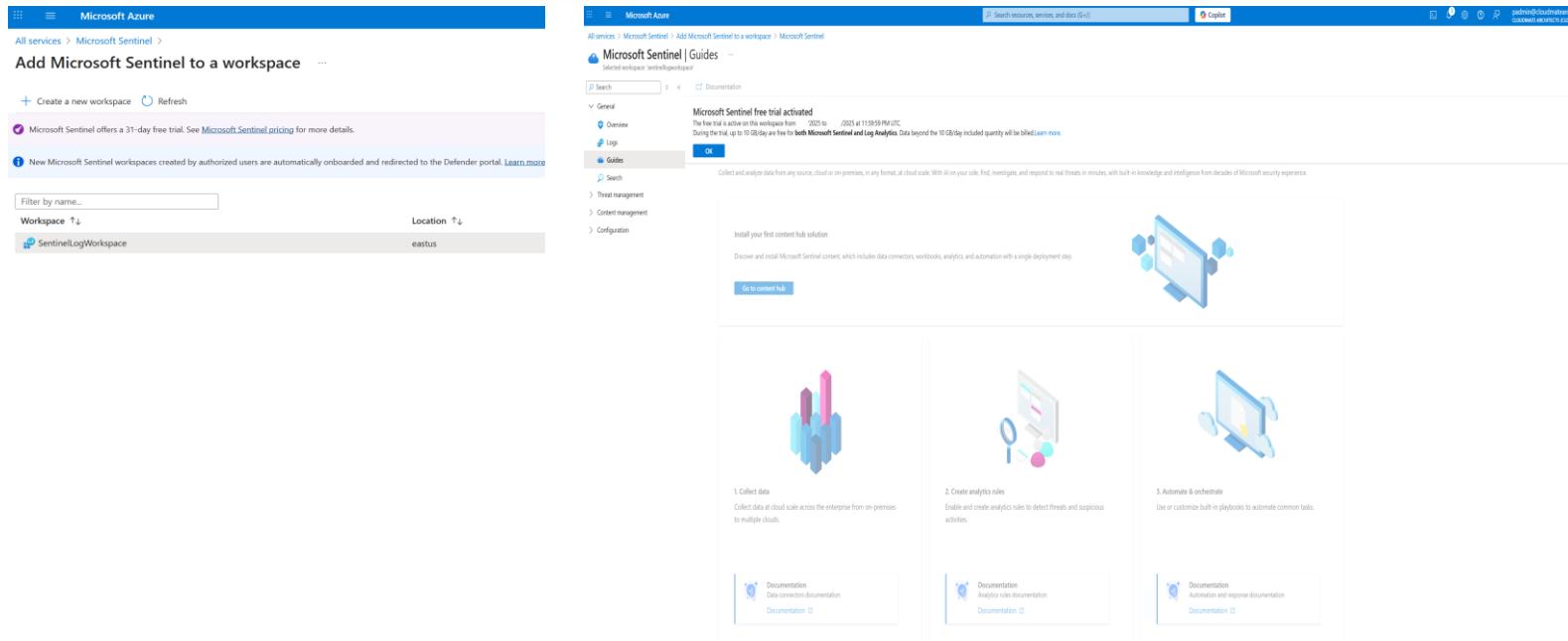
 **PerparimLabs**

Step 2 — Enable Microsoft Sentinel

- Azure Portal → Search Microsoft Sentinel
- Click Create
- Choose SentinelLogWorkspace
- Click Add



The screenshot shows the Microsoft Azure portal with the Microsoft Sentinel workspace creation interface. The top navigation bar is blue with the Microsoft Azure logo. Below it, the main content area has a blue header 'Microsoft Sentinel' with a 'Create' button. The main area is titled 'Add Microsoft Sentinel to a workspace' and includes a 'Create a new workspace' button, a 'Refresh' button, and a note about a 31-day free trial. It also shows a workspace named 'SentinelLogWorkspace' in the 'Workspace' dropdown and a location 'eastus'. At the bottom, there are filter and search options, and a note about viewing a new version of the experience.



The screenshot shows the Microsoft Sentinel workspace creation interface on the 'Guides' page. The top navigation bar is blue with the Microsoft Azure logo. The main content area is titled 'Microsoft Sentinel | Guides' and shows a note about a free trial activated. It includes a 'Search' bar, a sidebar with 'General', 'Overview', 'Logs', 'Guides', 'Search', 'Threat management', 'Content management', and 'Configuration' options, and a 'Documentation' link. Below the sidebar, there are three main sections: '1. Collect data', '2. Create analytics rules', and '3. Automate & orchestrate'. Each section has an icon and a brief description. At the bottom, there are 'Documentation' links for Data connector documentation, Analytics rules documentation, and Automation and response documentation.

Microsoft Azure

All services >

Microsoft Sentinel | Overview

Selected workspace: 'sentinellogworkspace'

Search

General

- Overview
- Logs
- Guides
- Search

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)
- SOC optimization

Content management

- Content hub
- Repositories
- Community

Configuration

- Workspace manager (Preview)
- Data connectors
- Analytics
- Summary rules
- Watchlist
- Automation
- Settings

Step 3 — Verify Sentinel Is Live

- Open your new Sentinel workspace
- Confirm dashboard shows:
- Data Connectors
- Analytics
- Workbooks
- Hunting



Sentinel Workspace Deployed

- Log Analytics workspace created
- Microsoft Sentinel enabled
- Sentinel dashboard verified
- Environment ready for future labs

